

# Demonstration of user interface concepts

June 3, 2022

DE 19-197 Prehearing Conference

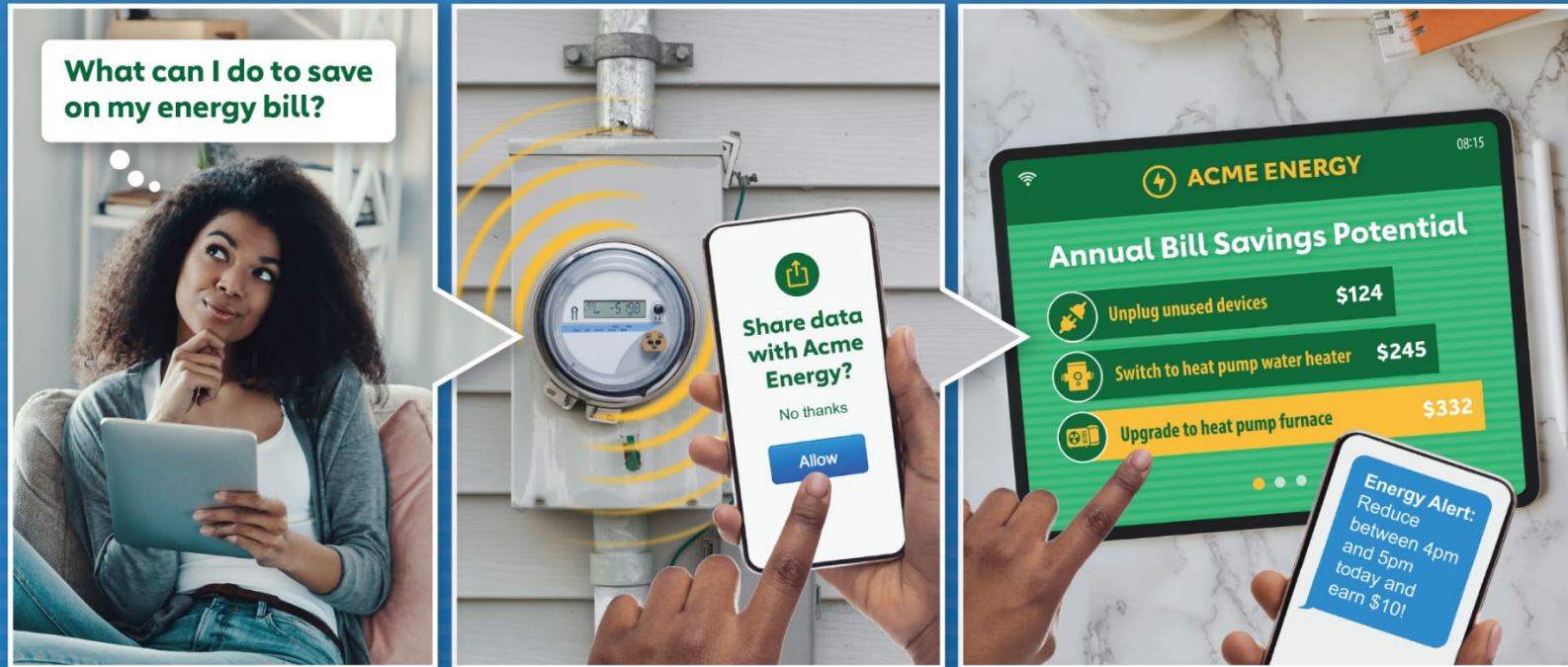
New Hampshire Public Utilities Commission

## Table of contents

1. High-level overview
2. Green Button Connect in other jurisdictions
3. Authorization form components
4. Live demonstration of a data-sharing platform

# 1. High-level overview

## How energy data portability benefits consumers

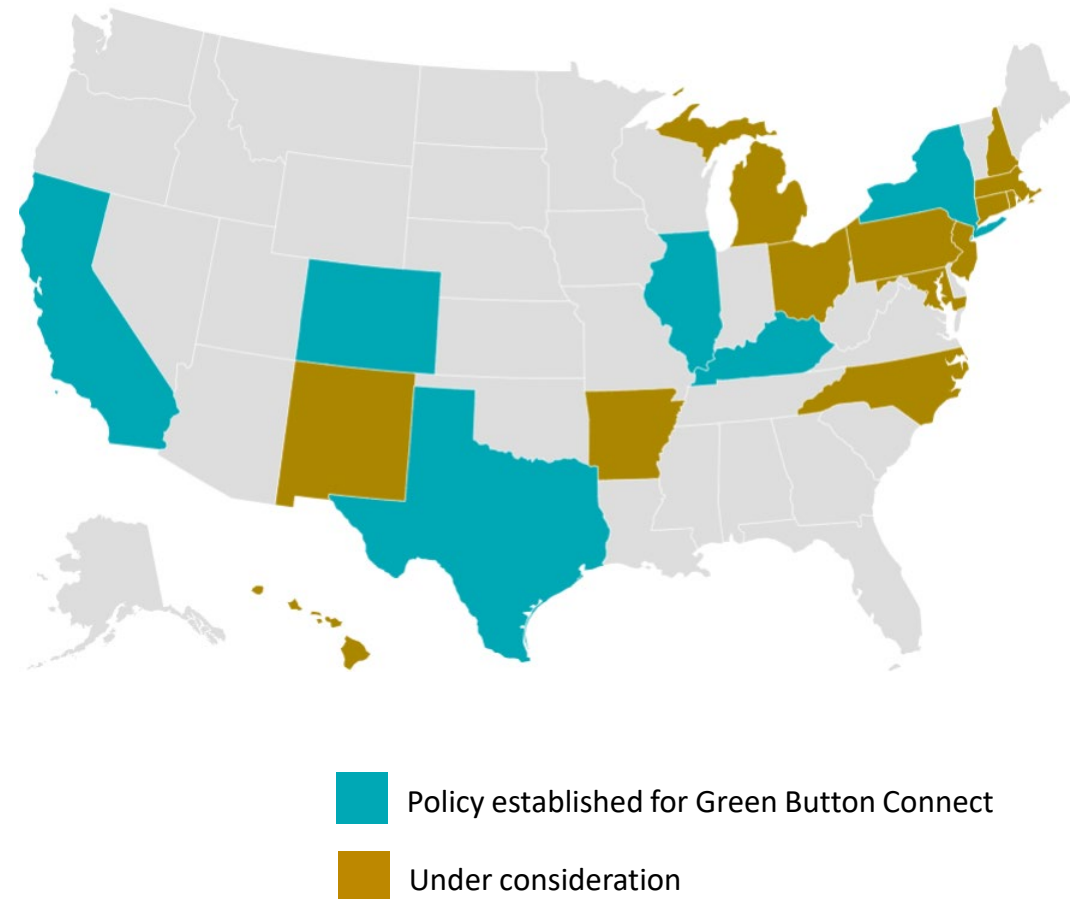


### Customer consent is:

1. Required to share any information (opt-in)
2. Freely given and informed
3. Necessary to access digital products and services that are available from competitive providers

## 2. Green Button Connect in other jurisdictions

- The **data-sharing authorization process** is a critical focus area for the Governance Council because it represents the intersection of technical and legal considerations in granting consent.
- The DE 19-197 settlement agreement outlines some requirements for the authorization process, but the Governance Council intends to evaluate and learn from other jurisdictions' experiences.
- The states with the most Green Button experience are California (since 2016), Illinois (since 2018), Texas (since 2020) and New York (since 2021).
- The Governance Council will carefully review these jurisdictions' policies and practices before finalizing the design for New Hampshire.



### 3. Authorization form components

#### Green Button Connect OAuth 2.0 Authorization Form - Wireframe

"Who"  
(what third party is  
requesting authorization)

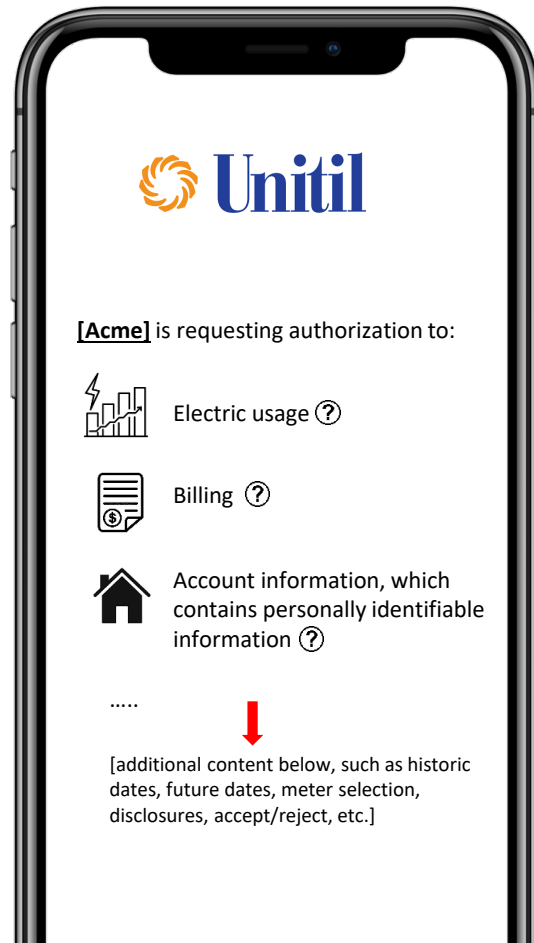
"What"  
(scope of  
what data fields to be shared,  
how far back (historical),  
how far forward (ongoing),  
and for which accounts/services)  
(pre-fillable by third party,  
can be modified by customer if  
third party allows editing)

"Why"  
(how the data is authorized to  
be used after consent is given)  
(pre-written by third party,  
customizable per data request)

"Yes/No"  
(one-click consent/decline)

- Before this step, the customer logs in to their utility’s website. This establishes their ***identity***.
- Next, customers are presented with a web page like this one, describing the “who,” “what” and “why” of sharing their energy information.
- The “why” will be developed to comply with RSA 363:38V(b) during the design phase.
- This “wireframe” was included in Appendix F of the unanimous settlement agreement.

### 3. Authorization form components



- The authorization occurs on a web page controlled by the utilities. This is to ensure security and to comply with technical standards such as OAuth2.0 and Green Button Connect.
- It will be optimized for various screen sizes (desktop, tablet, mobile). See hypothetical example on a mobile web browser.
- The final presentation for customers will be decided upon during the design phase after taking into account technical, statutory and Commission requirements, as well as designing for an excellent customer experience.

## 4. Live demonstration



- Lakefront Utilities in Ontario, Canada serves 10,300 customers
- This is one example of the ~60 electric and gas utilities in Ontario that are required by law to offer Green Button Connect by November, 2023
- Although the Governance Council has not finalized the design of the authorization form, Lakefront provides a good example that is publicly accessible through a “demo” account
- See the slides below if a live demonstration is not technically workable

## 4. Live demonstration (reference slides)



**Sandbox Mode:** You are currently limited to using **test accounts**. *(this message only appears in sandbox mode)*



### Verification Required

Your session has expired. We need to verify your identity again to access the requested page.

**Account:** HEATHER HOMEOWNER **test account**

Continue to verification >

[Need to login as another account?](#)

[Decline this authorization](#)







[Terms](#) | [Privacy](#) | [Help](#) | Powered by [UtilityAPI](#)

Clicking this button takes the customer to the **authentication** process (i.e. identity verification) on a web page. This process is specific to each utility, many of which use a combination of account number and telephone number. Customers with an online account can also enter their username and password (such customers have already established their online identity).

## 4. Live demonstration (reference slides)



[EnView Energy](#) is requesting authorization to:

	<b>Access your account details, energy usage, and bills.</b> This includes your account number, service address, rate plan, meter readings, and utility bill line items.	
	<b>Both historical and ongoing data</b> Share historical energy usage and bills going back 2 years, and continue to share energy usage and bills for 3 years.	
	<b>For all of your services</b> Share above data for all of your services (e.g. meters). <ul style="list-style-type: none"><li>• 123456789-0 (1234 Main Ave, Cobourg, Ontario) <i>Electric</i></li></ul>	

### How your data will be used:

for EnView energy management service *Written by EnView Energy*

[Authorize EnView Energy](#) [Decline](#)



You can revoke your authorization at any time. We will email you a receipt.



## 4. Live demonstration (reference slides)




By clicking on the “account details,” customers can select the types of information they want to share.



 **Access your account details, energy usage, and bills.** 

This includes your account number, service address, rate plan, meter readings, and utility bill line items.

**Data Categories:**


- Account details 
- Energy usage 
- Utility bills 


These are the categories of data you can choose to share with this third party. You can see more details on what specific data fields are shared in each category by clicking on the information icon beside each category.


## 4. Live demonstration (reference slides)





By clicking to edit timeframes, customers can select dates for both **historical** and **ongoing** sharing.


**Both historical and ongoing data** 

 Share historical energy usage and bills going back 2 years, and continue to share energy usage and bills for 3 years.

**Historical data:** 

Last 24 months (2 years) 

**Ongoing data:** 


For 36 months (3 years) 


These determine what timespan of data we share with the third party. You can choose to share both historical and ongoing (e.g. future) data, and specify a cutoff time when you want data sharing to stop.

## 4. Live demonstration (reference slides)


Customers select which **meters/services** they want to share. For example, commercial customers might have multiple locations, or a combination of electric and gas meters.



**For all of your services** 


 Share above data for all of your services (e.g. meters).

- 123456789-0 (1234 Main Ave, Cobourg, Ontario) *Electric*

**Select which services (e.g. meters) to share:** 

Share data for all my services, including services added in the future ([1 total](#))

Select specific services (1 selected)

**Filter**   [Select All](#) [Unselect All](#)

	Account No.	Service Address	Service Type
<input checked="" type="checkbox"/>	123456789-0	1234 Main Ave, Cobourg, Ontario	Electric

If you have multiple services (e.g. meters) associated with your utility account. You can choose to share data for all of your services or just some of them.

## New Hampshire Data Platform Security Control Mapping to Industry Standards

Question No	Question	NIST Cyber Security Framework	NIST 800-171 Protecting Confidential, Unclassified Information
1	Do you require anti-malware protection technologies on your computing systems (PCs, Servers, etc)? Examples of anti-malware protection technologies are: Norton AV, host-based intrusion prevention (e.g. McAfee IPS), or advanced endpoint protection technology (e.g. Crowdstrike).	<b>Category: Security Continuous Monitoring,</b> <b>Sub-Category: DE.CM-4</b> Malicious code is detected.	<b>Security Requirement: 3.14 System and Information Integrity</b> <b>3.14.3</b> Monitor system security alerts and advisories and take action in response.
2	Do you employ hard disk encryption technologies (e.g. whole disk, file level, etc) on your desktops and laptops and systems that may store data obtained from the Data Portal? For example, Macintosh computers default to encryption, Windows systems offer encryption at setup.	<b>Category: Data Security</b> <b>Sub-Category: PR.DS-1</b> Data-at-rest is protected.	<b>Security Requirement: 3.13 System and Communications Protection</b> <b>3.13.8</b> Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
3	Do you utilize Two-Factor Authentication controls for individuals accessing your systems from remote locations? Please describe.	<b>Category: Access Control</b> <b>Sub-Category: PR.AC-1</b> Identities and credentials are managed for authorized devices and users. <b>Sub-Category: PR.AC-3</b> Remote access is managed. <b>Sub-Category: PR.AC-7</b> Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	<b>Security Requirement: 3.05 Access Controls</b> <b>3.5.3</b> Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.[24] [25].

Question No	Question	NIST Cyber Security Framework	NIST 800-171 Protecting Confidential, Unclassified Information
4	Do you have a written Information Security policy, sponsored and approved by senior management, published and available to all employees? If yes, please describe the major components of the policy.	<b>Category: Governance</b> <b>Sub-Category: ID.GV-1</b> Organizational cybersecurity policy is established and communicated.	<b>Chapter 3 "The Requirements"</b> discusses the Security Plan which describes the controls listed in the document. The security plan is consistent to policies for the organization.
5	Does your information security policy include a written employee "Acceptable Use" policy that includes handling of customer data and use of company systems?	<b>Category: Information Protection Processes and Procedures</b> <b>Sub-Category: PR.IP-11</b> Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	<b>Security Requirement: 3.2 Awareness and Training</b> <b>3.2.1</b> Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
6	Do you have written policies/procedures/guidelines for maintaining and monitoring the security of customer data?	<b>Category: Governance</b> <b>Sub-Category: ID.GV-1</b> Organizational cybersecurity policy is established and communicated.	<b>Chapter 3 "The Requirements"</b> discusses the Security Plan which describes the controls listed in the document. The security plan is consistent to policies for the organization.
7	Do you follow documented processes for maintaining software currency and patch management to ensure that security-related patches (e.g. desktops, laptops, server OS, Database, Application, etc) are addressed within a reasonable timeframe? Please describe.	<b>Category: Information Protection Processes and Procedures</b> <b>Sub-Category: PR.IP-12</b> A vulnerability management plan is developed and implemented.	<b>Security Requirement: 3.11 Risk Assessment</b> <b>3.11.2</b> Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
8	If you have a data processing facility, do you employ physical security controls (e.g. card-controlled entry doors, security guards, etc.) to protect your data processing facilities? Please describe or provide program documentation (If a third-party hosting service is used, please describe their controls).	<b>Category: Identity Management, Authentication and Access Control</b> <b>Sub-Category: PR.AC-2</b> Physical access to assets is managed and protected	<b>Security Requirement: 3.10 Physical Security</b> <b>3.10.1</b> Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

Question No	Question	NIST Cyber Security Framework	NIST 800-171 Protecting Confidential, Unclassified Information
9	Do you conduct background checks (e.g. credit, criminal, drug, employment checks, etc) for all employees? Please describe.	<b>Category: Risk Assessment</b> <b>Sub-Category: ID.RA-5</b> Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	<b>Security Requirement: 3.9 Personnel Security</b> <b>3.9.1</b> Screen individuals prior to authorizing access to organizational systems containing CUI.
10	Do you have an Information Security Awareness program developed and implemented for all employees?	<b>Category: Awareness and Training</b> <b>Sub-Category: PR.AT-1</b> All users are informed and trained: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities <b>Sub-Category: PR.AT-4</b> Senior executives understand their roles and responsibilities.	<b>Security Requirement: 3.2 Awareness and Training</b> <b>3.2.1</b> Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
11	Do you have a documented Incident Response plan that includes monitoring for security events, and handling security incidents that addresses incident management responsibilities and evidence preservation? Do you have a process for backing up company and customer data and are thee appropriate access controls to the backed up data.? Please describe.	<b>Category: Information Protection Processes and Procedures</b> <b>Sub-Category: PR.IP-9</b> Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	<b>Security Requirement: 3.6 Incident Response</b> <b>3.6.1</b> Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Question No	Question	NIST Cyber Security Framework	NIST 800-171 Protecting Confidential, Unclassified Information
12	Do you change default system account names and passwords across all systems? Please describe.	<p><b>Category: Identity Management, Authentication and Access Control</b></p> <p><b>Sub-Category: PR.AC-1</b> Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.</p> <p><b>Sub-Category: PR.AC-4</b> Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.</p> <p><b>Sub-Category: PR.AC-7</b> Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).</p>	<p><b>Security Requirement: 3.5 Identification and Authentication</b></p> <p><b>3.5.2</b> Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.</p>
13	Do you perform regular data backups? If yes, how do you protect the backup media?	<p><b>Category: Information Protection Processes and Procedures</b></p> <p><b>Sub-category: PR.IP-4</b> Backups of information are conducted, maintained, and tested.</p>	<p><b>Security Requirement: 3.8 Media Protection</b></p> <p><b>3.8.9</b> Protect the confidentiality of backup CUI at storage locations.</p>
14	Do you utilize perimeter security technologies such as Firewalls and email scanning systems? Please describe.	<p><b>Category: Identity Management, Authentication and Access Control</b></p> <p><b>Sub-Category: PR.AC-5</b> Network integrity is protected (e.g., network segregation, network segmentation).</p>	<p><b>Security Requirement: 3.1 Access Control</b></p> <p><b>3.1.20</b> Verify and control/limit connections to and use of external systems.</p> <p><b>Security Requirement: 3.13 System and Communications Protection</b></p> <p><b>3.13.5</b> Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.</p>

# Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



## Note to Readers on the Update

Version 1.1 of this Cybersecurity Framework refines, clarifies, and enhances Version 1.0, which was issued in February 2014. It incorporates comments received on the two drafts of Version 1.1.

Version 1.1 is intended to be implemented by first-time and current Framework users. Current users should be able to implement Version 1.1 with minimal or no disruption; compatibility with Version 1.0 has been an explicit objective.

The following table summarizes the changes made between Version 1.0 and Version 1.1.

**Table NTR-1 - Summary of changes between Framework Version 1.0 and Version 1.1.**

Update	Description of Update
Clarified that terms like “compliance” can be confusing and mean something very different to various Framework stakeholders	Added clarity that the Framework has utility as a structure and language for organizing and expressing compliance with an organization’s own cybersecurity requirements. However, the variety of ways in which the Framework can be used by an organization means that phrases like “compliance with the Framework” can be confusing.
A new section on self-assessment	Added Section 4.0 <i>Self-Assessing Cybersecurity Risk with the Framework</i> to explain how the Framework can be used by organizations to understand and assess their cybersecurity risk, including the use of measurements.
Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes	An expanded Section 3.3 <i>Communicating Cybersecurity Requirements with Stakeholders</i> helps users better understand Cyber Supply Chain Risk Management (SCRM), while a new Section 3.4 <i>Buying Decisions</i> highlights use of the Framework in understanding risk associated with commercial off-the-shelf products and services. Additional Cyber SCRM criteria were added to the Implementation Tiers. Finally, a Supply Chain Risk Management Category, including multiple Subcategories, has been added to the Framework Core.
Refinements to better account for authentication, authorization, and identity proofing	The language of the Access Control Category has been refined to better account for authentication, authorization, and identity proofing. This included adding one Subcategory each for Authentication and Identity Proofing. Also, the Category has been renamed to Identity Management and Access Control (PR.AC) to better represent the scope of the Category and corresponding Subcategories.
Better explanation of the relationship between Implementation Tiers and Profiles	Added language to Section 3.2 <i>Establishing or Improving a Cybersecurity Program</i> on using Framework Tiers in Framework implementation. Added language to Framework Tiers to reflect integration of Framework considerations within organizational risk management programs. The Framework Tier concepts were also refined. Updated Figure 2.0 to include actions from the Framework Tiers.

April 16, 2018

Cybersecurity Framework

Version 1.1

Consideration of Coordinated Vulnerability Disclosure	A Subcategory related to the vulnerability disclosure lifecycle was added.
---	--

As with Version 1.0, Version 1.1 users are encouraged to customize the Framework to maximize individual organizational value.

## Acknowledgements

This publication is the result of an ongoing collaborative effort involving industry, academia, and government. The National Institute of Standards and Technology (NIST) launched the project by convening private- and public-sector organizations and individuals in 2013. Published in 2014 and revised during 2017 and 2018, this *Framework for Improving Critical Infrastructure Cybersecurity* has relied upon eight public workshops, multiple Requests for Comment or Information, and thousands of direct interactions with stakeholders from across all sectors of the United States along with many sectors from around the world.

The impetus to change Version 1.0 and the changes that appear in this Version 1.1 were based on:

- Feedback and frequently asked questions to NIST since release of Framework Version 1.0;
- [105 responses](#) to the December 2015 request for information (RFI), [Views on the Framework for Improving Critical Infrastructure Cybersecurity](#);
- Over [85 comments](#) on a December 5, 2017 proposed [second draft of Version 1.1](#);
- Over [120 comments](#) on a January 10, 2017, proposed [first draft Version 1.1](#); and
- Input from over 1,200 attendees at the [2016](#) and [2017](#) Framework workshops.

In addition, NIST previously released Version 1.0 of the Cybersecurity Framework with a companion document, [NIST Roadmap for Improving Critical Infrastructure Cybersecurity](#). This Roadmap highlighted key “areas of improvement” for further development, alignment, and collaboration. Through private and public-sector efforts, some areas of improvement have advanced enough to be included in this Framework Version 1.1.

NIST acknowledges and thanks all of those who have contributed to this Framework.

## Executive Summary

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

To better address these risks, the Cybersecurity Enhancement Act of 2014<sup>1</sup> (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework Version 1.0 under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" (February 2013), and provided guidance for future Framework evolution. The Framework that was developed under EO 13636, and continues to evolve according to CEA, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.

The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the

---

<sup>1</sup>See 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: <https://www.congress.gov/bill/113th-congress/senate-bill/1353/text>.

April 16, 2018

Cybersecurity Framework

Version 1.1

Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.

The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating with the private sector and government agencies at all levels. As the Framework is put into greater practice, additional lessons learned will be integrated into future versions. This will ensure the Framework is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Expanded and more effective use and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing evolving guidance for individual organizations while increasing the cybersecurity posture of the Nation's critical infrastructure and the broader economy and society.

## Table of Contents

Note to Readers on the Update .....	ii
Acknowledgements .....	iv
Executive Summary .....	v
1.0 Framework Introduction .....	1
2.0 Framework Basics.....	6
3.0 How to Use the Framework .....	13
4.0 Self-Assessing Cybersecurity Risk with the Framework.....	20
Appendix A: Framework Core.....	22
Appendix B: Glossary.....	45
Appendix C: Acronyms .....	48

## List of Figures

Figure 1: Framework Core Structure .....	6
Figure 2: Notional Information and Decision Flows within an Organization .....	12
Figure 3: Cyber Supply Chain Relationships.....	17

## List of Tables

Table 1: Function and Category Unique Identifiers .....	23
Table 2: Framework Core .....	24
Table 3: Framework Glossary.....	45

## 1.0 Framework Introduction

The United States depends on the reliable functioning of its critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company’s bottom line. It can drive up costs and affect revenue. It can harm an organization’s ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization’s overall risk management.

To strengthen the resilience of this infrastructure, the Cybersecurity Enhancement Act of 2014<sup>2</sup> (CEA) updated the role of the National Institute of Standards and Technology (NIST) to “facilitate and support the development of” cybersecurity risk frameworks. Through CEA, NIST must identify “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.” This formalized NIST’s previous work developing Framework Version 1.0 under Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” issued in February 2013<sup>3</sup>, and provided guidance for future Framework evolution.

Critical infrastructure<sup>4</sup> is defined in the U.S. Patriot Act of 2001<sup>5</sup> as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization’s size, threat exposure, or cybersecurity sophistication today.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation’s infrastructure. Members of each critical infrastructure sector perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). This reliance on technology, communication, and interconnectivity has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as technology and the data it produces and processes are increasingly used to deliver critical services and support business/mission decisions, the potential impacts of a cybersecurity incident on an

---

<sup>2</sup> See 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: <https://www.congress.gov/bill/113th-congress/senate-bill/1353/text>.

<sup>3</sup> Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. <https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf>

<sup>4</sup> The Department of Homeland Security (DHS) Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. <http://www.dhs.gov/critical-infrastructure-sectors>

<sup>5</sup> See 42 U.S.C. § 5195c(e)). The U.S. Patriot Act of 2001 (H.R.3162) became public law 107-56 on October 26, 2001 and may be found at: <https://www.congress.gov/bill/107th-congress/house-bill/3162>

organization, the health and safety of individuals, the environment, communities, and the broader economy and society should be considered.

To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of technology is required. Because each organization's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary.

Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization's approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

The Framework remains effective and supports technical innovation because it is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

- 1) Describe their current cybersecurity posture;
- 2) Describe their target state for cybersecurity;
- 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- 4) Assess progress toward the target state;
- 5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.



To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

While the Framework has been developed to improve cybersecurity risk management as it relates to critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size. The common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

## 1.1 Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities. These components are explained below.

- The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.
- *Framework Implementation Tiers* ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the

characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

- A *Framework Profile* (“Profile”) represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

## 1.2 Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO)

31000:2009<sup>6</sup>, ISO/International Electrotechnical Commission (IEC) 27005:2011<sup>7</sup>, NIST Special Publication (SP) 800-39<sup>8</sup>, and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline<sup>9</sup>.

### 1.3 Document Overview

The remainder of this document contains the following sections and appendices:

- [Section 2](#) describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- [Section 3](#) presents examples of how the Framework can be used.
- [Section 4](#) describes how to use the Framework for self-assessing and demonstrating cybersecurity through measurements.
- [Appendix A](#) presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- [Appendix B](#) contains a glossary of selected terms.
- [Appendix C](#) lists acronyms used in this document.

---

<sup>6</sup> International Organization for Standardization, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. <http://www.iso.org/iso/home/standards/iso31000.htm>

<sup>7</sup> International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. <https://www.iso.org/standard/56742.html>

<sup>8</sup> Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. <https://doi.org/10.6028/NIST.SP.800-39>

<sup>9</sup> U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, May 2012. [https://energy.gov/sites/prod/files/Cybersecurity\\_Risk\\_Management\\_Process\\_Guideline\\_-\\_Final\\_-\\_May\\_2012.pdf](https://energy.gov/sites/prod/files/Cybersecurity_Risk_Management_Process_Guideline_-_Final_-_May_2012.pdf)

## 2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

### 2.1 Framework Core

The *Framework Core* provides a set of activities to achieve specific cybersecurity *outcomes*, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in **Figure 1**:

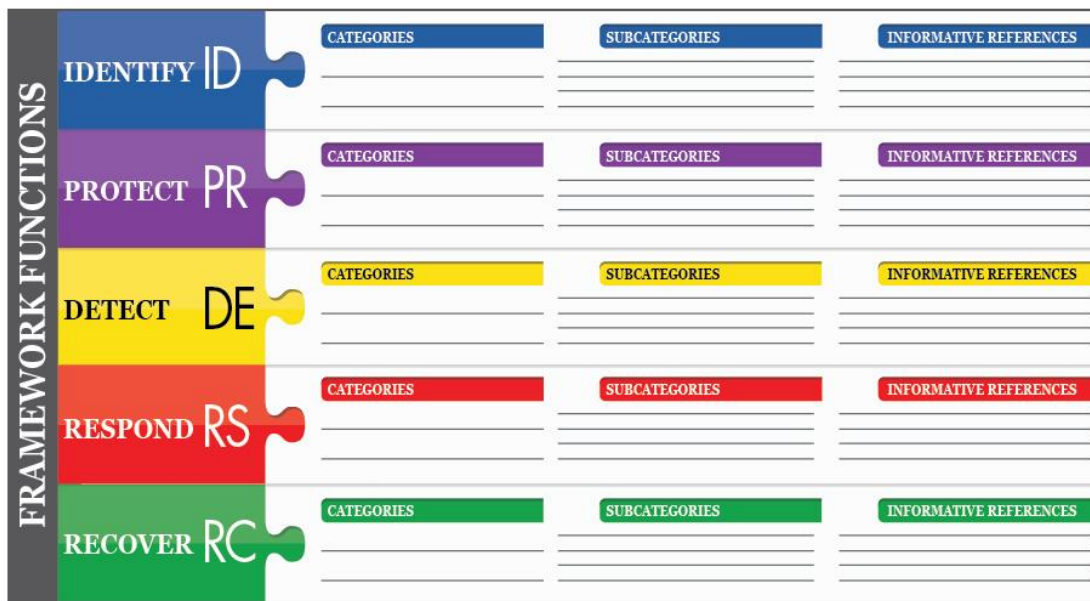


Figure 1: Framework Core Structure

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. See [Appendix A](#) for the complete Framework Core listing.

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

## 2.2 Framework Implementation Tiers

The Framework Implementation Tiers (“Tiers”) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization’s overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization’s management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization’s current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints.

Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.

Successful implementation of the Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination. Still, Tier selection and designation naturally affect Framework Profiles. The Tier recommendation by Business/Process Level managers, as approved by the Senior Executive Level, will help set the overall tone for how cybersecurity risk will be managed within the organization, and should influence prioritization within a Target Profile and assessments of progress in addressing gaps.

The Tier definitions are as follows:

### **Tier 1: Partial**

- *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- *External Participation* – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

### **Tier 2: Risk Informed**

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- *External Participation* – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.

### **Tier 3: Repeatable**

- *Risk Management Process* – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community’s broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

### **Tier 4: Adaptive**

- *Risk Management Process* – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
- *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.



- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

### **2.3 Framework Profile**

The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations. This Framework does not prescribe Profile templates, allowing for flexibility in implementation.

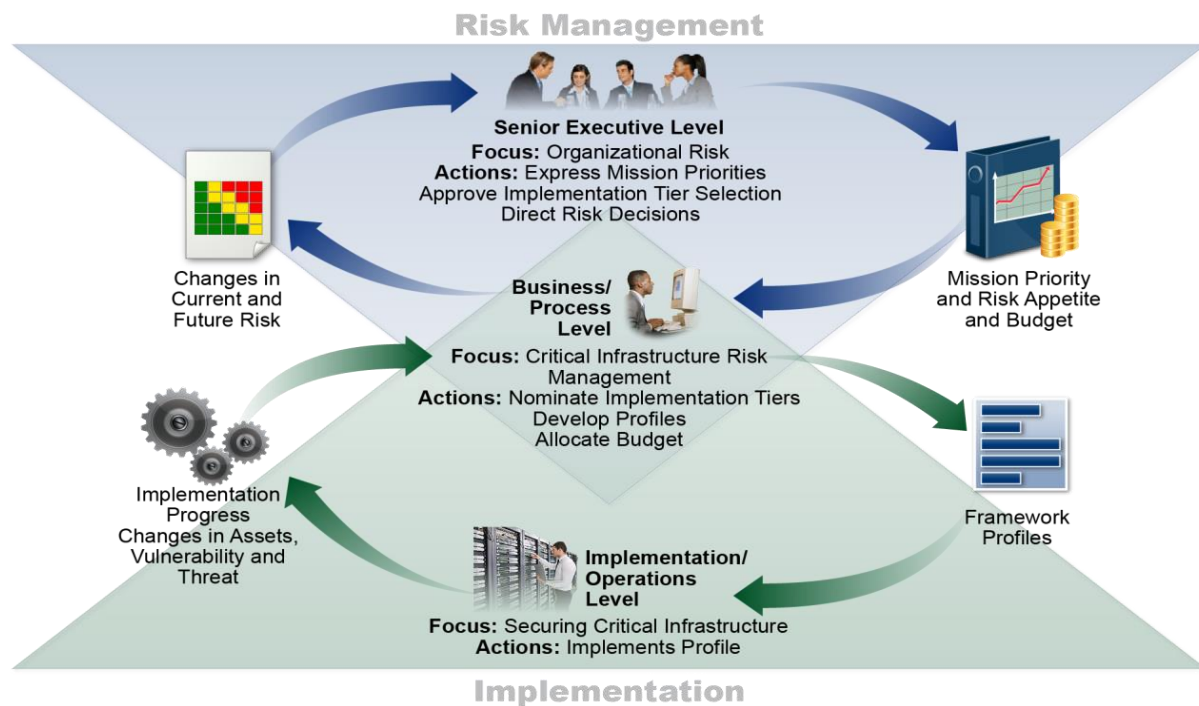
Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfill a given Category or Subcategory can contribute to the roadmap described above. Prioritizing the mitigation of gaps is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge the resources needed (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. Furthermore, the Framework is a risk-based approach where the applicability and fulfillment of a given Subcategory is subject to the Profile's scope.

## 2.4 Coordination of Framework Implementation

**Figure 2** describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization’s overall risk management process and to the implementation/operations level for awareness of business impact.



**Figure 2: Notional Information and Decision Flows within an Organization**

## 3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The Framework can be applied throughout the life cycle phases of plan, design, build/buy, deploy, operate, and decommission. The plan phase begins the cycle of any system and lays the groundwork for everything that follows. Overarching cybersecurity considerations should be declared and described as clearly as possible. The plan should recognize that those considerations and requirements are likely to evolve during the remainder of the life cycle. The design phase should account for cybersecurity requirements as a part of a larger multi-disciplinary systems engineering process.<sup>10</sup> A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as captured in a Framework Profile. The desired cybersecurity outcomes prioritized in a Target Profile should be incorporated when a) developing the system during the build phase and b) purchasing or outsourcing the system during the buy phase. That same Target Profile serves as a list of system cybersecurity features that should be assessed when deploying the system to verify all features are implemented. The cybersecurity outcomes determined by using the Framework then should serve as a basis for ongoing operation of the system. This includes occasional reassessment, capturing results in a Current Profile, to verify that cybersecurity requirements are still fulfilled. Typically, a complex web of dependencies (e.g., compensating and common controls) among systems means the outcomes documented in Target Profiles of related systems should be carefully considered as systems are decommissioned.

The following sections present different ways in which organizations can use the Framework.

### 3.1 Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization's current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired

---

<sup>10</sup> NIST Special Publication 800-160 Volume 1, *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, November 2016 (updated March 21, 2018), <https://doi.org/10.6028/NIST.SP.800-160v1>

outcomes, thus managing cybersecurity commensurate with the known risk. Alternatively, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including “How are we doing?” Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

### 3.2 Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

**Step 1: Prioritize and Scope.** The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

**Step 2: Orient.** Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

**Step 3: Create a Current Profile.** The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

**Step 4: Conduct a Risk Assessment.** This assessment could be guided by the organization’s overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

**Step 5: Create a Target Profile.** The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization’s desired cybersecurity outcomes. Organizations also may develop their own additional Categories and

Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

**Step 6: Determine, Analyze, and Prioritize Gaps.** The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

**Step 7: Implement Action Plan.** The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

### 3.3 Communicating Cybersecurity Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure products and services. Examples include:

- An organization may use a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
- An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.
- An organization can better manage cybersecurity risk among stakeholders by assessing their position in the critical infrastructure and the broader digital economy using Implementation Tiers.

Communication is especially important among stakeholders up and down supply chains. Supply chains are complex, globally distributed, and interconnected sets of resources and processes

between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, supply chain risk management (SCRM) is a critical organizational function.<sup>11</sup>

Cyber SCRM is the set of activities necessary to manage cybersecurity risk associated with external parties. More specifically, cyber SCRM addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization.

A primary objective of cyber SCRM is to identify, assess, and mitigate “products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain<sup>12</sup>.” Cyber SCRM activities may include:

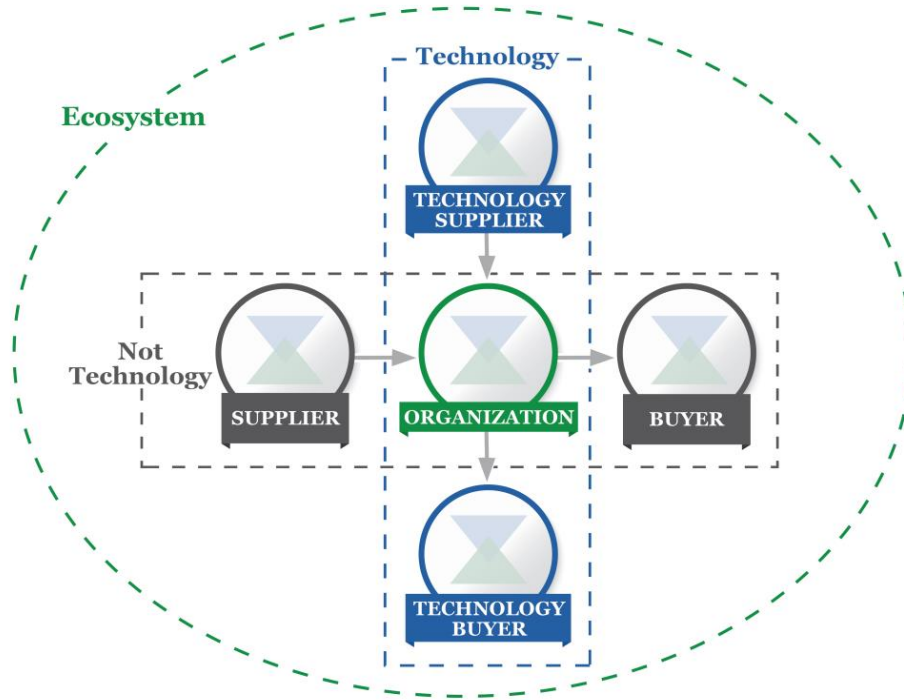
- Determining cybersecurity requirements for suppliers,
- Enacting cybersecurity requirements through formal agreement (e.g., contracts),
- Communicating to suppliers how those cybersecurity requirements will be verified and validated,
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies, and
- Governing and managing the above activities.

As depicted in Figure 3, cyber SCRM encompasses technology suppliers and buyers, as well as non-technology suppliers and buyers, where technology is minimally composed of information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). Figure 3 depicts an organization at a single point in time. However, through the normal course of business operations, most organizations will be both an upstream supplier and downstream buyer in relation to other organizations or end users.

---

<sup>11</sup> Communicating Cybersecurity Requirements (Section 3.3) and Buying Decisions (Section 3.4) address only two uses of the Framework for cyber SCRM and are not intended to address cyber SCRM comprehensively.

<sup>12</sup> NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, <https://doi.org/10.6028/NIST.SP.800-161>



**Figure 3: Cyber Supply Chain Relationships**

The parties described in Figure 3 comprise an organization’s cybersecurity ecosystem. These relationships highlight the crucial role of cyber SCRM in addressing cybersecurity risk in critical infrastructure and the broader digital economy. These relationships, the products and services they provide, and the risks they present should be identified and factored into the protective and detective capabilities of organizations, as well as their response and recovery protocols.

In the figure above, “Buyer” refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations. “Supplier” encompasses upstream product and service providers that are used for an organization’s internal purposes (e.g., IT infrastructure) or integrated into the products or services provided to the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

Whether considering individual Subcategories of the Core or the comprehensive considerations of a Profile, the Framework offers organizations and their partners a method to help ensure the new product or service meets critical security outcomes. By first selecting outcomes that are relevant to the context (e.g., transmission of Personally Identifiable Information (PII), mission critical service delivery, data verification services, product or service integrity) the organization then can evaluate partners against those criteria. For example, if a system is being purchased that will monitor Operational Technology (OT) for anomalous network communication, availability may be a particularly important cybersecurity objective to achieve and should drive a Technology Supplier evaluation against applicable Subcategories (e.g., ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

### 3.4 Buying Decisions

Since a Framework Target Profile is a prioritized list of organizational cybersecurity requirements, Target Profiles can be used to inform decisions about buying products and services. This transaction varies from Communicating Cybersecurity Requirements with Stakeholders (addressed in Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier. The objective should be to make the best buying decision among multiple suppliers, given a carefully determined list of cybersecurity requirements. Often, this means some degree of trade-off, comparing multiple products or services with known gaps to the Target Profile.

Once a product or service is purchased, the Profile also can be used to track and address residual cybersecurity risk. For example, if the service or product purchased did not meet all the objectives described in the Target Profile, the organization can address the residual risk through other management actions. The Profile also provides the organization a method for assessing if the product meets cybersecurity outcomes through periodic review and testing mechanisms.

### 3.5 Identifying Opportunities for New or Revised Informative References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

### 3.6 Methodology to Protect Privacy and Civil Liberties

This section describes a methodology to address individual privacy and civil liberties implications that may result from cybersecurity. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program engender privacy and civil liberties considerations. Technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and cybersecurity have a strong connection. An organization's cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed. Some examples include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; and cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including some types of incident detection or monitoring that may inhibit freedom of expression or association.

The government and its agents have a responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or its agents that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.



To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing.

As organizations assess the Framework Core in [Appendix A](#), the following processes and activities may be considered as a means to address the above-referenced privacy and civil liberties implications:

### **Governance of cybersecurity risk**

- An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program.
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained.
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.
- Process is in place to assess implementation of the above organizational measures and controls.

### **Approaches to identifying, authenticating, and authorizing individuals to access organizational assets and systems**

- Steps are taken to identify and address the privacy implications of identity management and access control measures to the extent that they involve collection, disclosure, or use of personal information.

### **Awareness and training measures**

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities.
- Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies.

### **Anomalous activity detection and system and assets monitoring**

- Process is in place to conduct a privacy review of an organization's anomalous activity detection and cybersecurity monitoring.

### **Response activities, including information sharing or other mitigation efforts**

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities.
- Process is in place to conduct a privacy review of an organization's cybersecurity mitigation efforts.

## 4.0 Self-Assessing Cybersecurity Risk with the Framework

The Cybersecurity Framework is designed to reduce risk by improving the management of cybersecurity risk to organizational objectives. Ideally, organizations using the Framework will be able to measure and assign values to their risk *along with* the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be.

Over time, self-assessment and measurement should improve decision making about investment priorities. For example, measuring – or at least robustly characterizing – aspects of an organization’s cybersecurity state and trends over time can enable that organization to understand and convey meaningful risk information to dependents, suppliers, buyers, and other parties. An organization can accomplish this internally or by seeking a third-party assessment. If done properly and with an appreciation of limitations, these measurements can provide a basis for strong trusted relationships, both inside and outside of an organization.

To examine the effectiveness of investments, an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes, and how those discrete cybersecurity outcomes are implemented and managed. While measurements of all those items is beyond the scope of the Framework, the cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities in the following ways:

- Making choices about how different portions of the cybersecurity operation should influence the selection of Target Implementation Tiers,
- Evaluating the organization’s approach to cybersecurity risk management by determining Current Implementation Tiers,
- Prioritizing cybersecurity outcomes by developing Target Profiles,
- Determining the degree to which specific cybersecurity steps achieve desired cybersecurity outcomes by assessing Current Profiles, and
- Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References.

The development of cybersecurity performance metrics is evolving. Organizations should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use, while avoiding reliance on artificial indicators of current state and progress in improving cybersecurity risk management. Judging cyber risk requires discipline and should be revisited periodically. Any time measurements are employed as part of the Framework process, organizations are encouraged to clearly identify and know why these measurements are important and how they will contribute to the overall management of cybersecurity risk. They also should be clear about the limitations of measurements that are used.

For example, tracking security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives. Verifying achievement of some organizational objectives requires analyzing the data only *after* that objective was to have been achieved. This type of lagging measure is more

April 16, 2018

Cybersecurity Framework

Version 1.1

absolute. However, it is often more valuable to predict whether a cybersecurity risk *may* occur, and the impact it *might* have, using a leading measure.

Organizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with a full appreciation of their usefulness and limitations.

## Appendix A: Framework Core

This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. The chosen presentation format for the Framework Core does not suggest a specific implementation order or imply a degree of importance of the Categories, Subcategories, and Informative References. The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation. Personal information is considered a component of data or assets referenced in the Categories when assessing security risks and protections.

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

For ease of use, each component of the Framework Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category are referenced numerically; the unique identifier for each Subcategory is included in Table 2.

Additional supporting material, including Informative References, relating to the Framework can be found on the NIST website at <http://www.nist.gov/cyberframework/>.

**Table 1: Function and Category Unique Identifiers**

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

April 16, 2018

Cybersecurity Framework

Version 1.1

Table 2: Framework Core

Function	Category	Subcategory	Informative References
<b>IDENTIFY</b> (ID)	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	<b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried	<b>CIS CSC 1</b> <b>COBIT 5</b> BAI09.01, BAI09.02 <b>ISA 62443-2-1:2009</b> 4.2.3.4 <b>ISA 62443-3-3:2013</b> SR 7.8 <b>ISO/IEC 27001:2013</b> A.8.1.1, A.8.1.2 <b>NIST SP 800-53 Rev. 4</b> CM-8, PM-5
		<b>ID.AM-2:</b> Software platforms and applications within the organization are inventoried	<b>CIS CSC 2</b> <b>COBIT 5</b> BAI09.01, BAI09.02, BAI09.05 <b>ISA 62443-2-1:2009</b> 4.2.3.4 <b>ISA 62443-3-3:2013</b> SR 7.8 <b>ISO/IEC 27001:2013</b> A.8.1.1, A.8.1.2, A.12.5.1 <b>NIST SP 800-53 Rev. 4</b> CM-8, PM-5
		<b>ID.AM-3:</b> Organizational communication and data flows are mapped	<b>CIS CSC 12</b> <b>COBIT 5</b> DSS05.02 <b>ISA 62443-2-1:2009</b> 4.2.3.4 <b>ISO/IEC 27001:2013</b> A.13.2.1, A.13.2.2 <b>NIST SP 800-53 Rev. 4</b> AC-4, CA-3, CA-9, PL-8
		<b>ID.AM-4:</b> External information systems are catalogued	<b>CIS CSC 12</b> <b>COBIT 5</b> APO02.02, APO10.04, DSS01.02 <b>ISO/IEC 27001:2013</b> A.11.2.6 <b>NIST SP 800-53 Rev. 4</b> AC-20, SA-9
		<b>ID.AM-5:</b> Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	<b>CIS CSC 13, 14</b> <b>COBIT 5</b> APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 <b>ISA 62443-2-1:2009</b> 4.2.3.6 <b>ISO/IEC 27001:2013</b> A.8.2.1 <b>NIST SP 800-53 Rev. 4</b> CP-2, RA-2, SA-14, SC-6
		<b>ID.AM-6:</b> Cybersecurity roles and responsibilities for the entire workforce and	<b>CIS CSC 17, 19</b> <b>COBIT 5</b> APO01.02, APO07.06, APO13.01, DSS06.03

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
<b>Business Environment (ID.BE):</b> The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.		third-party stakeholders (e.g., suppliers, customers, partners) are established	<b>ISA 62443-2-1:2009</b> 4.3.2.3.3 <b>ISO/IEC 27001:2013</b> A.6.1.1 <b>NIST SP 800-53 Rev. 4</b> CP-2, PS-7, PM-11
		<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated	<b>COBIT 5</b> APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 <b>ISO/IEC 27001:2013</b> A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 <b>NIST SP 800-53 Rev. 4</b> CP-2, SA-12
		<b>ID.BE-2:</b> The organization's place in critical infrastructure and its industry sector is identified and communicated	<b>COBIT 5</b> APO02.06, APO03.01 <b>ISO/IEC 27001:2013</b> Clause 4.1 <b>NIST SP 800-53 Rev. 4</b> PM-8
		<b>ID.BE-3:</b> Priorities for organizational mission, objectives, and activities are established and communicated	<b>COBIT 5</b> APO02.01, APO02.06, APO03.01 <b>ISA 62443-2-1:2009</b> 4.2.2.1, 4.2.3.6 <b>NIST SP 800-53 Rev. 4</b> PM-11, SA-14
		<b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established	<b>COBIT 5</b> APO10.01, BAI04.02, BAI09.02 <b>ISO/IEC 27001:2013</b> A.11.2.2, A.11.2.3, A.12.1.3 <b>NIST SP 800-53 Rev. 4</b> CP-8, PE-9, PE-11, PM-8, SA-14
		<b>ID.BE-5:</b> Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<b>COBIT 5</b> BAI03.02, DSS04.02 <b>ISO/IEC 27001:2013</b> A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 <b>NIST SP 800-53 Rev. 4</b> CP-2, CP-11, SA-13, SA-14
		<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the	<b>ID.GV-1:</b> Organizational cybersecurity policy is established and communicated

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
<b>Identify</b>	management of cybersecurity risk.	<b>ID.GV-2:</b> Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	<b>CIS CSC 19</b> <b>COBIT 5</b> APO01.02, APO10.03, APO13.02, DSS05.04 <b>ISA 62443-2-1:2009</b> 4.3.2.3.3 <b>ISO/IEC 27001:2013</b> A.6.1.1, A.7.2.1, A.15.1.1 <b>NIST SP 800-53 Rev. 4</b> PS-7, PM-1, PM-2
		<b>ID.GV-3:</b> Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	<b>CIS CSC 19</b> <b>COBIT 5</b> BAI02.01, MEA03.01, MEA03.04 <b>ISA 62443-2-1:2009</b> 4.4.3.7 <b>ISO/IEC 27001:2013</b> A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 <b>NIST SP 800-53 Rev. 4</b> -1 controls from all security control families
		<b>ID.GV-4:</b> Governance and risk management processes address cybersecurity risks	<b>COBIT 5</b> EDM03.02, APO12.02, APO12.05, DSS04.02 <b>ISA 62443-2-1:2009</b> 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 <b>ISO/IEC 27001:2013</b> Clause 6 <b>NIST SP 800-53 Rev. 4</b> SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	<b>ID.RA-1:</b> Asset vulnerabilities are identified and documented	<b>CIS CSC 4</b> <b>COBIT 5</b> APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 <b>ISA 62443-2-1:2009</b> 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 <b>ISO/IEC 27001:2013</b> A.12.6.1, A.18.2.3 <b>NIST SP 800-53 Rev. 4</b> CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		<b>ID.RA-2:</b> Cyber threat intelligence is received from information sharing forums and sources	<b>CIS CSC 4</b> <b>COBIT 5</b> BAI08.01 <b>ISA 62443-2-1:2009</b> 4.2.3, 4.2.3.9, 4.2.3.12 <b>ISO/IEC 27001:2013</b> A.6.1.4 <b>NIST SP 800-53 Rev. 4</b> SI-5, PM-15, PM-16



April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
		<b>ID.RA-3:</b> Threats, both internal and external, are identified and documented	<b>CIS CSC 4</b> <b>COBIT 5</b> APO12.01, APO12.02, APO12.03, APO12.04 <b>ISA 62443-2-1:2009</b> 4.2.3, 4.2.3.9, 4.2.3.12 <b>ISO/IEC 27001:2013</b> Clause 6.1.2 <b>NIST SP 800-53 Rev. 4</b> RA-3, SI-5, PM-12, PM-16
		<b>ID.RA-4:</b> Potential business impacts and likelihoods are identified	<b>CIS CSC 4</b> <b>COBIT 5</b> DSS04.02 <b>ISA 62443-2-1:2009</b> 4.2.3, 4.2.3.9, 4.2.3.12 <b>ISO/IEC 27001:2013</b> A.16.1.6, Clause 6.1.2 <b>NIST SP 800-53 Rev. 4</b> RA-2, RA-3, SA-14, PM-9, PM-11
		<b>ID.RA-5:</b> Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	<b>CIS CSC 4</b> <b>COBIT 5</b> APO12.02 <b>ISO/IEC 27001:2013</b> A.12.6.1 <b>NIST SP 800-53 Rev. 4</b> RA-2, RA-3, PM-16
		<b>ID.RA-6:</b> Risk responses are identified and prioritized	<b>CIS CSC 4</b> <b>COBIT 5</b> APO12.05, APO13.02 <b>ISO/IEC 27001:2013</b> Clause 6.1.3 <b>NIST SP 800-53 Rev. 4</b> PM-4, PM-9
	<b>Risk Management Strategy (ID.RM):</b> The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	<b>ID.RM-1:</b> Risk management processes are established, managed, and agreed to by organizational stakeholders	<b>CIS CSC 4</b> <b>COBIT 5</b> APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 <b>ISA 62443-2-1:2009</b> 4.3.4.2 <b>ISO/IEC 27001:2013</b> Clause 6.1.3, Clause 8.3, Clause 9.3 <b>NIST SP 800-53 Rev. 4</b> PM-9
	<b>ID.RM-2:</b> Organizational risk tolerance is determined and clearly expressed	<b>COBIT 5</b> APO12.06 <b>ISA 62443-2-1:2009</b> 4.3.2.6.5 <b>ISO/IEC 27001:2013</b> Clause 6.1.3, Clause 8.3 <b>NIST SP 800-53 Rev. 4</b> PM-9	

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
		<b>ID.RM-3:</b> The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	<b>COBIT 5</b> APO12.02 <b>ISO/IEC 27001:2013</b> Clause 6.1.3, Clause 8.3 <b>NIST SP 800-53 Rev. 4</b> SA-14, PM-8, PM-9, PM-11
	<b>Supply Chain Risk Management (ID.SC):</b> The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	<b>ID.SC-1:</b> Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	<b>CIS CSC 4</b> <b>COBIT 5</b> APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 <b>ISA 62443-2-1:2009</b> 4.3.4.2 <b>ISO/IEC 27001:2013</b> A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 <b>NIST SP 800-53 Rev. 4</b> SA-9, SA-12, PM-9
		<b>ID.SC-2:</b> Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	<b>COBIT 5</b> APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 <b>ISA 62443-2-1:2009</b> 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 <b>ISO/IEC 27001:2013</b> A.15.2.1, A.15.2.2 <b>NIST SP 800-53 Rev. 4</b> RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		<b>ID.SC-3:</b> Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.	<b>COBIT 5</b> APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 <b>ISA 62443-2-1:2009</b> 4.3.2.6.4, 4.3.2.6.7 <b>ISO/IEC 27001:2013</b> A.15.1.1, A.15.1.2, A.15.1.3 <b>NIST SP 800-53 Rev. 4</b> SA-9, SA-11, SA-12, PM-9
		<b>ID.SC-4:</b> Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	<b>COBIT 5</b> APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 <b>ISA 62443-2-1:2009</b> 4.3.2.6.7 <b>ISA 62443-3-3:2013</b> SR 6.1 <b>ISO/IEC 27001:2013</b> A.15.2.1, A.15.2.2

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
			<p><b>NIST SP 800-53 Rev. 4</b> AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12</p> <p><b>CIS CSC</b> 19, 20</p> <p><b>COBIT 5</b> DSS04.04</p> <p><b>ISA 62443-2-1:2009</b> 4.3.2.5.7, 4.3.4.5.11</p> <p><b>ISA 62443-3-3:2013</b> SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4</p> <p><b>ISO/IEC 27001:2013</b> A.17.1.3</p> <p><b>NIST SP 800-53 Rev. 4</b> CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9</p>
<p><b>PROTECT (PR)</b></p>	<p><b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p><b>PR.AC-1:</b> Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes</p>	<p><b>CIS CSC</b> 1, 5, 15, 16</p> <p><b>COBIT 5</b> DSS05.04, DSS06.03</p> <p><b>ISA 62443-2-1:2009</b> 4.3.3.5.1</p> <p><b>ISA 62443-3-3:2013</b> SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9</p> <p><b>ISO/IEC 27001:2013</b> A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3</p> <p><b>NIST SP 800-53 Rev. 4</b> AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11</p>
		<p><b>PR.AC-2:</b> Physical access to assets is managed and protected</p>	<p><b>COBIT 5</b> DSS01.04, DSS05.05</p> <p><b>ISA 62443-2-1:2009</b> 4.3.3.3.2, 4.3.3.3.8</p> <p><b>ISO/IEC 27001:2013</b> A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8</p> <p><b>NIST SP 800-53 Rev. 4</b> PE-2, PE-3, PE-4, PE-5, PE-6, PE-8</p>
		<p><b>PR.AC-3:</b> Remote access is managed</p>	<p><b>CIS CSC</b> 12</p> <p><b>COBIT 5</b> APO13.01, DSS01.04, DSS05.03</p> <p><b>ISA 62443-2-1:2009</b> 4.3.3.6.6</p> <p><b>ISA 62443-3-3:2013</b> SR 1.13, SR 2.6</p> <p><b>ISO/IEC 27001:2013</b> A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1</p>

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
			<b>NIST SP 800-53 Rev. 4</b> AC-1, AC-17, AC-19, AC-20, SC-15
		<b>PR.AC-4:</b> Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<b>CIS CSC</b> 3, 5, 12, 14, 15, 16, 18 <b>COBIT 5</b> DSS05.04 <b>ISA 62443-2-1:2009</b> 4.3.3.7.3 <b>ISA 62443-3-3:2013</b> SR 2.1 <b>ISO/IEC 27001:2013</b> A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 <b>NIST SP 800-53 Rev. 4</b> AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		<b>PR.AC-5:</b> Network integrity is protected (e.g., network segregation, network segmentation)	<b>CIS CSC</b> 9, 14, 15, 18 <b>COBIT 5</b> DSS01.05, DSS05.02 <b>ISA 62443-2-1:2009</b> 4.3.3.4 <b>ISA 62443-3-3:2013</b> SR 3.1, SR 3.8 <b>ISO/IEC 27001:2013</b> A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 <b>NIST SP 800-53 Rev. 4</b> AC-4, AC-10, SC-7
		<b>PR.AC-6:</b> Identities are proofed and bound to credentials and asserted in interactions	<b>CIS CSC</b> , 16 <b>COBIT 5</b> DSS05.04, DSS05.05, DSS05.07, DSS06.03 <b>ISA 62443-2-1:2009</b> 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 <b>ISA 62443-3-3:2013</b> SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 <b>ISO/IEC 27001:2013</b> , A.7.1.1, A.9.2.1 <b>NIST SP 800-53 Rev. 4</b> AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		<b>PR.AC-7:</b> Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	<b>CIS CSC</b> 1, 12, 15, 16 <b>COBIT 5</b> DSS05.04, DSS05.10, DSS06.10 <b>ISA 62443-2-1:2009</b> 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
Awareness and Training	(PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.		<p><b>ISA 62443-3-3:2013</b> SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10</p> <p><b>ISO/IEC 27001:2013</b> A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4</p> <p><b>NIST SP 800-53 Rev. 4</b> AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11</p>
		<b>PR.AT-1:</b> All users are informed and trained	<p><b>CIS CSC</b> 17, 18</p> <p><b>COBIT 5</b> APO07.03, BAI05.07</p> <p><b>ISA 62443-2-1:2009</b> 4.3.2.4.2</p> <p><b>ISO/IEC 27001:2013</b> A.7.2.2, A.12.2.1</p> <p><b>NIST SP 800-53 Rev. 4</b> AT-2, PM-13</p>
		<b>PR.AT-2:</b> Privileged users understand their roles and responsibilities	<p><b>CIS CSC</b> 5, 17, 18</p> <p><b>COBIT 5</b> APO07.02, DSS05.04, DSS06.03</p> <p><b>ISA 62443-2-1:2009</b> 4.3.2.4.2, 4.3.2.4.3</p> <p><b>ISO/IEC 27001:2013</b> A.6.1.1, A.7.2.2</p> <p><b>NIST SP 800-53 Rev. 4</b> AT-3, PM-13</p>
		<b>PR.AT-3:</b> Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	<p><b>CIS CSC</b> 17</p> <p><b>COBIT 5</b> APO07.03, APO07.06, APO10.04, APO10.05</p> <p><b>ISA 62443-2-1:2009</b> 4.3.2.4.2</p> <p><b>ISO/IEC 27001:2013</b> A.6.1.1, A.7.2.1, A.7.2.2</p> <p><b>NIST SP 800-53 Rev. 4</b> PS-7, SA-9, SA-16</p>
		<b>PR.AT-4:</b> Senior executives understand their roles and responsibilities	<p><b>CIS CSC</b> 17, 19</p> <p><b>COBIT 5</b> EDM01.01, APO01.02, APO07.03</p> <p><b>ISA 62443-2-1:2009</b> 4.3.2.4.2</p> <p><b>ISO/IEC 27001:2013</b> A.6.1.1, A.7.2.2</p> <p><b>NIST SP 800-53 Rev. 4</b> AT-3, PM-13</p>
		<b>PR.AT-5:</b> Physical and cybersecurity personnel understand their roles and responsibilities	<p><b>CIS CSC</b> 17</p> <p><b>COBIT 5</b> APO07.03</p> <p><b>ISA 62443-2-1:2009</b> 4.3.2.4.2</p> <p><b>ISO/IEC 27001:2013</b> A.6.1.1, A.7.2.2</p>

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
Data Security (PR.DS)	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.		<b>NIST SP 800-53 Rev. 4</b> AT-3, IR-2, PM-13
		<b>PR.DS-1:</b> Data-at-rest is protected	<b>CIS CSC</b> 13, 14 <b>COBIT 5</b> APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 <b>ISA 62443-3-3:2013</b> SR 3.4, SR 4.1 <b>ISO/IEC 27001:2013</b> A.8.2.3 <b>NIST SP 800-53 Rev. 4</b> MP-8, SC-12, SC-28
		<b>PR.DS-2:</b> Data-in-transit is protected	<b>CIS CSC</b> 13, 14 <b>COBIT 5</b> APO01.06, DSS05.02, DSS06.06 <b>ISA 62443-3-3:2013</b> SR 3.1, SR 3.8, SR 4.1, SR 4.2 <b>ISO/IEC 27001:2013</b> A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 <b>NIST SP 800-53 Rev. 4</b> SC-8, SC-11, SC-12
		<b>PR.DS-3:</b> Assets are formally managed throughout removal, transfers, and disposition	<b>CIS CSC</b> 1 <b>COBIT 5</b> BAI09.03 <b>ISA 62443-2-1:2009</b> 4.3.3.3.9, 4.3.4.4.1 <b>ISA 62443-3-3:2013</b> SR 4.2 <b>ISO/IEC 27001:2013</b> A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 <b>NIST SP 800-53 Rev. 4</b> CM-8, MP-6, PE-16
		<b>PR.DS-4:</b> Adequate capacity to ensure availability is maintained	<b>CIS CSC</b> 1, 2, 13 <b>COBIT 5</b> APO13.01, BAI04.04 <b>ISA 62443-3-3:2013</b> SR 7.1, SR 7.2 <b>ISO/IEC 27001:2013</b> A.12.1.3, A.17.2.1 <b>NIST SP 800-53 Rev. 4</b> AU-4, CP-2, SC-5
		<b>PR.DS-5:</b> Protections against data leaks are implemented	<b>CIS CSC</b> 13 <b>COBIT 5</b> APO01.06, DSS05.04, DSS05.07, DSS06.02 <b>ISA 62443-3-3:2013</b> SR 5.2 <b>ISO/IEC 27001:2013</b> A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
<b>Information Protection Processes and Procedures</b>			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 <b>NIST SP 800-53 Rev. 4</b> AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		<b>PR.DS-6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity	<b>CIS CSC</b> 2, 3 <b>COBIT 5</b> APO01.06, BAI06.01, DSS06.02 <b>ISA 62443-3-3:2013</b> SR 3.1, SR 3.3, SR 3.4, SR 3.8 <b>ISO/IEC 27001:2013</b> A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 <b>NIST SP 800-53 Rev. 4</b> SC-16, SI-7
		<b>PR.DS-7:</b> The development and testing environment(s) are separate from the production environment	<b>CIS CSC</b> 18, 20 <b>COBIT 5</b> BAI03.08, BAI07.04 <b>ISO/IEC 27001:2013</b> A.12.1.4 <b>NIST SP 800-53 Rev. 4</b> CM-2
		<b>PR.DS-8:</b> Integrity checking mechanisms are used to verify hardware integrity	<b>COBIT 5</b> BAI03.05 <b>ISA 62443-2-1:2009</b> 4.3.4.4.4 <b>ISO/IEC 27001:2013</b> A.11.2.4 <b>NIST SP 800-53 Rev. 4</b> SA-10, SI-7
	<b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	<b>PR.IP-1:</b> A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	<b>CIS CSC</b> 3, 9, 11 <b>COBIT 5</b> BAI10.01, BAI10.02, BAI10.03, BAI10.05 <b>ISA 62443-2-1:2009</b> 4.3.4.3.2, 4.3.4.3.3 <b>ISA 62443-3-3:2013</b> SR 7.6 <b>ISO/IEC 27001:2013</b> A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 <b>NIST SP 800-53 Rev. 4</b> CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		<b>PR.IP-2:</b> A System Development Life Cycle to manage systems is implemented	<b>CIS CSC</b> 18 <b>COBIT 5</b> APO13.01, BAI03.01, BAI03.02, BAI03.03 <b>ISA 62443-2-1:2009</b> 4.3.4.3.3

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
Information Security			<b>ISO/IEC 27001:2013</b> A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 <b>NIST SP 800-53 Rev. 4</b> PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		<b>PR.IP-3:</b> Configuration change control processes are in place	<b>CIS CSC</b> 3, 11 <b>COBIT 5</b> BAI01.06, BAI06.01 <b>ISA 62443-2-1:2009</b> 4.3.4.3.2, 4.3.4.3.3 <b>ISA 62443-3-3:2013</b> SR 7.6 <b>ISO/IEC 27001:2013</b> A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 <b>NIST SP 800-53 Rev. 4</b> CM-3, CM-4, SA-10
		<b>PR.IP-4:</b> Backups of information are conducted, maintained, and tested	<b>CIS CSC</b> 10 <b>COBIT 5</b> APO13.01, DSS01.01, DSS04.07 <b>ISA 62443-2-1:2009</b> 4.3.4.3.9 <b>ISA 62443-3-3:2013</b> SR 7.3, SR 7.4 <b>ISO/IEC 27001:2013</b> A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 <b>NIST SP 800-53 Rev. 4</b> CP-4, CP-6, CP-9
		<b>PR.IP-5:</b> Policy and regulations regarding the physical operating environment for organizational assets are met	<b>COBIT 5</b> DSS01.04, DSS05.05 <b>ISA 62443-2-1:2009</b> 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 <b>ISO/IEC 27001:2013</b> A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 <b>NIST SP 800-53 Rev. 4</b> PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		<b>PR.IP-6:</b> Data is destroyed according to policy	<b>COBIT 5</b> BAI09.03, DSS05.06 <b>ISA 62443-2-1:2009</b> 4.3.4.4.4 <b>ISA 62443-3-3:2013</b> SR 4.2 <b>ISO/IEC 27001:2013</b> A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 <b>NIST SP 800-53 Rev. 4</b> MP-6



April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
		<b>PR.IP-7:</b> Protection processes are improved	<b>COBIT 5</b> APO11.06, APO12.06, DSS04.05 <b>ISA 62443-2-1:2009</b> 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 <b>ISO/IEC 27001:2013</b> A.16.1.6, Clause 9, Clause 10 <b>NIST SP 800-53 Rev. 4</b> CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		<b>PR.IP-8:</b> Effectiveness of protection technologies is shared	<b>COBIT 5</b> BAI08.04, DSS03.04 <b>ISO/IEC 27001:2013</b> A.16.1.6 <b>NIST SP 800-53 Rev. 4</b> AC-21, CA-7, SI-4
		<b>PR.IP-9:</b> Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	<b>CIS CSC</b> 19 <b>COBIT 5</b> APO12.06, DSS04.03 <b>ISA 62443-2-1:2009</b> 4.3.2.5.3, 4.3.4.5.1 <b>ISO/IEC 27001:2013</b> A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 <b>NIST SP 800-53 Rev. 4</b> CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		<b>PR.IP-10:</b> Response and recovery plans are tested	<b>CIS CSC</b> 19, 20 <b>COBIT 5</b> DSS04.04 <b>ISA 62443-2-1:2009</b> 4.3.2.5.7, 4.3.4.5.11 <b>ISA 62443-3-3:2013</b> SR 3.3 <b>ISO/IEC 27001:2013</b> A.17.1.3 <b>NIST SP 800-53 Rev. 4</b> CP-4, IR-3, PM-14
		<b>PR.IP-11:</b> Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	<b>CIS CSC</b> 5, 16 <b>COBIT 5</b> APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 <b>ISA 62443-2-1:2009</b> 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 <b>ISO/IEC 27001:2013</b> A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 <b>NIST SP 800-53 Rev. 4</b> PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.		<b>PR.IP-12:</b> A vulnerability management plan is developed and implemented	<b>CIS CSC 4, 18, 20</b> <b>COBIT 5 BAI03.10, DSS05.01, DSS05.02</b> <b>ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3</b> <b>NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2</b>
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	<b>PR.MA-1:</b> Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	<b>COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05</b> <b>ISA 62443-2-1:2009 4.3.3.3.7</b> <b>ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6</b> <b>NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6</b>
		<b>PR.MA-2:</b> Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	<b>CIS CSC 3, 5</b> <b>COBIT 5 DSS05.04</b> <b>ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8</b> <b>ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1</b> <b>NIST SP 800-53 Rev. 4 MA-4</b>
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	<b>PR.PT-1:</b> Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<b>CIS CSC 1, 3, 5, 6, 14, 15, 16</b> <b>COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01</b> <b>ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4</b> <b>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12</b> <b>ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1</b> <b>NIST SP 800-53 Rev. 4 AU Family</b>
		<b>PR.PT-2:</b> Removable media is protected and its use restricted according to policy	<b>CIS CSC 8, 13</b> <b>COBIT 5 APO13.01, DSS05.02, DSS05.06</b> <b>ISA 62443-3-3:2013 SR 2.3</b> <b>ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9</b>

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
			<p><b>NIST SP 800-53 Rev. 4</b> MP-2, MP-3, MP-4, MP-5, MP-7, MP-8</p>
		<p><b>PR.PT-3:</b> The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</p>	<p><b>CIS CSC</b> 3, 11, 14  <b>COBIT 5</b> DSS05.02, DSS05.05, DSS06.06  <b>ISA 62443-2-1:2009</b> 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4  <b>ISA 62443-3-3:2013</b> SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7  <b>ISO/IEC 27001:2013</b> A.9.1.2  <b>NIST SP 800-53 Rev. 4</b> AC-3, CM-7</p>
		<p><b>PR.PT-4:</b> Communications and control networks are protected</p>	<p><b>CIS CSC</b> 8, 12, 15  <b>COBIT 5</b> DSS05.02, APO13.01  <b>ISA 62443-3-3:2013</b> SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6  <b>ISO/IEC 27001:2013</b> A.13.1.1, A.13.2.1, A.14.1.3  <b>NIST SP 800-53 Rev. 4</b> AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43</p>
		<p><b>PR.PT-5:</b> Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations</p>	<p><b>COBIT 5</b> BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05  <b>ISA 62443-2-1:2009</b> 4.3.2.5.2  <b>ISA 62443-3-3:2013</b> SR 7.1, SR 7.2  <b>ISO/IEC 27001:2013</b> A.17.1.2, A.17.2.1  <b>NIST SP 800-53 Rev. 4</b> CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6</p>
<p><b>DETECT (DE)</b></p>	<p><b>Anomalies and Events (DE.AE):</b>                      Anomalous activity is detected</p>	<p><b>DE.AE-1:</b> A baseline of network operations and expected data flows for</p>	<p><b>CIS CSC</b> 1, 4, 6, 12, 13, 15, 16  <b>COBIT 5</b> DSS03.01  <b>ISA 62443-2-1:2009</b> 4.4.3.3</p>

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
	and the potential impact of events is understood.	users and systems is established and managed	<b>ISO/IEC 27001:2013</b> A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 <b>NIST SP 800-53 Rev. 4</b> AC-4, CA-3, CM-2, SI-4
		<b>DE.AE-2:</b> Detected events are analyzed to understand attack targets and methods	<b>CIS CSC</b> 3, 6, 13, 15 <b>COBIT 5</b> DSS05.07 <b>ISA 62443-2-1:2009</b> 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 <b>ISA 62443-3-3:2013</b> SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 <b>ISO/IEC 27001:2013</b> A.12.4.1, A.16.1.1, A.16.1.4 <b>NIST SP 800-53 Rev. 4</b> AU-6, CA-7, IR-4, SI-4
		<b>DE.AE-3:</b> Event data are collected and correlated from multiple sources and sensors	<b>CIS CSC</b> 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 <b>COBIT 5</b> BAI08.02 <b>ISA 62443-3-3:2013</b> SR 6.1 <b>ISO/IEC 27001:2013</b> A.12.4.1, A.16.1.7 <b>NIST SP 800-53 Rev. 4</b> AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		<b>DE.AE-4:</b> Impact of events is determined	<b>CIS CSC</b> 4, 6 <b>COBIT 5</b> APO12.06, DSS03.01 <b>ISO/IEC 27001:2013</b> A.16.1.4 <b>NIST SP 800-53 Rev. 4</b> CP-2, IR-4, RA-3, SI-4
		<b>DE.AE-5:</b> Incident alert thresholds are established	<b>CIS CSC</b> 6, 19 <b>COBIT 5</b> APO12.06, DSS03.01 <b>ISA 62443-2-1:2009</b> 4.2.3.10 <b>ISO/IEC 27001:2013</b> A.16.1.4 <b>NIST SP 800-53 Rev. 4</b> IR-4, IR-5, IR-8
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify	<b>DE.CM-1:</b> The network is monitored to detect potential cybersecurity events	<b>CIS CSC</b> 1, 7, 8, 12, 13, 15, 16 <b>COBIT 5</b> DSS01.03, DSS03.05, DSS05.07 <b>ISA 62443-3-3:2013</b> SR 6.2 <b>NIST SP 800-53 Rev. 4</b> AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
	the effectiveness of protective measures.	<b>DE.CM-2:</b> The physical environment is monitored to detect potential cybersecurity events	<b>COBIT 5</b> DSS01.04, DSS01.05 <b>ISA 62443-2-1:2009</b> 4.3.3.3.8 <b>ISO/IEC 27001:2013</b> A.11.1.1, A.11.1.2 <b>NIST SP 800-53 Rev. 4</b> CA-7, PE-3, PE-6, PE-20
		<b>DE.CM-3:</b> Personnel activity is monitored to detect potential cybersecurity events	<b>CIS CSC</b> 5, 7, 14, 16 <b>COBIT 5</b> DSS05.07 <b>ISA 62443-3-3:2013</b> SR 6.2 <b>ISO/IEC 27001:2013</b> A.12.4.1, A.12.4.3 <b>NIST SP 800-53 Rev. 4</b> AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		<b>DE.CM-4:</b> Malicious code is detected	<b>CIS CSC</b> 4, 7, 8, 12 <b>COBIT 5</b> DSS05.01 <b>ISA 62443-2-1:2009</b> 4.3.4.3.8 <b>ISA 62443-3-3:2013</b> SR 3.2 <b>ISO/IEC 27001:2013</b> A.12.2.1 <b>NIST SP 800-53 Rev. 4</b> SI-3, SI-8
		<b>DE.CM-5:</b> Unauthorized mobile code is detected	<b>CIS CSC</b> 7, 8 <b>COBIT 5</b> DSS05.01 <b>ISA 62443-3-3:2013</b> SR 2.4 <b>ISO/IEC 27001:2013</b> A.12.5.1, A.12.6.2 <b>NIST SP 800-53 Rev. 4</b> SC-18, SI-4, SC-44
		<b>DE.CM-6:</b> External service provider activity is monitored to detect potential cybersecurity events	<b>COBIT 5</b> APO07.06, APO10.05 <b>ISO/IEC 27001:2013</b> A.14.2.7, A.15.2.1 <b>NIST SP 800-53 Rev. 4</b> CA-7, PS-7, SA-4, SA-9, SI-4
		<b>DE.CM-7:</b> Monitoring for unauthorized personnel, connections, devices, and software is performed	<b>CIS CSC</b> 1, 2, 3, 5, 9, 12, 13, 15, 16 <b>COBIT 5</b> DSS05.02, DSS05.05 <b>ISO/IEC 27001:2013</b> A.12.4.1, A.14.2.7, A.15.2.1 <b>NIST SP 800-53 Rev. 4</b> AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		<b>DE.CM-8:</b> Vulnerability scans are performed	<b>CIS CSC</b> 4, 20

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
<p><b>Detection Processes (DE.DP):</b>                      Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>			<p><b>COBIT 5</b> BAI03.10, DSS05.01  <b>ISA 62443-2-1:2009</b> 4.2.3.1, 4.2.3.7  <b>ISO/IEC 27001:2013</b> A.12.6.1  <b>NIST SP 800-53 Rev. 4</b> RA-5</p>
		<p><b>DE.DP-1:</b> Roles and responsibilities for detection are well defined to ensure accountability</p>	<p><b>CIS CSC</b> 19  <b>COBIT 5</b> APO01.02, DSS05.01, DSS06.03  <b>ISA 62443-2-1:2009</b> 4.4.3.1  <b>ISO/IEC 27001:2013</b> A.6.1.1, A.7.2.2  <b>NIST SP 800-53 Rev. 4</b> CA-2, CA-7, PM-14</p>
		<p><b>DE.DP-2:</b> Detection activities comply with all applicable requirements</p>	<p><b>COBIT 5</b> DSS06.01, MEA03.03, MEA03.04  <b>ISA 62443-2-1:2009</b> 4.4.3.2  <b>ISO/IEC 27001:2013</b> A.18.1.4, A.18.2.2, A.18.2.3  <b>NIST SP 800-53 Rev. 4</b> AC-25, CA-2, CA-7, SA-18, SI-4, PM-14</p>
		<p><b>DE.DP-3:</b> Detection processes are tested</p>	<p><b>COBIT 5</b> APO13.02, DSS05.02  <b>ISA 62443-2-1:2009</b> 4.4.3.2  <b>ISA 62443-3-3:2013</b> SR 3.3  <b>ISO/IEC 27001:2013</b> A.14.2.8  <b>NIST SP 800-53 Rev. 4</b> CA-2, CA-7, PE-3, SI-3, SI-4, PM-14</p>
		<p><b>DE.DP-4:</b> Event detection information is communicated</p>	<p><b>CIS CSC</b> 19  <b>COBIT 5</b> APO08.04, APO12.06, DSS02.05  <b>ISA 62443-2-1:2009</b> 4.3.4.5.9  <b>ISA 62443-3-3:2013</b> SR 6.1  <b>ISO/IEC 27001:2013</b> A.16.1.2, A.16.1.3  <b>NIST SP 800-53 Rev. 4</b> AU-6, CA-2, CA-7, RA-5, SI-4</p>
		<p><b>DE.DP-5:</b> Detection processes are continuously improved</p>	<p><b>COBIT 5</b> APO11.06, APO12.06, DSS04.05  <b>ISA 62443-2-1:2009</b> 4.4.3.4  <b>ISO/IEC 27001:2013</b> A.16.1.6  <b>NIST SP 800-53 Rev. 4</b>, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14</p>

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
<b>RESPOND (RS)</b>	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	<b>RS.RP-1:</b> Response plan is executed during or after an incident	<b>CIS CSC 19</b> <b>COBIT 5 APO12.06, BAI01.10</b> <b>ISA 62443-2-1:2009 4.3.4.5.1</b> <b>ISO/IEC 27001:2013 A.16.1.5</b> <b>NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8</b>
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	<b>RS.CO-1:</b> Personnel know their roles and order of operations when a response is needed	<b>CIS CSC 19</b> <b>COBIT 5 EDM03.02, APO01.02, APO12.03</b> <b>ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4</b> <b>ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1</b> <b>NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8</b>
		<b>RS.CO-2:</b> Incidents are reported consistent with established criteria	<b>CIS CSC 19</b> <b>COBIT 5 DSS01.03</b> <b>ISA 62443-2-1:2009 4.3.4.5.5</b> <b>ISO/IEC 27001:2013 A.6.1.3, A.16.1.2</b> <b>NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8</b>
		<b>RS.CO-3:</b> Information is shared consistent with response plans	<b>CIS CSC 19</b> <b>COBIT 5 DSS03.04</b> <b>ISA 62443-2-1:2009 4.3.4.5.2</b> <b>ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2</b> <b>NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4</b>
		<b>RS.CO-4:</b> Coordination with stakeholders occurs consistent with response plans	<b>CIS CSC 19</b> <b>COBIT 5 DSS03.04</b> <b>ISA 62443-2-1:2009 4.3.4.5.5</b> <b>ISO/IEC 27001:2013 Clause 7.4</b> <b>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</b>
		<b>RS.CO-5:</b> Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	<b>CIS CSC 19</b> <b>COBIT 5 BAI08.04</b> <b>ISO/IEC 27001:2013 A.6.1.4</b> <b>NIST SP 800-53 Rev. 4 SI-5, PM-15</b>

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
<b>Analysis</b>	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	<b>RS.AN-1:</b> Notifications from detection systems are investigated	<b>CIS CSC 4, 6, 8, 19</b> <b>COBIT 5 DSS02.04, DSS02.07</b> <b>ISA 62443-2-1:2009</b> 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 <b>ISA 62443-3-3:2013</b> SR 6.1 <b>ISO/IEC 27001:2013</b> A.12.4.1, A.12.4.3, A.16.1.5 <b>NIST SP 800-53 Rev. 4</b> AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		<b>RS.AN-2:</b> The impact of the incident is understood	<b>COBIT 5 DSS02.02</b> <b>ISA 62443-2-1:2009</b> 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 <b>ISO/IEC 27001:2013</b> A.16.1.4, A.16.1.6 <b>NIST SP 800-53 Rev. 4</b> CP-2, IR-4
		<b>RS.AN-3:</b> Forensics are performed	<b>COBIT 5 APO12.06, DSS03.02, DSS05.07</b> <b>ISA 62443-3-3:2013</b> SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 <b>ISO/IEC 27001:2013</b> A.16.1.7 <b>NIST SP 800-53 Rev. 4</b> AU-7, IR-4
		<b>RS.AN-4:</b> Incidents are categorized consistent with response plans	<b>CIS CSC 19</b> <b>COBIT 5 DSS02.02</b> <b>ISA 62443-2-1:2009</b> 4.3.4.5.6 <b>ISO/IEC 27001:2013</b> A.16.1.4 <b>NIST SP 800-53 Rev. 4</b> CP-2, IR-4, IR-5, IR-8
		<b>RS.AN-5:</b> Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	<b>CIS CSC 4, 19</b> <b>COBIT 5 EDM03.02, DSS05.07</b> <b>NIST SP 800-53 Rev. 4</b> SI-5, PM-15
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	<b>RS.MI-1:</b> Incidents are contained	<b>CIS CSC 19</b> <b>COBIT 5 APO12.06</b> <b>ISA 62443-2-1:2009</b> 4.3.4.5.6 <b>ISA 62443-3-3:2013</b> SR 5.1, SR 5.2, SR 5.4 <b>ISO/IEC 27001:2013</b> A.12.2.1, A.16.1.5



April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
			<b>NIST SP 800-53 Rev. 4 IR-4</b>
		<b>RS.MI-2:</b> Incidents are mitigated	<b>CIS CSC 4, 19</b> <b>COBIT 5 APO12.06</b> <b>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10</b> <b>ISO/IEC 27001:2013 A.12.2.1, A.16.1.5</b> <b>NIST SP 800-53 Rev. 4 IR-4</b>
		<b>RS.MI-3:</b> Newly identified vulnerabilities are mitigated or documented as accepted risks	<b>CIS CSC 4</b> <b>COBIT 5 APO12.06</b> <b>ISO/IEC 27001:2013 A.12.6.1</b> <b>NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5</b>
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	<b>RS.IM-1:</b> Response plans incorporate lessons learned	<b>COBIT 5 BAI01.13</b> <b>ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4</b> <b>ISO/IEC 27001:2013 A.16.1.6, Clause 10</b> <b>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</b>
		<b>RS.IM-2:</b> Response strategies are updated	<b>COBIT 5 BAI01.13, DSS04.08</b> <b>ISO/IEC 27001:2013 A.16.1.6, Clause 10</b> <b>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</b>
	<b>RECOVER (RC)</b>	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	<b>RC.RP-1:</b> Recovery plan is executed during or after a cybersecurity incident
<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.			<b>RC.IM-1:</b> Recovery plans incorporate lessons learned
		<b>RC.IM-2:</b> Recovery strategies are updated	<b>COBIT 5 APO12.06, BAI07.08</b> <b>ISO/IEC 27001:2013 A.16.1.6, Clause 10</b> <b>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</b>

April 16, 2018

Cybersecurity Framework

Version 1.1

Function	Category	Subcategory	Informative References
	<b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	<b>RC.CO-1:</b> Public relations are managed	<b>COBIT 5 EDM03.02</b> <b>ISO/IEC 27001:2013 A.6.1.4, Clause 7.4</b>
		<b>RC.CO-2:</b> Reputation is repaired after an incident	<b>COBIT 5 MEA03.02</b> <b>ISO/IEC 27001:2013 Clause 7.4</b>
		<b>RC.CO-3:</b> Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	<b>COBIT 5 APO12.06</b> <b>ISO/IEC 27001:2013 Clause 7.4</b> <b>NIST SP 800-53 Rev. 4 CP-2, IR-4</b>

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): <http://www.isaca.org/COBIT/Pages/default.aspx>
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): <https://www.cisecurity.org>
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: <https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731>
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: <https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785>
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: <https://www.iso.org/standard/54534.html>
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). <https://doi.org/10.6028/NIST.SP.800-53r4>. Informative References are only mapped to the control level, though any control enhancement might be found useful in achieving a subcategory outcome.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.

Informative References are not exhaustive, in that not every element (e.g., control, requirement) of a given Informative Reference is mapped to Framework Core Subcategories.

## Appendix B: Glossary

This appendix defines selected terms used in the publication.

**Table 3: Framework Glossary**

<b>Buyer</b>	The people or organizations that consume a given product or service.
<b>Category</b>	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”
<b>Critical Infrastructure</b>	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
<b>Cybersecurity</b>	The process of protecting information by preventing, detecting, and responding to attacks.
<b>Cybersecurity Event</b>	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
<b>Cybersecurity Incident</b>	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
<b>Detect (function)</b>	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
<b>Framework</b>	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”
<b>Framework Core</b>	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
<b>Framework Implementation Tier</b>	A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.

<b>Framework Profile</b>	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
<b>Function</b>	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
<b>Identify (function)</b>	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
<b>Informative Reference</b>	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the “Data-in-transit is protected” Subcategory of the “Data Security” Category in the “Protect” function.
<b>Mobile Code</b>	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
<b>Protect (function)</b>	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
<b>Privileged User</b>	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
<b>Recover (function)</b>	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
<b>Respond (function)</b>	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
<b>Risk</b>	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
<b>Risk Management</b>	The process of identifying, assessing, and responding to risk.
<b>Subcategory</b>	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

April 16, 2018

Cybersecurity Framework

Version 1.1

<b>Supplier</b>	Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers.
<b>Taxonomy</b>	A scheme of classification.

## Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

<b>ANSI</b>	American National Standards Institute
<b>CEA</b>	Cybersecurity Enhancement Act of 2014
<b>CIS</b>	Center for Internet Security
<b>COBIT</b>	Control Objectives for Information and Related Technology
<b>CPS</b>	Cyber-Physical Systems
<b>CSC</b>	Critical Security Control
<b>DHS</b>	Department of Homeland Security
<b>EO</b>	Executive Order
<b>ICS</b>	Industrial Control Systems
<b>IEC</b>	International Electrotechnical Commission
<b>IoT</b>	Internet of Things
<b>IR</b>	Interagency Report
<b>ISA</b>	International Society of Automation
<b>ISAC</b>	Information Sharing and Analysis Center
<b>ISAO</b>	Information Sharing and Analysis Organization
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	Information Technology
<b>NIST</b>	National Institute of Standards and Technology
<b>OT</b>	Operational Technology
<b>PII</b>	Personally Identifiable Information
<b>RFI</b>	Request for Information
<b>RMP</b>	Risk Management Process
<b>SCRM</b>	Supply Chain Risk Management
<b>SP</b>	Special Publication

**NIST Special Publication 800-171**  
**Revision 2**

---

# **Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**

---

**RON ROSS**  
**VICTORIA PILLITTERI**  
**KELLEY DEMPSEY**  
**MARK RIDDLE**  
**GARY GUISSANIE**

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-171r2>

**NIST Special Publication 800-171**  
**Revision 2**

# Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

**RON ROSS**  
**VICTORIA PILLITTERI**  
**KELLEY DEMPSEY**

*Computer Security Division  
National Institute of Standards and Technology*

**MARK RIDDLE**  
*Information Security Oversight Office  
National Archives and Records Administration*

**GARY GUISSANIE**  
*Institute for Defense Analyses*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-171r2>

**February 2020**

INCLUDES UPDATES AS OF 01-28-2021; SEE PAGE X



U.S. Department of Commerce  
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology  
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*



## Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. Such information security standards and guidelines shall not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, OMB Director, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis, and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-171, Revision 2  
Natl. Inst. Stand. Technol. Spec. Publ. 800-171, Revision 2, **113 pages** (February 2020)

CODEN: NSPUE2

This publication is available free of charge from:

<https://doi.org/10.6028/NIST.SP.800-171r2>

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Many NIST publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

### Comments on this publication may be submitted to:

National Institute of Standards and Technology  
Attn: Computer Security Division, Information Technology Laboratory  
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930  
Email: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)

All comments are subject to release under the Freedom of Information Act (FOIA) [\[FOIA96\]](#)

## Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and privacy and its collaborative activities with industry, government, and academic organizations.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

## **Abstract**

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

## **Keywords**

Basic Security Requirement; Contractor Systems; Controlled Unclassified Information; CUI Registry; Derived Security Requirement; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; Nonfederal Organizations; Nonfederal Systems; Security Assessment; Security Control; Security Requirement.

## **Trademark Information**

All names are trademarks or registered trademarks of their respective owners.

## Acknowledgements

The authors wish to recognize the scientists, engineers, and research staff from the Computer Security Division and Applied Cybersecurity Division for their exceptional contributions in helping to improve the content of the publication. A special note of thanks to Pat O'Reilly, Jim Foti, Jeff Brewer and the NIST web team for their outstanding administrative support. Finally, the authors also gratefully acknowledge the contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

### **HISTORICAL CONTRIBUTIONS TO NIST SPECIAL PUBLICATION 800-171**

The authors acknowledge the many individuals who contributed to previous versions of Special Publication 800-171 since its inception in June 2015. They include Carol Bales, Matthew Barrett, Jon Boyens, Devin Casey, Christian Enloe, Peggy Himes, Robert Glenn, Elizabeth Lennon, Vicki Michetti, Dorian Pappas, Karen Quigg, Mary Thomas, Matthew Scholl, Murugiah Souppaya, Patricia Toth, and Patrick Viscuso.

## Patent Disclosure Notice

*NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.*

*As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.*

*No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.*

### CAUTIONARY NOTE

The Federal Information Security Modernization Act [FISMA] of 2014 requires federal agencies to identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency; or information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. This publication focuses on protecting the *confidentiality* of Controlled Unclassified Information (CUI) in *nonfederal* systems and organizations, and recommends specific security requirements to achieve that objective. It does not change the requirements set forth in [FISMA], nor does it alter the responsibility of federal agencies to comply with the full provisions of the statute, the policies established by OMB, and the supporting security standards and guidelines developed by NIST.

The requirements recommended for use in this publication are derived from [FIPS 200] and the moderate security control baseline in [SP 800-53] and are based on the CUI regulation [32 CFR 2002]. The requirements and controls have been determined over time to provide the necessary protection for federal information and systems that are covered under [FISMA]. The tailoring criteria applied to the [FIPS 200] requirements and [SP 800-53] controls are **not** an endorsement for the elimination of those requirements and controls; rather, the tailoring criteria focuses on the protection of CUI from unauthorized disclosure in nonfederal systems and organizations. Moreover, since the security requirements are derivative from the NIST publications listed above, organizations should **not** assume that satisfying those particular requirements will automatically satisfy the security requirements and controls in [FIPS 200] and [SP 800-53].

In addition to the security objective of *confidentiality*, the objectives of *integrity* and *availability* remain a high priority for organizations that are concerned with establishing and maintaining a comprehensive information security program. While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the system level support both security objectives. Therefore, the basic and derived security requirements in this publication provide protection from unauthorized disclosure and unauthorized modification of CUI. Organizations that are interested in or are required to comply with the recommendations in this publication are strongly advised to review the complete listing of controls in the moderate baseline in [Appendix E](#) to ensure that their individual security plans and control deployments provide the necessary and sufficient protection to address the cyber and kinetic threats to organizational missions and business operations.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

### **CUI SECURITY REQUIREMENTS**

The recommended security requirements contained in this publication are only *applicable* to a nonfederal system or organization when *mandated* by a federal agency in a contract, grant, or other agreement. The security requirements apply to the components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

### FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Organizations that have implemented or plan to implement the NIST *Framework for Improving Critical Infrastructure Cybersecurity* [NIST CSF] can find in [Appendix D](#), a direct mapping of the Controlled Unclassified Information (CUI) security requirements to the security controls in [\[SP 800-53\]](#) and [\[ISO 27001\]](#). These controls are also mapped to the Categories and Subcategories associated with Cybersecurity Framework Core Functions: *Identify, Protect, Detect, Respond*, and *Recover*. The security control mappings can be useful to organizations that wish to demonstrate compliance to the security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls.

#### **ADDITIONAL RESOURCES**

Mapping security controls to the Cybersecurity Framework:  
<https://csrc.nist.gov/publications/detail/nistir/8170/draft>.

Mapping CUI security requirements to the Cybersecurity Framework:  
<https://csrc.nist.gov/projects/cybersecurity-framework/informative-reference-catalog/details/1>.



## Table of Contents

<b>CHAPTER ONE</b>	<b>INTRODUCTION</b> .....	<b>1</b>
1.1	PURPOSE AND APPLICABILITY .....	2
1.2	TARGET AUDIENCE .....	4
1.3	ORGANIZATION OF THIS SPECIAL PUBLICATION .....	4
<b>CHAPTER TWO</b>	<b>THE FUNDAMENTALS</b> .....	<b>5</b>
2.1	BASIC ASSUMPTIONS .....	5
2.2	DEVELOPMENT OF SECURITY REQUIREMENTS .....	6
<b>CHAPTER THREE</b>	<b>THE REQUIREMENTS</b> .....	<b>9</b>
3.1	ACCESS CONTROL.....	10
3.2	AWARENESS AND TRAINING .....	16
3.3	AUDIT AND ACCOUNTABILITY .....	17
3.4	CONFIGURATION MANAGEMENT .....	20
3.5	IDENTIFICATION AND AUTHENTICATION .....	23
3.6	INCIDENT RESPONSE .....	26
3.7	MAINTENANCE.....	27
3.8	MEDIA PROTECTION .....	29
3.9	PERSONNEL SECURITY.....	31
3.10	PHYSICAL PROTECTION .....	32
3.11	RISK ASSESSMENT .....	33
3.12	SECURITY ASSESSMENT.....	34
3.13	SYSTEM AND COMMUNICATIONS PROTECTION.....	36
3.14	SYSTEM AND INFORMATION INTEGRITY.....	40
<b>APPENDIX A</b>	<b>REFERENCES</b> .....	<b>44</b>
<b>APPENDIX B</b>	<b>GLOSSARY</b> .....	<b>51</b>
<b>APPENDIX C</b>	<b>ACRONYMS</b> .....	<b>60</b>
<b>APPENDIX D</b>	<b>MAPPING TABLES</b> .....	<b>61</b>
<b>APPENDIX E</b>	<b>TAILORING CRITERIA</b> .....	<b>84</b>

## Errata

This table contains changes that have been incorporated into Special Publication 800-171. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature.

DATE	TYPE	CHANGE	PAGE
01-28-2021	Editorial	Front Matter Blue Box: Change “The requirements apply only” to “The security requirements apply”	vii
01-28-2021	Editorial	Chapter One, Section 1.1, Paragraph 1: Delete: “The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.”	2
01-28-2021	Editorial	Chapter One, Section 1.1, Paragraph 2: Add “The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization’s security posture to a level beyond that which it requires for protecting its missions, operations, and assets.”	2
01-28-2021	Editorial	Chapter One, Section 1.1, Paragraph 3: Change: “The requirements are” to “The recommended security requirements in this publication are”	3
01-28-2021	Editorial	Chapter One, Section 1.1, Paragraph 6: Delete: “If nonfederal organizations entrusted with protecting CUI designate systems or components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements to only those systems or components. Isolating CUI into its own security domain by applying architectural design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices) may be the most cost-effective and efficient approach for nonfederal organizations to satisfy the security requirements and protect the confidentiality of CUI. Security domains may employ physical separation, logical separation, or a combination of both. This approach can reasonably provide adequate security for the CUI and avoid increasing the organization’s security posture to a level beyond which it typically requires for protecting its missions, operations, and assets.”	4

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

## CHAPTER ONE

# INTRODUCTION

### THE NEED TO PROTECT CONTROLLED UNCLASSIFIED INFORMATION

Today, more than at any time in history, the federal government is relying on external service providers to help carry out a wide range of federal missions and business functions using information systems.<sup>1</sup> Many federal contractors process, store, and transmit sensitive federal information to support the delivery of essential products and services to federal agencies (e.g., providing financial services; providing web and electronic mail services; processing security clearances or healthcare data; providing cloud services; and developing communications, satellite, and weapons systems). Federal information is frequently provided to or shared with entities such as state and local governments, colleges and universities, and independent research organizations. The protection of sensitive federal information while residing in *nonfederal systems*<sup>2</sup> and organizations is of paramount importance to federal agencies, and can directly impact the ability of the federal government to carry out its designated missions and business operations.

The protection of unclassified federal information in nonfederal systems and organizations is dependent on the federal government providing a process for identifying the different types of information that are used by federal agencies. [EO 13556] established a governmentwide Controlled Unclassified Information (CUI)<sup>3</sup> Program to standardize the way the executive branch handles unclassified information that requires protection.<sup>4</sup> Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI. The CUI Program is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry [NARA CUI]. The CUI Registry is the online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent. The CUI Registry identifies approved CUI categories, provides general descriptions for each, identifies the basis for controls, and sets out procedures for the use of CUI including, but not limited to, marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

---

<sup>1</sup> An *information system* is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems, for example: industrial/process control systems, cyber-physical systems, embedded systems, and devices. The term *system* is used throughout this publication to represent all types of computing platforms that can process, store, or transmit CUI.

<sup>2</sup> A *federal information system* is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. A system that does not meet such criteria is a *nonfederal system*.

<sup>3</sup> *Controlled Unclassified Information* is any information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under [EO 13526] or any predecessor or successor order, or [ATOM54], as amended.

<sup>4</sup> [EO 13556] designated the National Archives and Records Administration (NARA) as the Executive Agent to implement the CUI Program.

[EO 13556] also required that the CUI Program emphasize openness, transparency, and uniformity of governmentwide practices, and that the implementation of the program take place in a manner consistent with applicable policies established by the Office of Management and Budget (OMB) and federal standards and guidelines issued by the National Institute of Standards and Technology (NIST). The federal CUI *regulation*,<sup>5</sup> developed by the CUI Executive Agent, provides guidance to federal agencies on the designation, safeguarding, dissemination, marking, decontrolling, and disposition of CUI, establishes self-inspection and oversight requirements, and delineates other facets of the program.

## 1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide federal agencies with recommended security requirements<sup>6</sup> for protecting the *confidentiality* of CUI: (1) when the CUI is resident in a nonfederal system and organization; (2) when the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency;<sup>7</sup> and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.<sup>8</sup>

The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.<sup>9</sup> If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI *security domain*. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.

<sup>5</sup> [32 CFR 2002] was issued on September 14, 2016 and became effective on November 14, 2016.

<sup>6</sup> The term *requirements* can be used in different contexts. In the context of federal information security and privacy policies, the term is generally used to refer to information security and privacy obligations imposed on organizations. For example, OMB Circular A-130 imposes a series of information security and privacy requirements with which federal agencies must comply when managing information resources. In addition to the use of the term requirements in the context of federal policy, the term requirements is used in this guideline in a broader sense to refer to an expression of the set of stakeholder protection needs for a particular system or organization. Stakeholder protection needs and corresponding security requirements may be derived from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments). The term requirements, as used in this guideline, includes both legal and policy requirements, as well as an expression of the broader set of stakeholder protection needs that may be derived from other sources. All of these requirements, when applied to a system, help determine the required characteristics of the system.

<sup>7</sup> Nonfederal organizations that collect or maintain information *on behalf of* a federal agency or that use or operate a system *on behalf of* an agency, must comply with the requirements in [FISMA], including the requirements in [FIPS 200] and the security controls in [SP 800-53] (See [44 USC 3554] (a)(1)(A)).

<sup>8</sup> The requirements in this publication can be used to comply with the [FISMA] requirement for senior agency officials to provide information security for the information that supports the operations and assets under their control, including CUI that is resident in nonfederal systems and organizations (See [44 USC 3554] (a)(1)(A) and (a)(2)).

<sup>9</sup> System *components* include, for example: mainframes, workstations, servers; input and output devices; network components; operating systems; virtual machines; and applications.

The recommended security requirements in this publication are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. In CUI guidance and the CUI Federal Acquisition Regulation (FAR),<sup>10</sup> the CUI Executive Agent will address determining compliance with security requirements.<sup>11</sup>

In accordance with the federal CUI regulation, federal agencies using federal systems to process, store, or transmit CUI, at a minimum, must comply with:

- [Federal Information Processing Standards \(FIPS\) Publication 199](#), *Standards for Security Categorization of Federal Information and Information Systems* (moderate confidentiality);<sup>12</sup>
- [Federal Information Processing Standards \(FIPS\) Publication 200](#), *Minimum Security Requirements for Federal Information and Information Systems*;
- [NIST Special Publication 800-53](#), *Security and Privacy Controls for Federal Information Systems and Organizations*; and
- [NIST Special Publication 800-60](#), *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The responsibility of federal agencies to protect CUI does not change when such information is shared with nonfederal partners. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by *nonfederal organizations* using nonfederal systems.<sup>13</sup> The recommended requirements for safeguarding CUI in nonfederal systems and organizations are derived from the above authoritative federal standards and guidelines to maintain a consistent level of protection. However, recognizing that the scope of the safeguarding requirements in the federal CUI regulation is limited to the security objective of confidentiality (i.e., not directly addressing integrity and availability) and that some of the security requirements expressed in the NIST standards and guidelines are uniquely federal, the requirements in this publication have been *tailored* for nonfederal entities.

The tailoring criteria described in [Chapter Two](#) are not intended to reduce or minimize the federal requirements for the safeguarding of CUI as expressed in the federal CUI regulation. Rather, the intent is to express the requirements in a manner that allows for and facilitates the equivalent safeguarding measures within nonfederal systems and organizations and does not diminish the level of protection of CUI required for moderate confidentiality. Additional or differing requirements, other than the requirements described in this publication, may be applied only when such requirements are based on law, regulation, or governmentwide policy and when indicated in the CUI Registry as CUI-specified or when an agreement establishes

---

<sup>10</sup> NARA, as the CUI Executive Agent, plans to sponsor a single FAR clause that will apply the requirements of the federal CUI regulation and NIST Special Publication 800-171 to contractors. Until the FAR clause is in place, the requirements in NIST Special Publication 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

<sup>11</sup> [\[SP 800-171A\]](#) provides assessment procedures to determine compliance to the CUI security requirements.

<sup>12</sup> [\[FIPS 199\]](#) defines three values of potential impact (i.e., low, moderate, high) on organizations, assets, or individuals in the event of a breach of security (e.g., a loss of confidentiality).

<sup>13</sup> A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal system. Examples include: state, local, and tribal governments; colleges and universities; and contractors.

requirements to protect CUI Basic<sup>14</sup> at higher than moderate confidentiality. The provision of safeguarding requirements for CUI in a specified category will be addressed by the National Archives and Records Administration (NARA) in its CUI guidance and in the CUI FAR; and reflected as specific requirements in contracts or other agreements. Nonfederal organizations may use the same CUI infrastructure for multiple government contracts or agreements, if the CUI infrastructure meets the safeguarding requirements for the organization's CUI-related contracts and/or agreements including any specific safeguarding required or permitted by the authorizing law, regulation, or governmentwide policy.

## 1.2 TARGET AUDIENCE

This publication serves a diverse group of individuals and organizations in both the public and private sectors including, but not limited to, individuals with:

- System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators);
- Acquisition or procurement responsibilities (e.g., contracting officers);
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers); and
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts).

The above roles and responsibilities can be viewed from two distinct perspectives: the *federal perspective* as the entity establishing and conveying the security requirements in contractual vehicles or other types of inter-organizational agreements; and the *nonfederal perspective* as the entity responding to and complying with the security requirements set forth in contracts or agreements.

## 1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- [Chapter Two](#) describes the fundamental assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI; the format and structure of the requirements; and the tailoring criteria applied to the NIST standards and guidelines to obtain the requirements.
- [Chapter Three](#) describes the fourteen families of security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.
- [Supporting appendices](#) provide additional information related to the protection of CUI in nonfederal systems and organizations including: general references; definitions and terms; acronyms; mapping tables relating security requirements to the security controls in [\[SP 800-53\]](#) and [\[ISO 27001\]](#); and tailoring actions applied to the moderate security control baseline.

---

<sup>14</sup> CUI Basic is defined in the CUI Registry [\[NARA CUI\]](#).

## CHAPTER TWO

# THE FUNDAMENTALS

## ASSUMPTIONS AND METHODOLOGY FOR DEVELOPING SECURITY REQUIREMENTS

This chapter describes the assumptions and the methodology used to develop the recommended security requirements to protect CUI in nonfederal systems and organizations; the structure of the basic and derived security requirements; and the tailoring criteria applied to the federal information security requirements and controls.

### 2.1 BASIC ASSUMPTIONS

The recommended security requirements described in this publication have been developed based on three fundamental assumptions:

- Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal systems or nonfederal systems including the environments in which those systems operate;
- Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal systems and organizations; and
- The confidentiality impact value for CUI is no less than [\[FIPS 199\]](#) *moderate*.<sup>15 16</sup>

The assumptions reinforce the concept that federal information designated as CUI has the same intrinsic *value* and potential *adverse impact* if compromised—whether such information resides in a federal or a nonfederal organization. Thus, protecting the confidentiality of CUI is critical to the mission and business success of federal agencies and the economic and national security interests of the nation. Additional assumptions also impacting the development of the security requirements and the expectation of federal agencies in working with nonfederal entities include:

- Nonfederal organizations have information technology infrastructures in place, and are not necessarily developing or acquiring systems specifically for processing, storing, or transmitting CUI;
- Nonfederal organizations have specific safeguarding measures in place to protect their information which may also be sufficient to satisfy the security requirements;
- Nonfederal organizations may not have the necessary organizational structure or resources to satisfy every security requirement and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement; and
- Nonfederal organizations can implement a variety of potential security solutions directly or using external service providers (e.g., managed services) to satisfy security requirements.

<sup>15</sup> The moderate impact *value* defined in [\[FIPS 199\]](#) may become part of a moderate impact *system* in [\[FIPS 200\]](#), which requires the use of the moderate baseline in [\[SP 800-53\]](#) as the starting point for tailoring actions.

<sup>16</sup> In accordance with [\[32 CFR 2002\]](#), CUI is categorized at no less than the moderate confidentiality impact value. However, when federal law, regulation, or governmentwide policy establishing the control of the CUI specifies controls that differ from those of the moderate confidentiality baseline, then these will be followed.

### IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI

Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the recommended security requirements contained in this publication are consistent with and are complementary to the standards and guidelines used by federal agencies to protect CUI.

## 2.2 DEVELOPMENT OF SECURITY REQUIREMENTS

The security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations have a well-defined structure that consists of a *basic security requirements* section and a *derived security requirements* section. The basic security requirements are obtained from [FIPS 200], which provides the high-level and fundamental security requirements for federal information and systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in [SP 800-53]. Starting with the security requirements and the security controls in the moderate baseline (i.e., the minimum level of protection required for CUI in federal systems and organizations), the requirements and controls are *tailored* to eliminate requirements, controls, or parts of controls that are:

- Uniquely federal (i.e., primarily the responsibility of the federal government);
- Not directly related to protecting the confidentiality of CUI; or
- Expected to be routinely satisfied by nonfederal organizations without specification.<sup>17</sup>

[Appendix E](#) provides a complete listing of security controls that support the CUI derived security requirements and those controls that have been eliminated from the moderate baseline based on the CUI tailoring criteria described above.

The combination of the basic and derived security requirements captures the intent of [FIPS 200] and [SP 800-53] with respect to the protection of the *confidentiality* of CUI in nonfederal systems and organizations. [Appendix D](#) provides informal mappings of the security requirements to the relevant security controls in [SP 800-53] and [ISO 27001]. The mappings promote a better understanding of the CUI security requirements, and are *not* intended to impose additional requirements on nonfederal organizations.

---

<sup>17</sup> The security requirements developed from the tailored [FIPS 200] security requirements and the [SP 800-53] moderate security control baseline represent a subset of the safeguarding measures that are necessary for a *comprehensive* information security program. The strength and quality of such programs in nonfederal organizations depend on the degree to which the organizations implement the security requirements and controls that are expected to be routinely satisfied without specification by the federal government. This includes implementing security policies, procedures, and practices that support an effective risk-based information security program. Nonfederal organizations are encouraged to refer to [Appendix E](#) and [SP 800-53] for a complete listing of security controls in the moderate baseline deemed out of scope for the security requirements in [Chapter Three](#).



The following *Media Protection* family example illustrates the structure of a CUI requirement:

**Basic Security Requirements**

- 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
- 3.8.2 Limit access to CUI on system media to authorized users.
- 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

**Derived Security Requirements**

- 3.8.4 Mark media with necessary CUI markings and distribution limitations.
- 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- 3.8.7 Control the use of removable media on system components.
- 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.
- 3.8.9 Protect the confidentiality of backup CUI at storage locations.

For ease of use, the security requirements are organized into fourteen *families*. Each family contains the requirements related to the general security topic of the family. The families are closely aligned with the minimum-security requirements for federal information and systems described in [FIPS 200]. The *contingency planning, system and services acquisition, and planning* requirements are not included within the scope of this publication due to the tailoring criteria.<sup>18</sup> Table 1 lists the security requirement families addressed in this publication.

**TABLE 1: SECURITY REQUIREMENT FAMILIES**

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

<sup>18</sup> Three exceptions include: a requirement to protect the confidentiality of system backups (derived from CP-9) from the *contingency planning* family; a requirement to develop and implement a system security plan (derived from PL-2) from the *planning* family; and a requirement to implement system security engineering principles (derived from SA-8) from the *system and services acquisition* family. The requirements are included in the CUI *media protection, security assessment, and system and communications protection* requirements families, respectively.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

A *discussion* section follows each CUI security requirement providing additional information to facilitate the implementation and assessment of the requirements. This information is derived primarily from the security controls discussion sections in [SP 800-53] and is provided to give organizations a better understanding of the mechanisms and procedures used to implement the controls used to protect CUI. The discussion section is *informative*, not *normative*. It is not intended to extend the scope of a requirement or to influence the solutions organizations may use to satisfy a requirement. The use of examples is notional, not exhaustive, and not reflective of potential options available to organizations. Figure 1 illustrates basic security requirement 3.8.3 with its supporting discussion section and informative references.

**3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.**

**DISCUSSION**

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.

[SP 800-88] provides guidance on media sanitization.

**FIGURE 1: FORMAT AND STRUCTURE OF CUI SECURITY REQUIREMENT**

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

## CHAPTER THREE

# THE REQUIREMENTS

### SECURITY REQUIREMENTS FOR PROTECTING THE CONFIDENTIALITY OF CUI

This chapter describes fourteen families of recommended security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.<sup>19</sup> The security controls from [SP 800-53] associated with the basic and derived requirements are listed in Appendix D.<sup>20</sup> Organizations can use the NIST publication to obtain additional, non-prescriptive information related to the recommended security requirements (e.g., explanatory information in the discussion section for each of the referenced security controls, mapping tables to [ISO 27001] security controls, and a catalog of optional controls that can be used to specify additional security requirements, if needed). This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk. Nonfederal organizations can implement a variety of potential security solutions either directly or using managed services, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement.<sup>21</sup>

#### DISCUSSION SECTION

The discussion section associated with each CUI requirement is *informative*, not *normative*. It is not intended to extend the scope of a requirement or to influence the solutions organizations may use to satisfy a requirement. In addition, the use of examples is notional, not exhaustive, and not reflective of potential options available to organizations.

Nonfederal organizations describe, in a system security plan, how the security requirements are met or how organizations plan to meet the requirements and address known and anticipated threats. The system security plan describes: the system boundary; operational environment; how security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations develop plans of action that describe how unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and the plan of action as separate or combined documents and in any chosen format.<sup>22</sup>

<sup>19</sup> The security objectives of confidentiality and integrity are closely related since many of the underlying security mechanisms at the system level support both objectives. Therefore, the basic and derived security requirements in this publication provide protection from unauthorized disclosure and unauthorized modification of CUI.

<sup>20</sup> The security control references in Appendix D are included to promote a better understanding of the recommended security requirements and do not expand the scope of the requirements.

<sup>21</sup> To promote consistency, transparency, and comparability, the compensatory security measures selected by organizations are based on or derived from *existing* and *recognized* security standards and control sets, including, for example, [ISO 27001] or [SP 800-53].

<sup>22</sup> [NIST CUI] provides supplemental material for Special Publication 800-171 including templates for system security plans and plans of action.

When requested, the system security plan (or extracts thereof) and the associated plans of action for any planned implementations or mitigations are submitted to the responsible federal agency/contracting office to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to a risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

The recommended security requirements in this publication apply only to the components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components. Some systems, including specialized systems (e.g., industrial/process control systems, medical devices, Computer Numerical Control machines), may have limitations on the application of certain security requirements.

To accommodate such issues, the system security plan, as reflected in requirement [3.12.4](#), is used to describe any enduring exceptions to the security requirements. Individual, isolated, or temporary deficiencies are managed through plans of action, as reflected in requirement [3.12.2](#).

### THE MEANING OF ORGANIZATIONAL SYSTEMS

The term *organizational system* is used in many of the recommended CUI security requirements in this publication. This term has a specific meaning regarding the scope of applicability for the security requirements. The requirements apply only to the components of nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components. The appropriate scoping for the CUI security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI.

## 3.1 ACCESS CONTROL

### *Basic Security Requirements*

#### **[3.1.1](#) Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).**

##### **DISCUSSION**

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged versus non-privileged) are addressed in requirement 3.1.2.

#### **[3.1.2](#) Limit system access to the types of transactions and functions that authorized users are permitted to execute.**

## DISCUSSION

Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

### *Derived Security Requirements*

#### **3.1.3 Control the flow of CUI in accordance with approved authorizations.**

## DISCUSSION

Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: keeping export-controlled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within the organization; restricting requests to the Internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Transferring information between systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes: prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

#### **3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.**

## DISCUSSION

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management, quality assurance and testing, system management, programming, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

**3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.**

**DISCUSSION**

Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

**3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.**

**DISCUSSION**

This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

**3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.**

**DISCUSSION**

Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in [3.1.2](#).

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

**3.1.8 Limit unsuccessful logon attempts.**

**DISCUSSION**

This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the

organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

### **3.1.9 Provide privacy and security notices consistent with applicable CUI rules.**

#### **DISCUSSION**

System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for legal review and approval of warning banner content.

### **3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.**

#### **DISCUSSION**

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

Pattern-hiding displays can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.

### **3.1.11 Terminate (automatically) a user session after a defined condition.**

#### **DISCUSSION**

This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

### **3.1.12 Monitor and control remote access sessions.**

#### **DISCUSSION**

Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with

appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

[[SP 800-46](#)], [[SP 800-77](#)], and [[SP 800-113](#)] provide guidance on secure remote access and virtual private networks.

### **[3.1.13](#) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.**

#### **DISCUSSION**

Cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. See [[NIST CRYPTO](#)]; [[NIST CAVP](#)]; [[NIST CMVP](#)]; National Security Agency Cryptographic Standards.

### **[3.1.14](#) Route remote access via managed access control points.**

#### **DISCUSSION**

Routing remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.

### **[3.1.15](#) Authorize remote execution of privileged commands and remote access to security-relevant information.**

#### **DISCUSSION**

A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.

### **[3.1.16](#) Authorize wireless access prior to allowing such connections.**

#### **DISCUSSION**

Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide credential protection and mutual authentication.

[[SP 800-97](#)] provide guidance on secure wireless networks.

### **[3.1.17](#) Protect wireless access using authentication and encryption.**



## DISCUSSION

Organizations authenticate individuals and devices to help protect wireless access to the system. Special attention is given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems. See [\[NIST CRYPTO\]](#).

### **[3.1.18](#) Control connection of mobile devices.**

#### DISCUSSION

A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features for synchronizing local data with remote locations. Examples of mobile devices include smart phones, e-readers, and tablets.

Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include: device identification and authentication; configuration management; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). The need to provide adequate security for mobile devices goes beyond this requirement. Many controls for mobile devices are reflected in other CUI security requirements.

[\[SP 800-124\]](#) provides guidance on mobile device security.

### **[3.1.19](#) Encrypt CUI on mobile devices and mobile computing platforms.<sup>23</sup>**

#### DISCUSSION

Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices and computing platforms. Container-based encryption provides a more fine-grained approach to the encryption of data and information including encrypting selected data structures such as files, records, or fields. See [\[NIST CRYPTO\]](#).

### **[3.1.20](#) Verify and control/limit connections to and use of external systems.**

#### DISCUSSION

External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of CUI, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems.

Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If

---

<sup>23</sup> Mobile devices and computing platforms include, for example, smartphones and tablets.

terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations.

Note that while “external” typically refers to outside of the organization’s direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external” to that system.

### **3.1.21 Limit use of portable storage devices on external systems.**

#### **DISCUSSION**

Limits on the use of organization-controlled portable storage devices in external systems include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. Note that while “external” typically refers to outside of the organization’s direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. Among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external” to that system.

### **3.1.22 Control CUI posted or processed on publicly accessible systems.**

#### **DISCUSSION**

In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

## **3.2 AWARENESS AND TRAINING**

### *Basic Security Requirements*

#### **3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.**

#### **DISCUSSION**

Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security

incidents. The content also addresses awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events.

[[SP 800-50](#)] provides guidance on security awareness and training programs.

### **3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.**

#### **DISCUSSION**

Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of organizations and the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, systems integrators, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and other personnel having access to system-level software, security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

[[SP 800-181](#)] provides guidance on role-based information security training in the workplace. [[SP 800-161](#)] provides guidance on supply chain risk management.

#### *Derived Security Requirements*

### **3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.**

#### **DISCUSSION**

Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

## **3.3 AUDIT AND ACCOUNTABILITY**

#### *Basic Security Requirements*

### **3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.**

## DISCUSSION

An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.

Audit record content that may be necessary to satisfy this requirement includes time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred).

Detailed information that organizations may consider in audit records includes full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making.

[[SP 800-92](#)] provides guidance on security log management.

### **3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.**

#### DISCUSSION

This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, communications at system boundaries, configuration settings, physical access, nonlocal maintenance, use of maintenance tools, temperature and humidity, equipment delivery and removal, system component inventory, use of mobile code, and use of Voice over Internet Protocol (VoIP).

#### *Derived Security Requirements*

### **3.3.3 Review and update logged events.**

## DISCUSSION

The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.

### **3.3.4 Alert in the event of an audit logging process failure.**

#### DISCUSSION

Audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

### **3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.**

#### DISCUSSION

Correlating audit record review, analysis, and reporting processes helps to ensure that they do not operate independently, but rather collectively. Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

### **3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.**

#### DISCUSSION

Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities. Audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

### **3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.**

#### DISCUSSION

Internal system clocks are used to generate time stamps, which include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network. See [\[IETF 5905\]](#).

**3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.**

**DISCUSSION**

Audit information includes all information (e.g., audit records, audit log settings, and audit reports) needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct audit and logging activities. This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements.

**3.3.9 Limit management of audit logging functionality to a subset of privileged users.**

**DISCUSSION**

Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records. This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

## **3.4 CONFIGURATION MANAGEMENT**

### *Basic Security Requirements*

**3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.**

**DISCUSSION**

Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration

Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., system association, system owner). Information deemed necessary for effective accountability of system components includes hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include manufacturer, device type, model, serial number, and physical location.

[[SP 800-128](#)] provides guidance on security-focused configuration management.

### **3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.**

#### **DISCUSSION**

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, input and output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

Security parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security requirements. Security parameters include: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors.

[[SP 800-70](#)] and [[SP 800-128](#)] provide guidance on security configuration settings.

#### *Derived Security Requirements*

### **3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.**

#### **DISCUSSION**

Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.

[[SP 800-128](#)] provides guidance on configuration change control.

### **3.4.4 Analyze the security impact of changes prior to implementation.**

## DISCUSSION

Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required.

[[SP 800-128](#)] provides guidance on configuration change control and security impact analysis.

### **3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.**

#### DISCUSSION

Any changes to the hardware, software, or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries.

Access restrictions include physical and logical access control requirements, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems), and change windows (e.g., changes occur only during certain specified times). In addition to security concerns, commonly-accepted due diligence for configuration management includes access restrictions as an essential part in ensuring the ability to effectively manage the configuration.

[[SP 800-128](#)] provides guidance on configuration change control.

### **3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.**

#### DISCUSSION

Systems can provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. It is sometimes convenient to provide multiple services from single system components. However, doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per component.

Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

### **3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.**



## DISCUSSION

Restricting the use of nonessential software (programs) includes restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time. The organization makes a security-based determination which functions, ports, protocols, and/or services are restricted. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of protocols organizations consider preventing the use of, restricting, or disabling.

### **3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.**

## DISCUSSION

The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup.

[\[SP 800-167\]](#) provides guidance on application whitelisting.

### **3.4.9 Control and monitor user-installed software.**

## DISCUSSION

Users can install software in organizational systems if provided the necessary privileges. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation through policies. Permitted software installations include updates and security patches to existing software and applications from organization-approved “app stores.” Prohibited software installations may include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

## 3.5 IDENTIFICATION AND AUTHENTICATION

### *Basic Security Requirements*

#### **3.5.1 Identify system users, processes acting on behalf of users, and devices.**

## DISCUSSION

Common device identifiers include Media Access Control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device.

[\[SP 800-63-3\]](#) provides guidance on digital identities.

### **3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.**

#### **DISCUSSION**

Individual authenticators include the following: passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include certificates and passwords.

[[SP 800-63-3](#)] provides guidance on digital identities.

#### *Derived Security Requirements*

### **3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.**<sup>24 25</sup>

#### **DISCUSSION**

Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security.

Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.

---

<sup>24</sup> *Multifactor authentication* requires two or more different factors to achieve authentication. The factors include: something you know (e.g., password/PIN); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). The requirement for multifactor authentication should not be interpreted as requiring federal Personal Identity Verification (PIV) card or Department of Defense Common Access Card (CAC)-like solutions. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.

<sup>25</sup> *Local access* is any access to a system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. *Network access* is any access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

[\[SP 800-63-3\]](#) provides guidance on digital identities.

**[3.5.4](#) Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.**

**DISCUSSION**

Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

[\[SP 800-63-3\]](#) provides guidance on digital identities.

**[3.5.5](#) Prevent reuse of identifiers for a defined period.**

**DISCUSSION**

Identifiers are provided for users, processes acting on behalf of users, or devices ([3.5.1](#)). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

**[3.5.6](#) Disable identifiers after a defined period of inactivity.**

**DISCUSSION**

Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.

**[3.5.7](#) Enforce a minimum password complexity and change of characters when new passwords are created.**

**DISCUSSION**

This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.

**[3.5.8](#) Prohibit password reuse for a specified number of generations.**

**DISCUSSION**

Password lifetime restrictions do not apply to temporary passwords.

**[3.5.9](#) Allow temporary password use for system logons with an immediate change to a permanent password.**

**DISCUSSION**

Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.

**[3.5.10](#) Store and transmit only cryptographically-protected passwords.**

## DISCUSSION

Cryptographically-protected passwords use salted one-way cryptographic hashes of passwords. See [\[NIST CRYPTO\]](#).

### **3.5.11 Obscure feedback of authentication information.**

#### DISCUSSION

The feedback from systems does not provide any information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring authenticator feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.

## **3.6 INCIDENT RESPONSE**

### *Basic Security Requirements*

#### **3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.**

#### DISCUSSION

Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also includes incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required.

[\[SP 800-61\]](#) provides guidance on incident handling. [\[SP 800-86\]](#) and [\[SP 800-101\]](#) provide guidance on integrating forensic techniques into incident response. [\[SP 800-161\]](#) provides guidance on supply chain risk management.

#### **3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.**

## DISCUSSION

Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies.

[\[SP 800-61\]](#) provides guidance on incident handling.

### *Derived Security Requirements*

#### **[3.6.3](#) Test the organizational incident response capability.**

## DISCUSSION

Organizations test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (both parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

[\[SP 800-84\]](#) provides guidance on testing programs for information technology capabilities.

## 3.7 MAINTENANCE

### *Basic Security Requirements*

#### **[3.7.1](#) Perform maintenance on organizational systems.<sup>26</sup>**

## DISCUSSION

This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

#### **[3.7.2](#) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.**

## DISCUSSION

This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the

---

<sup>26</sup> In general, system maintenance requirements tend to support the security objective of *availability*. However, improper system maintenance or a failure to perform maintenance can result in the unauthorized disclosure of CUI, thus compromising *confidentiality* of that information.

controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems. Maintenance tools can include hardware, software, and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.

### *Derived Security Requirements*

#### **3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.**

##### **DISCUSSION**

This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

[[SP 800-88](#)] provides guidance on media sanitization.

#### **3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.**

##### **DISCUSSION**

If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.

#### **3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.**

##### **DISCUSSION**

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. The authentication techniques employed in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in [3.5.3](#).

#### **3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.**

##### **DISCUSSION**

This requirement applies to individuals who are performing hardware or software maintenance on organizational systems, while [3.10.1](#) addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

## 3.8 MEDIA PROTECTION

### *Basic Security Requirements*

#### **3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.**

##### **DISCUSSION**

System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Access to CUI on system media can be limited by physically controlling such media, which includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media.

[\[SP 800-111\]](#) provides guidance on storage encryption technologies for end user devices.

#### **3.8.2 Limit access to CUI on system media to authorized users.**

##### **DISCUSSION**

Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

#### **3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.**

##### **DISCUSSION**

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.

[\[SP 800-88\]](#) provides guidance on media sanitization.

## *Derived Security Requirements*

### **3.8.4 Mark media with necessary CUI markings and distribution limitations.<sup>27</sup>**

#### **DISCUSSION**

The term security marking refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. See [[NARA MARK](#)].

### **3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.**

#### **DISCUSSION**

Controlled areas are areas or spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting systems and information. Controls to maintain accountability for media during transport include locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

### **3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.**

#### **DISCUSSION**

This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives). See [[NIST CRYPTO](#)].

[[SP 800-111](#)] provides guidance on storage encryption technologies for end user devices.

### **3.8.7 Control the use of removable media on system components.**

#### **DISCUSSION**

In contrast to requirement [3.8.1](#), which restricts user access to media, this requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices.

Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable

---

<sup>27</sup> The implementation of this requirement is per marking guidance in [[32 CFR 2002](#)] and [[NARA CUI](#)]. Standard Form (SF) 902 (approximate size 2.125" x 1.25") and SF 903 (approximate size 2.125" x .625") can be used on media that contains CUI such as hard drives, or USB devices. Both forms are available from <https://www.gsaadvantage.gov>. SF 902: NSN 7540-01-679-3318. SF 903: NSN 7540-01-679-3319.



storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices.

**3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.**

**DISCUSSION**

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the overall risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

**3.8.9 Protect the confidentiality of backup CUI at storage locations.**

**DISCUSSION**

Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information at designated storage locations. Backed-up information containing CUI may include system-level information and user-level information. System-level information includes system-state information, operating system software, application software, and licenses. User-level information includes information other than system-level information.

## **3.9 PERSONNEL SECURITY**

### *Basic Security Requirements*

**3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.**

**DISCUSSION**

Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

**3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.**

**DISCUSSION**

Protecting CUI during and after personnel actions may include returning system-related property and conducting exit interviews. System-related property includes hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions

within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

#### *Derived Security Requirements*

None.

### **3.10 PHYSICAL PROTECTION**

#### *Basic Security Requirements*

#### **3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.**

##### **DISCUSSION**

This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

#### **3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.**

##### **DISCUSSION**

Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

#### *Derived Security Requirements*

#### **3.10.3 Escort visitors and monitor visitor activity.**

##### **DISCUSSION**

Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

#### **3.10.4 Maintain audit logs of physical access.**

## DISCUSSION

Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

### **3.10.5 Control and manage physical access devices.**

#### DISCUSSION

Physical access devices include keys, locks, combinations, and card readers.

### **3.10.6 Enforce safeguarding measures for CUI at alternate work sites.**

#### DISCUSSION

Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

[[SP 800-46](#)] and [[SP 800-114](#)] provide guidance on enterprise and user security when teleworking.

## **3.11 RISK ASSESSMENT**

### *Basic Security Requirements*

#### **3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.**

#### DISCUSSION

Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle.

[[SP 800-30](#)] provides guidance on conducting risk assessments.

### *Derived Security Requirements*

#### **3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.**

#### DISCUSSION

Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static

analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.

To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated, scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention, and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of system vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning.

[[SP 800-40](#)] provides guidance on vulnerability management.

### **[3.11.3](#) Remediate vulnerabilities in accordance with risk assessments.**

#### **DISCUSSION**

Vulnerabilities discovered, for example, via the scanning conducted in response to [3.11.2](#), are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

## **3.12 SECURITY ASSESSMENT**

### *Basic Security Requirements*

#### **[3.12.1](#) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.**

#### **DISCUSSION**

Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the system life cycle.

[[SP 800-53](#)] provides guidance on security and privacy controls for systems and organizations. [[SP 800-53A](#)] provides guidance on developing security assessment plans and conducting assessments.

### **3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.**

#### **DISCUSSION**

The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization. [[NIST CUI](#)] provides supplemental material for Special Publication 800-171 including templates for plans of action.

### **3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.**

#### **DISCUSSION**

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make effective and timely risk management decisions.

Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements.

[[SP 800-137](#)] provides guidance on continuous monitoring.

### **3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.<sup>28</sup>**

#### **DISCUSSION**

System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the design or implementation of the controls.

---

<sup>28</sup> There is no prescribed format or specified level of detail for *system security plans*. However, organizations ensure that the required information in 3.12.4 is conveyed in those plans.

System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

[[SP 800-18](#)] provides guidance on developing security plans. [[NIST CUI](#)] provides supplemental material for Special Publication 800-171 including templates for system security plans.

#### *Derived Security Requirements*

None.

### **3.13 SYSTEM AND COMMUNICATIONS PROTECTION**

#### *Basic Security Requirements*

#### **3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.**

##### **DISCUSSION**

Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

[[SP 800-41](#)] provides guidance on firewalls and firewall policy. [[SP 800-125B](#)] provides guidance on security for virtualization technologies.

#### **3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.**

##### **DISCUSSION**

Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security

engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples of these concepts and principles include developing layered protections; establishing security policies, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions.

[[SP 800-160-1](#)] provides guidance on systems security engineering.

### *Derived Security Requirements*

#### **[3.13.3](#) Separate user functionality from system management functionality.**

##### **DISCUSSION**

System management functionality includes functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of these or other methods, as appropriate. This type of separation includes web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

#### **[3.13.4](#) Prevent unauthorized and unintended information transfer via shared system resources.**

##### **DISCUSSION**

The control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This requirement also applies to encrypted representations of information. This requirement does not address information remanence, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

#### **[3.13.5](#) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.**

##### **DISCUSSION**

Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud-based technologies.

[[SP 800-41](#)] provides guidance on firewalls and firewall policy. [[SP 800-125B](#)] provides guidance on security for virtualization technologies.

**[3.13.6](#) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).**

**DISCUSSION**

This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

**[3.13.7](#) Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).**

**DISCUSSION**

Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling allows unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. This requirement is implemented in remote devices (e.g., notebook computers, smart phones, and tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. This requirement is implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

**[3.13.8](#) Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.**

**DISCUSSION**

This requirement applies to internal and external networks and any system components that can transmit information including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of controlled boundaries are susceptible to both interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of the controls for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement compensating safeguards or explicitly accept the additional risk. An example of an alternative physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted. See [[NIST CRYPTO](#)].

**[3.13.9](#) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.**

**DISCUSSION**

This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include de-allocating associated TCP/IP address or port



pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of user inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

**3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.**

**DISCUSSION**

Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards specifying appropriate options, levels, and parameters.

[[SP 800-56A](#)] and [[SP 800-57-1](#)] provide guidance on cryptographic key management and key establishment.

**3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.**

**DISCUSSION**

Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Cryptographic standards include FIPS-validated cryptography and/or NSA-approved cryptography. See [[NIST CRYPTO](#)]; [[NIST CAVP](#)]; and [[NIST CMVP](#)].

**3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.<sup>29</sup>**

**DISCUSSION**

Collaborative computing devices include networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

**3.13.13 Control and monitor the use of mobile code.**

**DISCUSSION**

Mobile code technologies include Java, JavaScript, ActiveX, Postscript, PDF, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations, notebook computers, and devices (e.g., smart phones). Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including requiring mobile code to be digitally signed by a trusted source.

---

<sup>29</sup> Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

[\[SP 800-28\]](#) provides guidance on mobile code.

### **[3.13.14](#) Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.**

#### **DISCUSSION**

VoIP has different requirements, features, functionality, availability, and service limitations when compared with the Plain Old Telephone Service (POTS) (i.e., the standard telephone service). In contrast, other telephone services are based on high-speed, digital communications lines, such as Integrated Services Digital Network (ISDN) and Fiber Distributed Data Interface (FDDI). The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

[\[SP 800-58\]](#) provides guidance on Voice Over IP Systems.

### **[3.13.15](#) Protect the authenticity of communications sessions.**

#### **DISCUSSION**

Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

[\[SP 800-77\]](#), [\[SP 800-95\]](#), and [\[SP 800-113\]](#) provide guidance on secure communications sessions.

### **[3.13.16](#) Protect the confidentiality of CUI at rest.**

#### **DISCUSSION**

Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also use other controls including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest. See [\[NIST CRYPTO\]](#).

## **3.14 SYSTEM AND INFORMATION INTEGRITY**

### *Basic Security Requirements*

#### **[3.14.1](#) Identify, report, and correct system flaws in a timely manner.**

##### **DISCUSSION**

Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness

Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.

[[SP 800-40](#)] provides guidance on patch management technologies.

### **3.14.2 Provide protection from malicious code at designated locations within organizational systems.**

#### **DISCUSSION**

Designated locations include system entry and exit points which may include firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

[[SP 800-83](#)] provides guidance on malware incident prevention.

### **3.14.3 Monitor system security alerts and advisories and take action in response.**

#### **DISCUSSION**

There are many publicly available sources of system security alerts and advisories. For example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Examples of response actions include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations

[[SP 800-161](#)] provides guidance on supply chain risk management.

#### *Derived Security Requirements*

### **3.14.4 Update malicious code protection mechanisms when new releases are available.**

## DISCUSSION

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

### **3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.**

#### DISCUSSION

Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

### **3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.**

#### DISCUSSION

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms supporting critical applications, with such devices being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives.

System monitoring is an integral part of continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound/outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised

systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

[\[SP 800-94\]](#) provides guidance on intrusion detection and prevention systems.

### **[3.14.7](#) Identify unauthorized use of organizational systems.**

#### **DISCUSSION**

System monitoring includes external and internal monitoring. System monitoring can detect unauthorized use of organizational systems. System monitoring is an integral part of continuous monitoring and incident response programs. Monitoring is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Output from system monitoring serves as input to continuous monitoring and incident response programs.

Unusual/unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

[\[SP 800-94\]](#) provides guidance on intrusion detection and prevention systems.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

## APPENDIX A

### REFERENCES

LAWS, EXECUTIVE ORDERS, REGULATIONS, INSTRUCTIONS, STANDARDS, AND GUIDELINES<sup>30</sup>

#### LAWS AND EXECUTIVE ORDERS

- [ATOM54] Atomic Energy Act (P.L. 83-703), August 1954.  
<https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919>
- [FOIA96] Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996.  
<https://www.govinfo.gov/app/details/PLAW-104publ231>
- [FISMA] Federal Information Security Modernization Act (P.L. 113-283), December 2014.  
<https://www.govinfo.gov/app/details/PLAW-113publ283>
- [40 USC 11331] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 ed.  
<https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331>
- [44 USC 3502] Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed.  
<https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapI-sec3502>
- [44 USC 3552] Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed.  
<https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552>
- [44 USC 3554] Title 44 U.S. Code, Sec. 3554, Federal agency responsibilities. 2017 ed.  
<https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3554>
- [EO 13526] Executive Order 13526 (2009) Classified National Security Information. (The White House, Washington, DC), DCPD-200901022, December 29, 2009.  
<https://www.govinfo.gov/app/details/DCPD-200901022>
- [EO 13556] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, Washington, DC), DCPD-201000942, November 4, 2010.  
<https://www.govinfo.gov/app/details/DCPD-201000942>

#### POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS

- [32 CFR 2002] 32 CFR Part 2002, Controlled Unclassified Information, September 2016.  
<https://www.govinfo.gov/app/details/CFR-2017-title32-vol6/CFR-2017-title32-vol6-part2002/summary>

<sup>30</sup> References in this section without specific publication dates or revision numbers are assumed to refer to the most recent updates to those publications.

- [OMB A-130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 2016.  
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>
- [CNSSI 4009] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009.  
<https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

#### STANDARDS, GUIDELINES, AND REPORTS

- [ISO 27001] International Organization for Standardization/International Electrotechnical Commission (2013) Information Technology—Security techniques— Information security management systems—Requirements. (International Organization for Standardization, Geneva, Switzerland), ISO/IEC 27001:2013.  
<https://www.iso.org/standard/54534.html>
- [FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199.  
<https://doi.org/10.6028/NIST.FIPS.199>
- [FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200.  
<https://doi.org/10.6028/NIST.FIPS.200>
- [SP 800-18] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-18r1>
- [SP 800-28] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2.  
<https://doi.org/10.6028/NIST.SP.800-28ver2>
- [SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-30r1>

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

- [SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.  
<https://doi.org/10.6028/NIST.SP.800-39>
- [SP 800-40] Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3.  
<https://doi.org/10.6028/NIST.SP.800-40r3>
- [SP 800-41] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-41r1>
- [SP 800-46] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2.  
<https://doi.org/10.6028/NIST.SP.800-46r2>
- [SP 800-50] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50.  
<https://doi.org/10.6028/NIST.SP.800-50>
- [SP 800-53] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015.  
<https://doi.org/10.6028/NIST.SP.800-53r4>
- [SP 800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014.  
<https://doi.org/10.6028/NIST.SP.800-53Ar4>
- [SP 800-53B] Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-53B. [Forthcoming].
- [SP 800-56A] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3.  
<https://doi.org/10.6028/NIST.SP.800-56Ar3>

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>



- [SP 800-57-1] Barker EB (2016) Recommendation for Key Management, Part 1: General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 4.  
<https://doi.org/10.6028/NIST.SP.800-57pt1r4>
- [SP 800-58] Kuhn R, Walsh TJ, Fries S (2005) Security Considerations for Voice Over IP Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-58.  
<https://doi.org/10.6028/NIST.SP.800-58>
- [SP 800-60-1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-60v1r1>
- [SP 800-60-2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-60v2r1>
- [SP 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2.  
<https://doi.org/10.6028/NIST.SP.800-61r2>
- [SP 800-63-3] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of December 1, 2017.  
<https://doi.org/10.6028/NIST.SP.800-63-3>
- [SP 800-70] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4.  
<https://doi.org/10.6028/NIST.SP.800-70r4>
- [SP 800-77] Frankel SE, Kent K, Lewkowski R, Orebaugh AD, Ritchey RW, Sharma SR (2005) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77.  
<https://doi.org/10.6028/NIST.SP.800-77>
- [SP 800-83] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-83r1>

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

- [SP 800-84] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84.  
<https://doi.org/10.6028/NIST.SP.800-84>
- [SP 800-86] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86.  
<https://doi.org/10.6028/NIST.SP.800-86>
- [SP 800-88] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-88r1>
- [SP 800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92.  
<https://doi.org/10.6028/NIST.SP.800-92>
- [SP 800-94] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94.  
<https://doi.org/10.6028/NIST.SP.800-94>
- [SP 800-95] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95.  
<https://doi.org/10.6028/NIST.SP.800-95>
- [SP 800-97] Frankel SE, Eydtt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-97.  
<https://doi.org/10.6028/NIST.SP.800-97>
- [SP 800-101] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-101, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-101r1>
- [SP 800-111] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111.  
<https://doi.org/10.6028/NIST.SP.800-111>
- [SP 800-113] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113.  
<https://doi.org/10.6028/NIST.SP.800-113>

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

- [SP 800-114] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-114r1>
- [SP 800-124] Souppaya MP, Scarfone KA (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-124r1>
- [SP 800-125B] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125B.  
<https://doi.org/10.6028/NIST.SP.800-125B>
- [SP 800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128.  
<https://doi.org/10.6028/NIST.SP.800-128>
- [SP 800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137.  
<https://doi.org/10.6028/NIST.SP.800-137>
- [SP 800-160-1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018.  
<https://doi.org/10.6028/NIST.SP.800-160v1>
- [SP 800-161] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161.  
<https://doi.org/10.6028/NIST.SP.800-161>
- [SP 800-167] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167.  
<https://doi.org/10.6028/NIST.SP.800-167>
- [SP 800-171A] Ross RS, Dempsey KL, Pillitteri VY (2018) Assessing Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171A.  
<https://doi.org/10.6028/NIST.SP.800-171A>

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

[SP 800-181] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181.  
<https://doi.org/10.6028/NIST.SP.800-181>

**MISCELLANEOUS PUBLICATIONS AND WEBSITES**

[IETF 5905] Mills D, Martin J (ed.), Burbank J, Kasch W (2010) Network Time Protocol Version 4: Protocol and Algorithms Specification. (Internet Engineering Task Force), IETF Request for Comments (RFC) 5905.  
<https://doi.org/10.17487/RFC5905>

[NARA CUI] National Archives and Records Administration (2019) *Controlled Unclassified Information (CUI) Registry*.  
<https://www.archives.gov/cui>

[NARA MARK] National Archives and Records Administration (2016) Marking Controlled Unclassified Information, Version 1.1. (National Archives, Washington, DC).  
<https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf>  
CUI Notice 2019-01, Controlled Unclassified Information Coversheets and Labels.  
<https://www.archives.gov/files/cui/documents/20190222-cui-notice-2019-01-coversheet-label.pdf>

[NIST CAVP] National Institute of Standards and Technology (2019) *Cryptographic Algorithm Validation Program*.  
<https://csrc.nist.gov/projects/cavp>

[NIST CMVP] National Institute of Standards and Technology (2019) *Cryptographic Module Validation Program*.  
<https://csrc.nist.gov/projects/cmvp>

[NIST CRYPTO] National Institute of Standards and Technology (2019) *Cryptographic Standards and Guidelines*.  
<https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines>

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD).  
<https://doi.org/10.6028/NIST.CSWP.04162018>

[NIST CUI] National Institute of Standards and Technology (2019) *Special Publication 800-171 Publication and Supporting Resources*.  
<https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final>

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

## APPENDIX B

### GLOSSARY

#### COMMON TERMS AND DEFINITIONS

**A**ppendix B provides definitions for security terminology used within Special Publication 800-171. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in [\[CNSSI 4009\]](#) *National Information Assurance Glossary*.

<b>agency</b> <a href="#">[OMB A-130]</a>	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.
<b>assessment</b>	See <i>security control assessment</i> .
<b>assessor</b>	See <i>security control assessor</i> .
<b>audit log</b>	A chronological record of system activities, including records of system accesses and operations performed in a given period.
<b>audit record</b>	An individual entry in an audit log related to an audited event.
<b>authentication</b> <a href="#">[FIPS 200, Adapted]</a>	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
<b>availability</b> <a href="#">[44 USC 3552]</a>	Ensuring timely and reliable access to and use of information.
<b>advanced persistent threat</b> <a href="#">[SP 800-39]</a>	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives.
<b>baseline configuration</b>	A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<b>bidirectional authentication</b>	Two parties authenticating each other at the same time. Also known as mutual authentication or two-way authentication.
<b>blacklisting</b>	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.
<b>confidentiality</b> <a href="#">[44 USC 3552]</a>	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
<b>configuration management</b>	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
<b>configuration settings</b>	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.
<b>controlled area</b>	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.
<b>controlled unclassified information</b> <a href="#">[EO 13556]</a>	Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, <i>Classified National Security Information</i> , December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.
<b>CUI categories</b> <a href="#">[32 CFR 2002]</a>	Those types of information for which laws, regulations, or governmentwide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.
<b>CUI Executive Agent</b> <a href="#">[32 CFR 2002]</a>	The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
<b>CUI program</b> <a href="#">[32 CFR 2002]</a>	The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<b>CUI registry</b> <a href="#">[32 CFR 2002]</a>	The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.
<b>cyber-physical systems</b>	Interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.
<b>dual authorization</b> <a href="#">[CNSSI 4009, Adapted]</a>	The system of storage and handling designed to prohibit individual access to certain resources by requiring the presence and actions of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.
<b>executive agency</b> <a href="#">[OMB A-130]</a>	An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91.
<b>external system (or component)</b>	A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
<b>external system service</b>	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
<b>external system service provider</b>	A provider of external system services to an organization through a variety of consumer-producer relationships including, but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
<b>external network</b>	A network not controlled by the organization.
<b>federal agency</b>	See <i>executive agency</i> .
<b>federal information system</b> <a href="#">[40 USC 11331]</a>	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<b>FIPS-validated cryptography</b>	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See <i>NSA-approved cryptography</i> .
<b>firmware</b> <a href="#">[CNSSI 4009]</a>	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. See <i>hardware</i> and <i>software</i> .
<b>hardware</b> <a href="#">[CNSSI 4009]</a>	The material physical components of a system. See <i>software</i> and <i>firmware</i> .
<b>identifier</b>	Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group.
<b>impact</b>	With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.
<b>impact value</b> <a href="#">[FIPS 199]</a>	The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.
<b>incident</b> <a href="#">[44 USC 3552]</a>	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
<b>information</b> <a href="#">[OMB A-130]</a>	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.
<b>information flow control</b>	Procedure to ensure that information transfers within a system are not made in violation of the security policy.
<b>information resources</b> <a href="#">[44 USC 3502]</a>	Information and related resources, such as personnel, equipment, funds, and information technology.



<b>information security</b> <a href="#">[44 USC 3552]</a>	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
<b>information system</b> <a href="#">[44 USC 3502]</a>	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
<b>information technology</b> <a href="#">[OMB A-130]</a>	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.
<b>insider threat</b>	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.
<b>integrity</b> <a href="#">[44 USC 3552]</a>	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
<b>internal network</b>	A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<b>least privilege</b>	The principle that a security architecture is designed so that each entity is granted the minimum system authorizations and resources that the entity needs to perform its function.
<b>local access</b>	Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
<b>malicious code</b>	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
<b>media</b> <a href="#">[FIPS 200]</a>	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.
<b>mobile code</b>	Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.
<b>mobile device</b>	A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.
<b>multifactor authentication</b>	Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). See <i>authenticator</i> .
<b>mutual authentication</b> <a href="#">[CNSSI 4009]</a>	The process of both entities involved in a transaction verifying each other. See <i>bidirectional authentication</i> .
<b>nonfederal organization</b>	An entity that owns, operates, or maintains a nonfederal system.
<b>nonfederal system</b>	A system that does not meet the criteria for a federal system.
<b>network</b>	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<b>network access</b>	Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
<b>nonlocal maintenance</b>	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.
<b>on behalf of (an agency)</b> <a href="#">[32 CFR 2002]</a>	A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those activities are not incidental to providing a service or product to the government.
<b>organization</b> <a href="#">[FIPS 200, Adapted]</a>	An entity of any size, complexity, or positioning within an organizational structure.
<b>personnel security</b> <a href="#">[SP 800-53]</a>	The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness.
<b>portable storage device</b>	A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).
<b>potential impact</b> <a href="#">[FIPS 199]</a>	The loss of confidentiality, integrity, or availability could be expected to have: (i) a <i>limited</i> adverse effect (FIPS Publication 199 low); (ii) a <i>serious</i> adverse effect (FIPS Publication 199 moderate); or (iii) a <i>severe</i> or <i>catastrophic</i> adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
<b>privileged account</b>	A system account with authorizations of a privileged user.
<b>privileged user</b>	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
<b>records</b>	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
<b>remote access</b>	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<b>remote maintenance</b>	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
<b>replay resistance</b>	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.
<b>risk</b> <a href="#">[OMB A-130]</a>	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
<b>risk assessment</b> <a href="#">[SP 800-30]</a>	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
<b>sanitization</b>	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.  Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
<b>security</b> <a href="#">[CNSSI 4009]</a>	A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.
<b>security assessment</b>	See <i>security control assessment</i> .
<b>security control</b> <a href="#">[OMB A-130]</a>	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
<b>security control assessment</b> <a href="#">[OMB A-130]</a>	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
<b>security domain</b> <a href="#">[CNSSI 4009, Adapted]</a>	A domain that implements a security policy and is administered by a single authority.
<b>security functions</b>	The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

<b>split tunneling</b>	The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.
<b>system</b>	See <i>information system</i> .
<b>system component</b> <a href="#">[SP 800-128]</a>	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.
<b>system security plan</b>	A document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. In particular, the system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.
<b>system service</b>	A capability provided by a system that facilitates information processing, storage, or transmission.
<b>threat</b> <a href="#">[SP 800-30]</a>	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
<b>system user</b>	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
<b>whitelisting</b>	A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites.
<b>wireless technology</b>	Technology that permits the transfer of information between separated points without physical connection. Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth.

## APPENDIX C

### ACRONYMS

#### COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
CISA	Cybersecurity and Infrastructure Security Agency
DMZ	Demilitarized Zone
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IoT	Internet of Things
IP	Internet Protocol
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISOO	Information Security Oversight Office
IT	Information Technology
ITL	Information Technology Laboratory
NARA	National Archives and Records Administration
NFO	Nonfederal Organization
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication
VoIP	Voice over Internet Protocol

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

## APPENDIX D

### MAPPING TABLES

#### MAPPING BASIC AND DERIVED SECURITY REQUIREMENTS TO SECURITY CONTROLS

Tables D-1 through D-14 provide a mapping of the basic and derived security requirements to the security controls in [\[SP 800-53\]](#).<sup>31</sup> The mapping tables are included for informational purposes and do not impart additional security requirements beyond those requirements defined in [Chapter Three](#). In some cases, the security controls include additional expectations beyond those required to protect CUI and have been tailored using the criteria in [Chapter Two](#). Only the portion of the security control relevant to the security requirement is applicable. The tables also include a secondary mapping of the security controls to the relevant controls in [\[ISO 27001\]](#). An asterisk (\*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control. Due to the tailoring actions carried out to develop the security requirements, satisfaction of a basic or derived requirement does *not* imply the corresponding NIST security control or control enhancement in [\[SP 800-53\]](#) has also been satisfied, since certain elements of the control or control enhancement that are not essential to protecting the confidentiality of CUI are not reflected in those requirements.

Organizations that have implemented or plan to implement the [\[NIST CSF\]](#) can use the mapping of the security requirements to the security controls in [\[SP 800-53\]](#) and [\[ISO 27001\]](#) to locate the equivalent controls in the Categories and Subcategories associated with the core Functions of the Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. The control mapping information can be useful to organizations that wish to demonstrate compliance to the security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls.

---

<sup>31</sup> The security controls in Tables D-1 through D-14 are taken from NIST Special Publication 800-53, Revision 4. These tables will be updated upon publication of [\[SP 800-53B\]](#) which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements in [Chapter Three](#).

**TABLE D-1: MAPPING ACCESS CONTROL REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.1 ACCESS CONTROL</u></b>				
<b>Basic Security Requirements</b>				
<p><b><u>3.1.1</u></b> Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</p> <p><b><u>3.1.2</u></b> Limit system access to the types of transactions and functions that authorized users are permitted to execute.</p>	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks
	A.14.1.3	Protecting application services transactions		
	A.18.1.3	Protection of records		
	AC-17	Remote Access	A.6.2.1	Mobile device policy
			A.6.2.2	Teleworking
			A.13.1.1	Network controls
A.13.2.1			Information transfer policies and procedures	
A.14.1.2			Securing application services on public networks	
<b>Derived Security Requirements</b>				
<p><b><u>3.1.3</u></b> Control the flow of CUI in accordance with approved authorizations.</p>	AC-4	Information Flow Enforcement	A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>



This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
<a href="#">3.1.4</a> Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5	Separation of Duties	A.6.1.2	Segregation of duties
<a href="#">3.1.5</a> Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6	Least Privilege	A.9.1.2	Access to networks and network services
			A.9.2.3	Management of privileged access rights
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
	AC-6(1)	Least Privilege <i>Authorize Access to Security Functions</i>	<i>No direct mapping.</i>	
AC-6(5)	Least Privilege <i>Privileged Accounts</i>	<i>No direct mapping.</i>		
<a href="#">3.1.6</a> Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	Least Privilege <i>Non-Privileged Access for Nonsecurity Functions</i>	<i>No direct mapping.</i>	
<a href="#">3.1.7</a> Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	AC-6(9)	Least Privilege <i>Log Use of Privileged Functions</i>	<i>No direct mapping.</i>	
	AC-6(10)	Least Privilege <i>Prohibit Non-Privileged Users from Executing Privileged Functions</i>	<i>No direct mapping.</i>	
<a href="#">3.1.8</a> Limit unsuccessful logon attempts.	AC-7	Unsuccessful Logon Attempts	A.9.4.2	Secure logon procedures
<a href="#">3.1.9</a> Provide privacy and security notices consistent with applicable CUI rules.	AC-8	System Use Notification	A.9.4.2	Secure logon procedures
<a href="#">3.1.10</a> Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	AC-11	Session Lock	A.11.2.8	Unattended user equipment
			A.11.2.9	Clear desk and clear screen policy
	AC-11(1)	Session Lock <i>Pattern-Hiding Displays</i>	<i>No direct mapping.</i>	
<a href="#">3.1.11</a> Terminate (automatically) a user session after a defined condition.	AC-12	Session Termination	<i>No direct mapping.</i>	
<a href="#">3.1.12</a> Monitor and control remote access sessions.	AC-17(1)	Remote Access <i>Automated Monitoring / Control</i>	<i>No direct mapping.</i>	

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<a href="#">3.1.13</a> Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2)	Remote Access <i>Protection of Confidentiality / Integrity Using Encryption</i>	<i>No direct mapping.</i>	
<a href="#">3.1.14</a> Route remote access via managed access control points.	AC-17(3)	Remote Access <i>Managed Access Control Points</i>	<i>No direct mapping.</i>	
<a href="#">3.1.15</a> Authorize remote execution of privileged commands and remote access to security-relevant information.	AC-17(4)	Remote Access <i>Privileged Commands / Access</i>	<i>No direct mapping.</i>	
<a href="#">3.1.16</a> Authorize wireless access prior to allowing such connections.	AC-18	Wireless Access	A.6.2.1	Mobile device policy
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
<a href="#">3.1.17</a> Protect wireless access using authentication and encryption.	AC-18(1)	Wireless Access <i>Authentication and Encryption</i>	<i>No direct mapping.</i>	
<a href="#">3.1.18</a> Control connection of mobile devices.	AC-19	Access Control for Mobile Devices	A.6.2.1	Mobile device policy
			A.11.2.6	Security of equipment and assets off-premises
			A.13.2.1	Information transfer policies and procedures
<a href="#">3.1.19</a> Encrypt CUI on mobile devices and mobile computing platforms.	AC-19(5)	Access Control for Mobile Devices <i>Full Device / Container-Based Encryption</i>	<i>No direct mapping.</i>	
<a href="#">3.1.20</a> Verify and control/limit connections to and use of external systems.	AC-20	Use of External Systems	A.11.2.6	Security of equipment and assets off-premises
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
<a href="#">3.1.21</a> Limit use of portable storage devices on external systems.	AC-20(1)	Use of External Systems <i>Limits on Authorized Use</i>	<i>No direct mapping.</i>	
<a href="#">3.1.22</a> Control CUI posted or processed on publicly accessible systems.	AC-20(2)	Use of External Systems <i>Portable Storage Devices</i>	<i>No direct mapping.</i>	
<a href="#">3.1.22</a> Control CUI posted or processed on publicly accessible systems.	AC-22	Publicly Accessible Content	<i>No direct mapping.</i>	

**TABLE D-2: MAPPING AWARENESS AND TRAINING REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.2 AWARENESS AND TRAINING</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.2.1</u></b> Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	AT-2	Security Awareness Training	A.7.2.2	Information security awareness, education, and training
	A.12.2.1	Controls against malware		
<b><u>3.2.2</u></b> Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	AT-3	Role-Based Security Training	A.7.2.2*	Information security awareness, education, and training
<b><i>Derived Security Requirements</i></b>				
<b><u>3.2.3</u></b> Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training <i>Insider Threat</i>	<i>No direct mapping.</i>	

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-3: MAPPING AUDIT AND ACCOUNTABILITY REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.3 AUDIT AND ACCOUNTABILITY</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.3.1</u></b> Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	AU-2	Event Logging	<i>No direct mapping.</i>	
	AU-3	Content of Audit Records	A.12.4.1*	Event logging
<b><u>3.3.2</u></b> Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	AU-3(1)	Content of Audit Records <i>Additional Audit Information</i>	<i>No direct mapping.</i>	
	AU-6	Audit Record Review, Analysis, and Reporting	A.12.4.1	Event logging
			A.16.1.2	Reporting information security events
			A.16.1.4	Assessment of and decision on information security events
	AU-11	Audit Record Retention	A.12.4.1	Event logging
			A.12.4.3	Administrator and operator logs
AU-12	Audit Record Generation	A.12.4.1	Event logging	
		A.16.1.7	Collection of evidence	
<b><i>Derived Security Requirements</i></b>				
<b><u>3.3.3</u></b> Review and update logged events.	AU-2(3)	Event Logging <i>Review and Updates</i>	<i>No direct mapping.</i>	
<b><u>3.3.4</u></b> Alert in the event of an audit logging process failure.	AU-5	Response to Audit Logging Process Failures	<i>No direct mapping.</i>	
<b><u>3.3.5</u></b> Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	AU-6(3)	Audit Record Review, Analysis, and Reporting <i>Correlate Audit Record Repositories</i>	<i>No direct mapping.</i>	
<b><u>3.3.6</u></b> Provide audit record reduction and report generation to support on-demand analysis and reporting.	AU-7	Audit Record Reduction and Report Generation	<i>No direct mapping.</i>	
<b><u>3.3.7</u></b> Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	AU-8	Time Stamps	A.12.4.4	Clock synchronization
	AU-8(1)	Time Stamps <i>Synchronization with Authoritative Time Source</i>	<i>No direct mapping.</i>	
<b><u>3.3.8</u></b> Protect audit information and audit logging tools from	AU-9	Protection of Audit Information	A.12.4.2	Protection of log information

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
unauthorized access, modification, and deletion.			A.12.4.3	Administrator and operator logs
			A.18.1.3	Protection of records
<a href="#">3.3.9</a> Limit management of audit logging functionality to a subset of privileged users.	AU-9(4)	Protection of Audit Information <i>Access by Subset of Privileged Users</i>	<i>No direct mapping.</i>	

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-4: MAPPING CONFIGURATION MANAGEMENT REQUIREMENTS TO CONTROLS<sup>32</sup>**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.4 CONFIGURATION MANAGEMENT</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.4.1</u></b> Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.  <b><u>3.4.2</u></b> Establish and enforce security configuration settings for information technology products employed in organizational systems.	CM-2	Baseline Configuration	<i>No direct mapping.</i>	
	CM-6	Configuration Settings	<i>No direct mapping.</i>	
	CM-8	System Component Inventory	A.8.1.1	Inventory of assets
			A.8.1.2	Ownership of assets
CM-8(1)	System Component Inventory <i>Updates During Installations / Removals</i>	<i>No direct mapping.</i>		
<b><i>Derived Security Requirements</i></b>				
<b><u>3.4.3</u></b> Track, review, approve or disapprove, and log changes to organizational systems.	CM-3	Configuration Change Control	A.12.1.2	Change management
			A.14.2.2	System change control procedures
			A.14.2.3	Technical review of applications after operating platform changes
			A.14.2.4	Restrictions on changes to software packages
<b><u>3.4.4</u></b> Analyze the security impact of changes prior to implementation.	CM-4	Security Impact Analysis	A.14.2.3	Technical review of applications after operating platform changes
<b><u>3.4.5</u></b> Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	CM-5	Access Restrictions for Change	A.9.2.3	Management of privileged access rights
			A.9.4.5	Access control to program source code
			A.12.1.2	Change management
			A.12.1.4	Separation of development, testing, and operational environments
			A.12.5.1	Installation of software on operational systems

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<sup>32</sup> CM-7(5), the least functionality whitelisting policy, is listed as an alternative to CM-7(4), the least functionality blacklisting policy, for organizations desiring greater protection for systems containing CUI. CM-7(5) is only required in federal systems at the high security control baseline in accordance with NIST Special Publication 800-53.

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<a href="#">3.4.6</a> Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	CM-7	Least Functionality	A.12.5.1*	Installation of software on operational systems
<a href="#">3.4.7</a> Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	CM-7(1)	Least Functionality <i>Periodic Review</i>	<i>No direct mapping.</i>	
	CM-7(2)	Least Functionality <i>Prevent program execution</i>	<i>No direct mapping.</i>	
<a href="#">3.4.8</a> Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	CM-7(4)	Least Functionality <i>Unauthorized Software / Blacklisting</i>	<i>No direct mapping.</i>	
	CM-7(5)	Least Functionality <i>Authorized Software / Whitelisting</i>	<i>No direct mapping.</i>	
<a href="#">3.4.9</a> Control and monitor user-installed software.	CM-11	User-Installed Software	A.12.5.1	Installation of software on operational systems
			A.12.6.2	Restrictions on software installation

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-5: MAPPING IDENTIFICATION AND AUTHENTICATION REQUIREMENTS TO CONTROLS<sup>33</sup>**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.5 IDENTIFICATION AND AUTHENTICATION</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.5.1</u></b> Identify system users, processes acting on behalf of users, and devices.	IA-2	Identification and Authentication (Organizational Users)	A.9.2.1	User registration and de-registration
	<b><u>3.5.2</u></b> Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	IA-3	Device Identification and Authentication	<i>No direct mapping.</i>
	IA-5	Authenticator Management	A.9.2.1	User registration and de-registration
			A.9.2.4	Management of secret authentication information of users
			A.9.3.1	Use of secret authentication information
			A.9.4.3	Password management system
<b><i>Derived Security Requirements</i></b>				
<b><u>3.5.3</u></b> Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1)	Identification and Authentication (Organizational Users) <i>Network Access to Privileged Accounts</i>	<i>No direct mapping.</i>	
	IA-2(2)	Identification and Authentication (Organizational Users) <i>Network Access to Non-Privileged Accounts</i>	<i>No direct mapping.</i>	
	IA-2(3)	Identification and Authentication (Organizational Users) <i>Local Access to Privileged Accounts</i>	<i>No direct mapping.</i>	
<b><u>3.5.4</u></b> Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA-2(8)	Identification and Authentication (Organizational Users) <i>Network Access to Privileged Accounts-Replay Resistant</i>	<i>No direct mapping.</i>	
	IA-2(9)	Identification and Authentication (Organizational Users) <i>Network Access to Non-Privileged Accounts-Replay Resistant</i>	<i>No direct mapping.</i>	

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<sup>33</sup> IA-2(8) is *not* currently in the NIST Special Publication 800-53 moderate security control baseline although it will be added to the baseline in the next update. Employing multifactor authentication without a replay-resistant capability for non-privileged accounts creates a significant vulnerability for systems transmitting CUI.



SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<a href="#">3.5.5</a> Prevent reuse of identifiers for a defined period.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration
<a href="#">3.5.6</a> Disable identifiers after a defined period of inactivity.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration
<a href="#">3.5.7</a> Enforce a minimum password complexity and change of characters when new passwords are created.	IA-5(1)	Authenticator Management <i>Password-Based Authentication</i>	<i>No direct mapping.</i>	
<a href="#">3.5.8</a> Prohibit password reuse for a specified number of generations.				
<a href="#">3.5.9</a> Allow temporary password use for system logons with an immediate change to a permanent password.				
<a href="#">3.5.10</a> Store and transmit only cryptographically-protected passwords.				
<a href="#">3.5.11</a> Obscure feedback of authentication information.	IA-6	Authenticator Feedback	A.9.4.2	Secure logon procedures

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-6: MAPPING INCIDENT RESPONSE REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.6 INCIDENT RESPONSE</u></b>				
<b><i>Basic Security Requirements</i></b>				
<p><b><u>3.6.1</u></b> Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.</p> <p><b><u>3.6.2</u></b> Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.</p>	IR-2	Incident Response Training	A.7.2.2*	Information security awareness, education, and training
	IR-4	Incident Handling	A.16.1.4	Assessment of and decision on information security events
			A.16.1.5	Response to information security incidents
			A.16.1.6	Learning from information security incidents
	IR-5	Incident Monitoring	<i>No direct mapping.</i>	
	IR-6	Incident Reporting	A.6.1.3	Contact with authorities
			A.16.1.2	Reporting information security events
IR-7	Incident Response Assistance	<i>No direct mapping.</i>		
<b><i>Derived Security Requirements</i></b>				
<b><u>3.6.3</u></b> Test the organizational incident response capability.	IR-3	Incident Response Testing	<i>No direct mapping.</i>	

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-7: MAPPING MAINTENANCE REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.7 MAINTENANCE</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.7.1</u></b> Perform maintenance on organizational systems.  <b><u>3.7.2</u></b> Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
			A.11.2.5*	Removal of assets
	MA-3	Maintenance Tools	<i>No direct mapping.</i>	
	MA-3(1)	Maintenance Tools <i>Inspect Tools</i>	<i>No direct mapping.</i>	
	MA-3(2)	Maintenance Tools <i>Inspect Media</i>	<i>No direct mapping.</i>	
<b><i>Derived Security Requirements</i></b>				
<b><u>3.7.3</u></b> Ensure equipment removed for off-site maintenance is sanitized of any CUI.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
			A.11.2.5*	Removal of assets
<b><u>3.7.4</u></b> Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	MA-3(2)	Maintenance Tools <i>Inspect Media</i>	<i>No direct mapping.</i>	
<b><u>3.7.5</u></b> Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	MA-4	Nonlocal Maintenance	<i>No direct mapping.</i>	
<b><u>3.7.6</u></b> Supervise the maintenance activities of maintenance personnel without required access authorization.	MA-5	Maintenance Personnel	<i>No direct mapping.</i>	

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-8: MAPPING MEDIA PROTECTION REQUIREMENTS TO CONTROLS<sup>34</sup>**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b>3.8 MEDIA PROTECTION</b>				
<b>Basic Security Requirements</b>				
<b>3.8.1</b> Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	MP-2	Media Access	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.11.2.9	Clear desk and clear screen policy
<b>3.8.2</b> Limit access to CUI on system media to authorized users.	MP-4	Media Storage	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.11.2.9	Clear desk and clear screen policy
<b>3.8.3</b> Sanitize or destroy system media containing CUI before disposal or release for reuse.	MP-6	Media Sanitization	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.8.3.2	Disposal of media
			A.11.2.7	Secure disposal or reuse of equipment
<b>Derived Security Requirements</b>				
<b>3.8.4</b> Mark media with necessary CUI markings and distribution limitations.	MP-3	Media Marking	A.8.2.2	Labelling of Information
<b>3.8.5</b> Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP-5	Media Transport	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.8.3.3	Physical media transfer
			A.11.2.5	Removal of assets
			A.11.2.6	Security of equipment and assets off-premises
<b>3.8.6</b> Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	MP-5(4)	Media Transport <i>Cryptographic Protection</i>	<i>No direct mapping.</i>	
<b>3.8.7</b> Control the use of removable media on system components.	MP-7	Media Use	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<sup>34</sup> CP-9, *Information System Backup*, is included with the Media Protection family since the Contingency Planning family was not included in the security requirements.

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<a href="#">3.8.8</a> Prohibit the use of portable storage devices when such devices have no identifiable owner.	MP-7(1)	Media Use <i>Prohibit Use Without Owner</i>	<i>No direct mapping.</i>	
<a href="#">3.8.9</a> Protect the confidentiality of backup CUI at storage locations.	CP-9	System Backup	A.12.3.1	Information backup
			A.17.1.2	Implementing information security continuity
			A.18.1.3	Protection of records

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-9: MAPPING PERSONNEL SECURITY REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.9 PERSONNEL SECURITY</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.9.1</u></b> Screen individuals prior to authorizing access to organizational systems containing CUI.	PS-3	Personnel Screening	A.7.1.1	Screening
<b><u>3.9.2</u></b> Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	PS-4	Personnel Termination	A.7.3.1	Termination or change of employment responsibilities
			A.8.1.4	Return of assets
	PS-5	Personnel Transfer	A.7.3.1	Termination or change of employment responsibilities
			A.8.1.4	Return of assets
<b><i>Derived Security Requirements</i></b>	None.			

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-10: MAPPING PHYSICAL PROTECTION REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.10 PHYSICAL PROTECTION</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.10.1</u></b> Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.  <b><u>3.10.2</u></b> Protect and monitor the physical facility and support infrastructure for organizational systems.	PE-2	Physical Access Authorizations	A.11.1.2*	Physical entry controls
	PE-4	Access Control for Transmission Medium	A.11.1.2	Physical entry controls
	PE-5	Access Control for Output Devices	A.11.2.3	Cabling security
			A.11.1.2	Physical entry controls
			A.11.1.3	Securing offices, rooms, and facilities
	PE-6	Monitoring Physical Access	<i>No direct mapping.</i>	
<b><i>Derived Security Requirements</i></b>				
<b><u>3.10.3</u></b> Escort visitors and monitor visitor activity.	PE-3	Physical Access Control	A.11.1.1	Physical security perimeter
<b><u>3.10.4</u></b> Maintain audit logs of physical access.			A.11.1.2	Physical entry controls
<b><u>3.10.5</u></b> Control and manage physical access devices.			A.11.1.3	Securing offices, rooms, and facilities
<b><u>3.10.6</u></b> Enforce safeguarding measures for CUI at alternate work sites.			PE-17	Alternate Work Site
	A.11.2.6	Security of equipment and assets off-premises		
	A.13.2.1	Information transfer policies and procedures		

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-11: MAPPING RISK ASSESSMENT REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.11 RISK ASSESSMENT</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.11.1</u></b> Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	RA-3	Risk Assessment	A.12.6.1*	Management of technical vulnerabilities
<b><i>Derived Security Requirements</i></b>				
<b><u>3.11.2</u></b> Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities
	RA-5(5)	Vulnerability Scanning <i>Privileged Access</i>	<i>No direct mapping.</i>	
<b><u>3.11.3</u></b> Remediate vulnerabilities in accordance with risk assessments.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>



**TABLE D-12: MAPPING SECURITY ASSESSMENT REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.12 SECURITY ASSESSMENT</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.12.1</u></b> Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	CA-2	Security Assessments	A.14.2.8	System security testing
			A.18.2.2	Compliance with security policies and standards
			A.18.2.3	Technical compliance review
<b><u>3.12.2</u></b> Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	CA-5	Plan of Action and Milestones	<i>No direct mapping.</i>	
	CA-7	Continuous Monitoring	<i>No direct mapping.</i>	
<b><u>3.12.3</u></b> Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.				
<b><u>3.12.4</u></b> Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	PL-2	System Security Plan	A.6.1.2	Information security coordination
<b><i>Derived Security Requirements</i></b>	None.			

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-13: MAPPING SYSTEM AND COMMUNICATIONS PROTECTION REQUIREMENTS TO CONTROLS<sup>35</sup>**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.13 SYSTEM AND COMMUNICATIONS PROTECTION</u></b>				
<b><i>Basic Security Requirements</i></b>				
<b><u>3.13.1</u></b> Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	SC-7	Boundary Protection	A.13.1.1	Network controls
			A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.3	Protecting application services transactions
<b><u>3.13.2</u></b> Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	SA-8	Security Engineering Principles	A.14.2.5	Secure system engineering principles
<b><i>Derived Security Requirements</i></b>				
<b><u>3.13.3</u></b> Separate user functionality from system management functionality.	SC-2	Application Partitioning	<i>No direct mapping.</i>	
<b><u>3.13.4</u></b> Prevent unauthorized and unintended information transfer via shared system resources.	SC-4	Information in Shared Resources	<i>No direct mapping.</i>	
<b><u>3.13.5</u></b> Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	SC-7	Boundary Protection	A.13.1.1	Network controls
			A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.3	Protecting application services transactions
<b><u>3.13.6</u></b> Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	SC-7(5)	Boundary Protection <i>Deny by Default / Allow by Exception</i>	<i>No direct mapping.</i>	

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<sup>35</sup> SA-8, *Security Engineering Principles*, is included with the System and Communications Protection family since the System and Services Acquisition family was not included in the security requirements.

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<a href="#">3.13.7</a> Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	SC-7(7)	Boundary Protection <i>Prevent Split Tunneling for Remote Devices</i>	<i>No direct mapping.</i>	
<a href="#">3.13.8</a> Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	SC-8	Transmission Confidentiality and Integrity	A.8.2.3	Handling of Assets
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.13.2.3	Electronic messaging
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
<a href="#">3.13.9</a> Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	SC-10	Network Disconnect	A.13.1.1	Network controls
<a href="#">3.13.10</a> Establish and manage cryptographic keys for cryptography employed in organizational systems.	SC-12	Cryptographic Key Establishment and Management	A.10.1.2	Key Management
<a href="#">3.13.11</a> Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC-13	Cryptographic Protection	A.10.1.1	Policy on the use of cryptographic controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.5	Regulation of cryptographic controls
<a href="#">3.13.12</a> Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	SC-15	Collaborative Computing Devices	A.13.2.1*	Information transfer policies and procedures
<a href="#">3.13.13</a> Control and monitor the use of mobile code.	SC-18	Mobile Code	<i>No direct mapping.</i>	

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<a href="#">3.13.14</a> Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	SC-19	Voice over Internet Protocol	<i>No direct mapping.</i>	
<a href="#">3.13.15</a> Protect the authenticity of communications sessions.	SC-23	Session Authenticity	<i>No direct mapping.</i>	
<a href="#">3.13.16</a> Protect the confidentiality of CUI at rest.	SC-28	Protection of Information at Rest	A.8.2.3*	Handling of Assets

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE D-14: MAPPING SYSTEM AND INFORMATION INTEGRITY REQUIREMENTS TO CONTROLS**

SECURITY REQUIREMENTS	NIST SP 800-53 <i>Relevant Security Controls</i>		ISO/IEC 27001 <i>Relevant Security Controls</i>	
<b><u>3.14 SYSTEM AND INFORMATION INTEGRITY</u></b>				
<b><i>Basic Security Requirements</i></b>				
<p><b><u>3.14.1</u></b> Identify, report, and correct system flaws in a timely manner.</p> <p><b><u>3.14.2</u></b> Provide protection from malicious code at designated locations within organizational systems.</p> <p><b><u>3.14.3</u></b> Monitor system security alerts and advisories and take action in response.</p>	SI-2	Flaw Remediation	A.12.6.1	Management of technical vulnerabilities
			A.14.2.2	System change control procedures
			A.14.2.3	Technical review of applications after operating platform changes
			A.16.1.3	Reporting information security weaknesses
	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
	SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*	Contact with special interest groups
<b><i>Derived Security Requirements</i></b>				
<p><b><u>3.14.4</u></b> Update malicious code protection mechanisms when new releases are available.</p> <p><b><u>3.14.5</u></b> Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.</p>	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
	SI-4(4)	System Monitoring <i>Inbound and Outbound Communications Traffic</i>	<i>No direct mapping.</i>	
<p><b><u>3.14.7</u></b> Identify unauthorized use of organizational systems.</p>	SI-4	System Monitoring	<i>No direct mapping.</i>	

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

## APPENDIX E

### TAILORING CRITERIA

#### LISTING OF MODERATE SECURITY CONTROL BASELINE AND TAILORING ACTIONS

This appendix provides a list of the security controls in the [SP 800-53]<sup>36</sup> moderate baseline, one of the sources along with [FIPS 200], used to develop the CUI security requirements described in Chapter Three. Tables E-1 through E-17 contain the specific tailoring actions that have been carried out on the controls in accordance with the tailoring criteria established by NIST and NARA. The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements.<sup>37</sup> There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government);
- The control or control enhancement is not directly related to protecting the confidentiality of CUI;<sup>38</sup> or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.<sup>39</sup>

The following symbols in Table E are used in Tables E-1 through E-17 to specify the tailoring actions taken or when no tailoring actions were required.

**TABLE E: TAILORING ACTION SYMBOLS**

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

<sup>36</sup> The security controls in Tables E-1 through E-14 are taken from NIST Special Publication 800-53, Revision 4. These tables will be updated upon publication of [SP 800-53B] which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements in Chapter Three.

<sup>37</sup> The same *tailoring criteria* were applied to the security requirements in [FIPS 200] resulting in the CUI basic security requirements described in Chapter Three.

<sup>38</sup> While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between the security objectives of confidentiality and integrity. Therefore, the security controls in the [SP 800-53] moderate baseline that support protection against unauthorized disclosure also support protection against unauthorized modification.

<sup>39</sup> The security controls tailored out of the moderate baseline (i.e., controls specifically marked as either NCO or NFO and highlighted in the darker blue shading in Tables E-1 through E-17), are often included as part of an organization's comprehensive security program.

**TABLE E-1: TAILORING ACTIONS FOR ACCESS CONTROLS**

<b>NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS</b>		<b>TAILORING ACTION</b>
AC-1	Access Control Policy and Procedures	NFO
AC-2	Account Management	CUI
AC-2(1)	<i>ACCOUNT MANAGEMENT / AUTOMATED SYSTEM ACCOUNT MANAGEMENT</i>	NCO
AC-2(2)	<i>ACCOUNT MANAGEMENT / REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS</i>	NCO
AC-2(3)	<i>ACCOUNT MANAGEMENT / DISABLE INACTIVE ACCOUNTS</i>	NCO
AC-2(4)	<i>ACCOUNT MANAGEMENT / AUTOMATED AUDIT ACTIONS</i>	NCO
AC-3	Access Enforcement	CUI
AC-4	Information Flow Enforcement	CUI
AC-5	Separation of Duties	CUI
AC-6	Least Privilege	CUI
AC-6(1)	<i>LEAST PRIVILEGE / AUTHORIZE ACCESS TO SECURITY FUNCTIONS</i>	CUI
AC-6(2)	<i>LEAST PRIVILEGE / NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS</i>	CUI
AC-6(5)	<i>LEAST PRIVILEGE / PRIVILEGED ACCOUNTS</i>	CUI
AC-6(9)	<i>LEAST PRIVILEGE / AUDITING USE OF PRIVILEGED FUNCTIONS</i>	CUI
AC-6(10)	<i>LEAST PRIVILEGE / PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS</i>	CUI
AC-7	Unsuccessful Logon Attempts	CUI
AC-8	System Use Notification	CUI
AC-11	Session Lock	CUI
AC-11(1)	<i>SESSION LOCK / PATTERN-HIDING DISPLAYS</i>	CUI
AC-12	Session Termination	CUI
AC-14	Permitted Actions without Identification or Authentication	FED
AC-17	Remote Access	CUI
AC-17(1)	<i>REMOTE ACCESS / AUTOMATED MONITORING / CONTROL</i>	CUI
AC-17(2)	<i>REMOTE ACCESS / PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION</i>	CUI
AC-17(3)	<i>REMOTE ACCESS / MANAGED ACCESS CONTROL POINTS</i>	CUI
AC-17(4)	<i>REMOTE ACCESS / PRIVILEGED COMMANDS / ACCESS</i>	CUI
AC-18	Wireless Access	CUI
AC-18(1)	<i>WIRELESS ACCESS / AUTHENTICATION AND ENCRYPTION</i>	CUI
AC-19	Access Control for Mobile Devices	CUI
AC-19(5)	<i>ACCESS CONTROL FOR MOBILE DEVICES / FULL DEVICE / CONTAINER-BASED ENCRYPTION</i>	CUI
AC-20	Use of External Systems	CUI
AC-20(1)	<i>USE OF EXTERNAL SYSTEMS / LIMITS ON AUTHORIZED USE</i>	CUI
AC-20(2)	<i>USE OF EXTERNAL SYSTEMS / PORTABLE STORAGE DEVICES</i>	CUI
AC-21	Information Sharing	FED
AC-22	Publicly Accessible Content	CUI

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-2: TAILORING ACTIONS FOR AWARENESS AND TRAINING CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
AT-1	Security Awareness and Training Policy and Procedures	NFO
AT-2	Security Awareness Training	CUI
AT-2(2)	<i>SECURITY AWARENESS / INSIDER THREAT</i>	CUI
AT-3	Role-Based Security Training	CUI
AT-4	Security Training Records	NFO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>



**TABLE E-3: TAILORING ACTIONS FOR AUDIT AND ACCOUNTABILITY CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
AU-1	Audit and Accountability Policy and Procedures	NFO
AU-2	Audit Events	CUI
AU-2(3)	<i>AUDIT EVENTS / REVIEWS AND UPDATES</i>	CUI
AU-3	Content of Audit Records	CUI
AU-3(1)	<i>CONTENT OF AUDIT RECORDS / ADDITIONAL AUDIT INFORMATION</i>	CUI
AU-4	Audit Storage Capacity	NCO
AU-5	Response to Audit Logging Process Failures	CUI
AU-6	Audit Review, Analysis, and Reporting	CUI
AU-6(1)	<i>AUDIT REVIEW, ANALYSIS, AND REPORTING / PROCESS INTEGRATION</i>	NCO
AU-6(3)	<i>AUDIT REVIEW, ANALYSIS, AND REPORTING / CORRELATE AUDIT REPOSITORIES</i>	CUI
AU-7	Audit Reduction and Report Generation	CUI
AU-7(1)	<i>AUDIT REDUCTION AND REPORT GENERATION / AUTOMATIC PROCESSING</i>	NCO
AU-8	Time Stamps	CUI
AU-8(1)	<i>TIME STAMPS / SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE</i>	CUI
AU-9	Protection of Audit Information	CUI
AU-9(4)	<i>PROTECTION OF AUDIT INFORMATION / ACCESS BY SUBSET OF PRIVILEGED USERS</i>	CUI
AU-11	Audit Record Retention	NCO
AU-12	Audit Generation	CUI

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-4: TAILORING ACTIONS FOR SECURITY ASSESSMENT AND AUTHORIZATION CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
CA-1	Security Assessment and Authorization Policies and Procedures	NFO
CA-2	Security Assessments	CUI
CA-2(1)	<i>SECURITY ASSESSMENTS / INDEPENDENT ASSESSORS</i>	NFO
CA-3	System Interconnections	NFO
CA-3(5)	<i>SYSTEM INTERCONNECTIONS / RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS</i>	NFO
CA-5	Plan of Action and Milestones	CUI
CA-6	Security Authorization	FED
CA-7	Continuous Monitoring	CUI
CA-7(1)	<i>CONTINUOUS MONITORING / INDEPENDENT ASSESSMENT</i>	NFO
CA-9	Internal System Connections	NFO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-5: TAILORING ACTIONS FOR CONFIGURATION MANAGEMENT CONTROLS<sup>40</sup>**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
CM-1	Configuration Management Policy and Procedures	NFO
CM-2	Baseline Configuration	CUI
CM-2(1)	<i>BASELINE CONFIGURATION   REVIEWS AND UPDATES</i>	NFO
CM-2(3)	<i>BASELINE CONFIGURATION   RETENTION OF PREVIOUS CONFIGURATIONS</i>	NCO
CM-2(7)	<i>BASELINE CONFIGURATION   CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS</i>	NFO
CM-3	Configuration Change Control	CUI
CM-3(2)	<i>CONFIGURATION CHANGE CONTROL   TEST / VALIDATE / DOCUMENT CHANGES</i>	NFO
CM-4	Security Impact Analysis	CUI
CM-5	Access Restrictions for Change	CUI
CM-6	Configuration Settings	CUI
CM-7	Least Functionality	CUI
CM-7(1)	<i>LEAST FUNCTIONALITY   PERIODIC REVIEW</i>	CUI
CM-7(2)	<i>LEAST FUNCTIONALITY   PREVENT PROGRAM EXECUTION</i>	CUI
CM-7(4)(5)	<i>LEAST FUNCTIONALITY   UNAUTHORIZED OR AUTHORIZED SOFTWARE / BLACKLISTING OR WHITELISTING</i>	CUI
CM-8	System Component Inventory	CUI
CM-8(1)	<i>SYSTEM COMPONENT INVENTORY   UPDATES DURING INSTALLATIONS / REMOVALS</i>	CUI
CM-8(3)	<i>SYSTEM COMPONENT INVENTORY   AUTOMATED UNAUTHORIZED COMPONENT DETECTION</i>	NCO
CM-8(5)	<i>SYSTEM COMPONENT INVENTORY   NO DUPLICATE ACCOUNTING OF COMPONENTS</i>	NFO
CM-9	Configuration Management Plan	NFO
CM-10	Software Usage Restrictions	NCO
CM-11	User-Installed Software	CUI

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<sup>40</sup> CM-7(5), Least Functionality *whitelisting*, is not in the moderate security control baseline in accordance with NIST Special Publication 800-53. However, it is offered as an optional and stronger policy alternative to *blacklisting*.

**TABLE E-6: TAILORING ACTIONS FOR CONTINGENCY PLANNING CONTROLS<sup>41</sup>**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
CP-1	Contingency Planning Policy and Procedures	NCO
CP-2	Contingency Plan	NCO
CP-2(1)	<i>CONTINGENCY PLAN   COORDINATE WITH RELATED PLANS</i>	NCO
CP-2(3)	<i>CONTINGENCY PLAN   RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS</i>	NCO
CP-2(8)	<i>CONTINGENCY PLAN   IDENTIFY CRITICAL ASSETS</i>	NCO
CP-3	Contingency Training	NCO
CP-4	Contingency Plan Testing	NCO
CP-4(1)	<i>CONTINGENCY PLAN TESTING   COORDINATE WITH RELATED PLANS</i>	NCO
CP-6	Alternate Storage Site	NCO
CP-6(1)	<i>ALTERNATE STORAGE SITE   SEPARATION FROM PRIMARY SITE</i>	NCO
CP-6(3)	<i>ALTERNATE STORAGE SITE   ACCESSIBILITY</i>	NCO
CP-7	Alternate Processing Site	NCO
CP-7(1)	<i>ALTERNATE PROCESSING SITE   SEPARATION FROM PRIMARY SITE</i>	NCO
CP-7(2)	<i>ALTERNATE PROCESSING SITE   ACCESSIBILITY</i>	NCO
CP-7(3)	<i>ALTERNATE PROCESSING SITE   PRIORITY OF SERVICE</i>	NCO
CP-8	Telecommunications Services	NCO
CP-8(1)	<i>TELECOMMUNICATIONS SERVICES   PRIORITY OF SERVICE PROVISIONS</i>	NCO
CP-8(2)	<i>TELECOMMUNICATIONS SERVICES   SINGLE POINTS OF FAILURE</i>	NCO
CP-9	System Backup	CUI
CP-9(1)	<i>SYSTEM BACKUP   TESTING FOR RELIABILITY / INTEGRITY</i>	NCO
CP-10	System Recovery and Reconstitution	NCO
CP-10(2)	<i>SYSTEM RECOVERY AND RECONSTITUTION   TRANSACTION RECOVERY</i>	NCO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<sup>41</sup> CP-9 is grouped with the security controls in the *Media Protection* family in Appendix D since the *Contingency Planning* family was not included in the security requirements.

**TABLE E-7: TAILORING ACTIONS FOR IDENTIFICATION AND AUTHENTICATION CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
IA-1	Identification and Authentication Policy and Procedures	NFO
IA-2	Identification and Authentication (Organizational Users)	CUI
IA-2(1)	<i>IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)   NETWORK ACCESS TO PRIVILEGED ACCOUNTS</i>	CUI
IA-2(2)	<i>IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)   NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS</i>	CUI
IA-2(3)	<i>IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)   LOCAL ACCESS TO PRIVILEGED ACCOUNTS</i>	CUI
IA-2(8)	<i>IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)   NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT</i>	CUI
IA-2(9)	<i>IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)   NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT</i>	CUI
IA-2(11)	<i>IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)   REMOTE ACCESS - SEPARATE DEVICE</i>	FED
IA-2(12)	<i>IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)   ACCEPTANCE OF PIV CREDENTIALS</i>	FED
IA-3	Device Identification and Authentication	CUI
IA-4	Identifier Management	CUI
IA-5	Authenticator Management	CUI
IA-5(1)	<i>AUTHENTICATOR MANAGEMENT   PASSWORD-BASED AUTHENTICATION</i>	CUI
IA-5(2)	<i>AUTHENTICATOR MANAGEMENT   PKI-BASED AUTHENTICATION</i>	FED
IA-5(3)	<i>AUTHENTICATOR MANAGEMENT   IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION</i>	FED
IA-5(11)	<i>AUTHENTICATOR MANAGEMENT   HARDWARE TOKEN-BASED AUTHENTICATION</i>	FED
IA-6	Authenticator Feedback	CUI
IA-7	Cryptographic Module Authentication	FED
IA-8	Identification and Authentication (Non-Organizational Users)	FED
IA-8(1)	<i>IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)   ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES</i>	FED
IA-8(2)	<i>IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)   ACCEPTANCE OF THIRD-PARTY CREDENTIALS</i>	FED
IA-8(3)	<i>IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)   USE OF FICAM-APPROVED PRODUCTS</i>	FED
IA-8(4)	<i>IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)   USE OF FICAM-ISSUED PROFILES</i>	FED

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-8: TAILORING ACTIONS FOR INCIDENT RESPONSE CONTROLS**

<b>NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS</b>		<b>TAILORING ACTION</b>
IR-1	Incident Response Policy and Procedures	NFO
IR-2	Incident Response Training	CUI
IR-3	Incident Response Testing	CUI
IR-3(2)	<i>INCIDENT RESPONSE TESTING   COORDINATION WITH RELATED PLANS</i>	NCO
IR-4	Incident Handling	CUI
IR-4(1)	<i>INCIDENT HANDLING   AUTOMATED INCIDENT HANDLING PROCESSES</i>	NCO
IR-5	Incident Monitoring	CUI
IR-6	Incident Reporting	CUI
IR-6(1)	<i>INCIDENT REPORTING   AUTOMATED REPORTING</i>	NCO
IR-7	Incident Response Assistance	CUI
IR-7(1)	<i>INCIDENT RESPONSE ASSISTANCE   AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT</i>	NCO
IR-8	Incident Response Plan	NFO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-9: TAILORING ACTIONS FOR MAINTENANCE CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
MA-1	System Maintenance Policy and Procedures	NFO
MA-2	Controlled Maintenance	CUI
MA-3	Maintenance Tools	CUI
MA-3(1)	<i>MAINTENANCE TOOLS   INSPECT TOOLS</i>	CUI
MA-3(2)	<i>MAINTENANCE TOOLS   INSPECT MEDIA</i>	CUI
MA-4	Nonlocal Maintenance	CUI
MA-4(2)	<i>NONLOCAL MAINTENANCE   DOCUMENT NONLOCAL MAINTENANCE</i>	NFO
MA-5	Maintenance Personnel	CUI
MA-6	Timely Maintenance	NCO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-10: TAILORING ACTIONS FOR MEDIA PROTECTION CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
MP-1	Media Protection Policy and Procedures	NFO
MP-2	Media Access	CUI
MP-3	Media Marking	CUI
MP-4	Media Storage	CUI
MP-5	Media Transport	CUI
MP-5(4)	<i>MEDIA TRANSPORT   CRYPTOGRAPHIC PROTECTION</i>	CUI
MP-6	Media Sanitization	CUI
MP-7	Media Use	CUI
MP-7(1)	<i>MEDIA USE   PROHIBIT USE WITHOUT OWNER</i>	CUI

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>



**TABLE E-11: TAILORING ACTIONS FOR PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PE-1	Physical and Environmental Protection Policy and Procedures	NFO
PE-2	Physical Access Authorizations	CUI
PE-3	Physical Access Control	CUI
PE-4	Access Control for Transmission Medium	CUI
PE-5	Access Control for Output Devices	CUI
PE-6	Monitoring Physical Access	CUI
PE-6(1)	<i>MONITORING PHYSICAL ACCESS / INTRUSION ALARMS / SURVEILLANCE EQUIPMENT</i>	NFO
PE-8	Visitor Access Records	NFO
PE-9	Power Equipment and Cabling	NCO
PE-10	Emergency Shutoff	NCO
PE-11	Emergency Power	NCO
PE-12	Emergency Lighting	NCO
PE-13	Fire Protection	NCO
PE-13(3)	<i>FIRE PROTECTION / AUTOMATIC FIRE SUPPRESSION</i>	NCO
PE-14	Temperature and Humidity Controls	NCO
PE-15	Water Damage Protection	NCO
PE-16	Delivery and Removal	NFO
PE-17	Alternate Work Site	CUI

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-12: TAILORING ACTIONS FOR PLANNING CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PL-1	Security Planning Policy and Procedures	NFO
PL-2	System Security Plan	CUI
PL-2(3)	<i>SYSTEM SECURITY PLAN / PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES</i>	NFO
PL-4	Rules of Behavior	NFO
PL-4(1)	<i>RULES OF BEHAVIOR / SOCIAL MEDIA AND NETWORKING RESTRICTIONS</i>	NFO
PL-8	Information Security Architecture	NFO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-13: TAILORING ACTIONS FOR PERSONNEL SECURITY CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PS-1	Personnel Security Policy and Procedures	NFO
PS-2	Position Risk Designation	FED
PS-3	Personnel Screening	CUI
PS-4	Personnel Termination	CUI
PS-5	Personnel Transfer	CUI
PS-6	Access Agreements	NFO
PS-7	Third-Party Personnel Security	NFO
PS-8	Personnel Sanctions	NFO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-14: TAILORING ACTIONS FOR RISK ASSESSMENT CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
RA-1	Risk Assessment Policy and Procedures	NFO
RA-2	Security Categorization	FED
RA-3	Risk Assessment	CUI
RA-5	Vulnerability Scanning	CUI
RA-5(1)	<i>VULNERABILITY SCANNING / UPDATE TOOL CAPABILITY</i>	NFO
RA-5(2)	<i>VULNERABILITY SCANNING / UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED</i>	NFO
RA-5(5)	<i>VULNERABILITY SCANNING / PRIVILEGED ACCESS</i>	CUI

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-15: TAILORING ACTIONS FOR SYSTEM AND SERVICES ACQUISITION CONTROLS<sup>42</sup>**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
SA-1	System and Services Acquisition Policy and Procedures	NFO
SA-2	Allocation of Resources	NFO
SA-3	System Development Life Cycle	NFO
SA-4	Acquisition Process	NFO
SA-4(1)	<i>ACQUISITION PROCESS   FUNCTIONAL PROPERTIES OF SECURITY CONTROLS</i>	NFO
SA-4(2)	<i>ACQUISITION PROCESS   DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS</i>	NFO
SA-4(9)	<i>ACQUISITION PROCESS   FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE</i>	NFO
SA-4(10)	<i>ACQUISITION PROCESS   USE OF APPROVED PIV PRODUCTS</i>	NFO
SA-5	System Documentation	NFO
SA-8	Security Engineering Principles	CUI
SA-9	External System Services	NFO
SA-9(2)	<i>EXTERNAL SYSTEMS   IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES</i>	NFO
SA-10	Developer Configuration Management	NFO
SA-11	Developer Security Testing and Evaluation	NFO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

<sup>42</sup> SA-8 is grouped with the security controls in the *System and Communications Protection* family in Appendix D since the *System and Services Acquisition* family was not included in the security requirements.

**TABLE E-16: TAILORING ACTIONS FOR SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
SC-1	System and Communications Protection Policy and Procedures	NFO
SC-2	Application Partitioning	CUI
SC-4	Information in Shared Resources	CUI
SC-5	Denial of Service Protection	NCO
SC-7	Boundary Protection	CUI
SC-7(3)	<i>BOUNDARY PROTECTION   ACCESS POINTS</i>	NFO
SC-7(4)	<i>BOUNDARY PROTECTION   EXTERNAL TELECOMMUNICATIONS SERVICES</i>	NFO
SC-7(5)	<i>BOUNDARY PROTECTION   DENY BY DEFAULT / ALLOW BY EXCEPTION</i>	CUI
SC-7(7)	<i>BOUNDARY PROTECTION   PREVENT SPLIT TUNNELING FOR REMOTE DEVICES</i>	CUI
SC-8	Transmission Confidentiality and Integrity	CUI
SC-8(1)	<i>TRANSMISSION CONFIDENTIALITY AND INTEGRITY   CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION</i>	CUI
SC-10	Network Disconnect	CUI
SC-12	Cryptographic Key Establishment and Management	CUI
SC-13	Cryptographic Protection	CUI
SC-15	Collaborative Computing Devices	CUI
SC-17	Public Key Infrastructure Certificates	FED
SC-18	Mobile Code	CUI
SC-19	Voice over Internet Protocol	CUI
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	NFO
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	NFO
SC-22	Architecture and Provisioning for Name/Address Resolution Service	NFO
SC-23	Session Authenticity	CUI
SC-28	Protection of Information at Rest	CUI
SC-39	Process Isolation	NFO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

**TABLE E-17: TAILORING ACTIONS FOR SYSTEM AND INFORMATION INTEGRITY CONTROLS**

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
SI-1	System and Information Integrity Policy and Procedures	NFO
SI-2	Flaw Remediation	CUI
SI-2(2)	<i>FLAW REMEDIATION   AUTOMATED FLAW REMEDIATION STATUS</i>	NCO
SI-3	Malicious Code Protection	CUI
SI-3(1)	<i>MALICIOUS CODE PROTECTION   CENTRAL MANAGEMENT</i>	NCO
SI-3(2)	<i>MALICIOUS CODE PROTECTION   AUTOMATIC UPDATES</i>	NCO
SI-4	System Monitoring	CUI
SI-4(2)	<i>SYSTEM MONITORING   AUTOMATED TOOLS FOR REAL-TIME ANALYSIS</i>	NCO
SI-4(4)	<i>SYSTEM MONITORING   INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC</i>	CUI
SI-4(5)	<i>SYSTEM MONITORING   SYSTEM-GENERATED ALERTS</i>	NFO
SI-5	Security Alerts, Advisories, and Directives	CUI
SI-7	Software, Firmware, and Information Integrity	NCO
SI-7(1)	<i>SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY   INTEGRITY CHECKS</i>	NCO
SI-7(7)	<i>SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY   INTEGRATION OF DETECTION AND RESPONSE</i>	NCO
SI-8	Spam Protection	NCO
SI-8(1)	<i>SPAM PROTECTION   CENTRAL MANAGEMENT</i>	NCO
SI-8(2)	<i>SPAM PROTECTION   AUTOMATIC UPDATES</i>	NCO
SI-10	Information Input Validation	NCO
SI-11	Error Handling	NCO
SI-12	Information Handling and Retention	FED
SI-16	Memory Protection	NFO

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-171r2>

# OAuth Standard



## Table of Contents

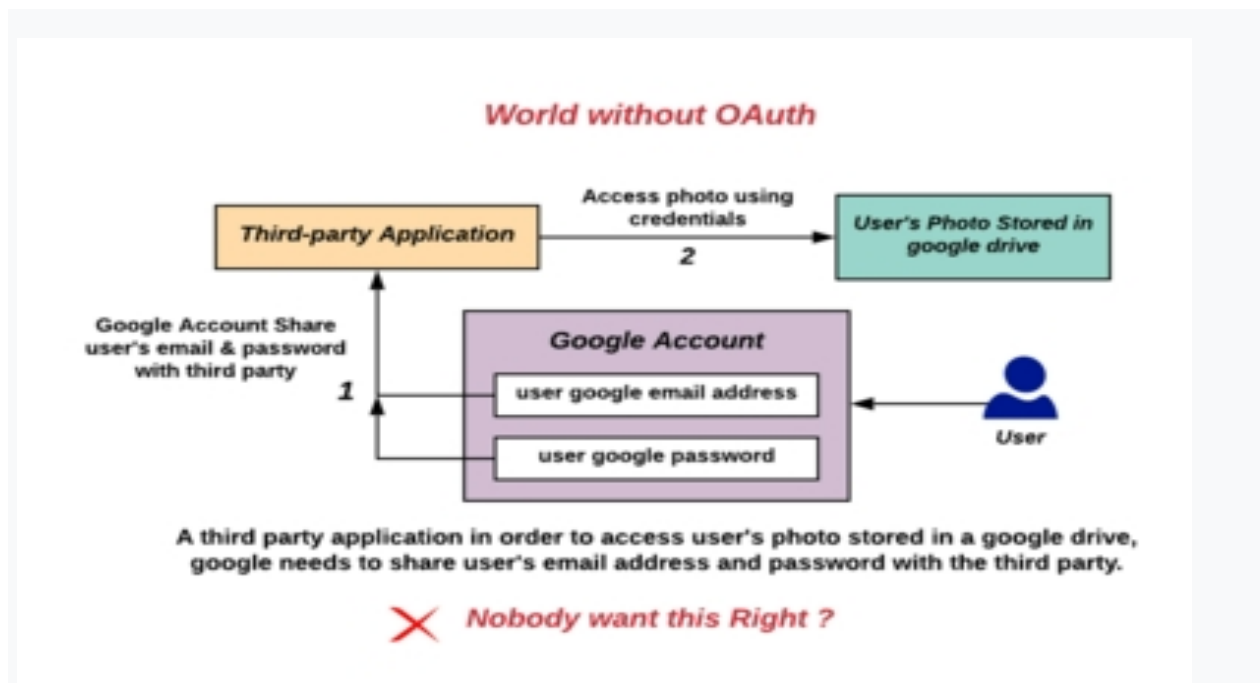
Introduction.....	1
Overview.....	1
History .....	1
Version History Security issues.....	1
Uses .....	1
OAuth and other standards .....	1
<b>OpenID vs. pseudo-authentication using OAuth</b> .....	<b>1</b>
OAuth and XACML .....	1
Controversy .....	1
See also.....	1
References .....	1
External links.....	1

## Introduction

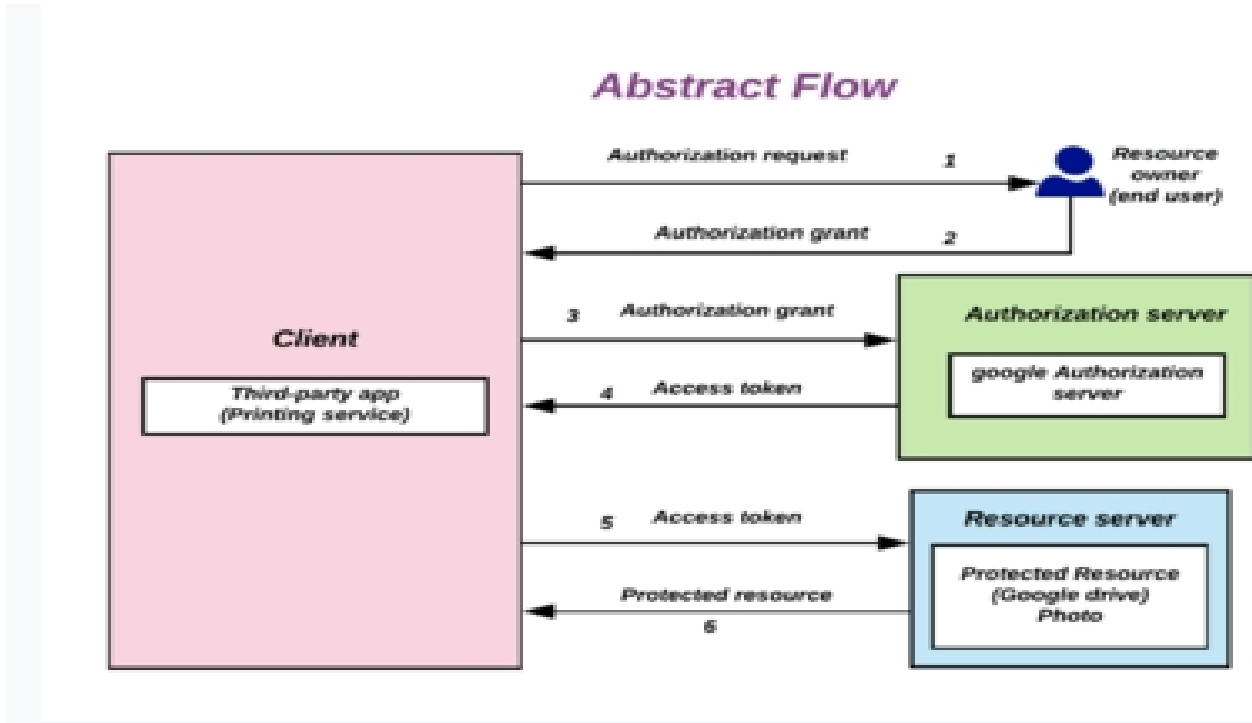
**OAuth** ("Open **A**uthorization"<sup>[1][2]</sup>) is an open standard for access delegation, commonly used as a way for internet users to grant websites or applications access to their information on other websites but without giving them the passwords.<sup>[3][4]</sup> This mechanism is used by companies such as Amazon,<sup>[5]</sup> Google, Facebook, Microsoft, and Twitter to permit the users to share information about their accounts with third-party applications or websites.

## Overview

Generally, OAuth provides clients a "secure delegated access" to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without providing credentials. Designed specifically to work with Hypertext Transfer Protocol (HTTP), OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner. The third party then uses the access token to access the protected resources hosted by the resource server.<sup>[2]</sup> In particular, OAuth 2.0 provides specific authorization flows for web applications, desktop applications, mobile phones, and smart devices.



A hypothetical authorization flow where login information is shared with a third-party application. This poses many security risks which can be prevented by the use of OAuth authorization flows.



A high-level overview of OAuth 2.0 flow. The resource owner credentials are used only on the authorization server, but not on the client (e.g. the third-party app).

## History



The OAuth logo, designed by American blogger [Chris Messina](#)

OAuth began in November 2006 when [Blaine Cook](#) was developing the [Twitter OpenID](#) implementation. Meanwhile, [Magnolia](#) needed a solution to allow its members with OpenIDs to authorize [Dashboard Widgets](#) to access their service. Cook, [Chris Messina](#) and Larry Halff from Magnolia met with [David Recordon](#) to discuss using OpenID with the Twitter and Magnolia [APIs](#) to delegate authentication. They concluded that there were no open standards for API access delegation.<sup>[6]</sup>

The OAuth [discussion group](#) was created in April 2007, for the small group of implementers to write the draft proposal for an open protocol. DeWitt Clinton from [Google](#) learned of the OAuth project, and expressed his

interest in supporting the effort. In July 2007, the team drafted an initial specification. Eran Hammer joined and coordinated the many OAuth contributions creating a more formal specification. On 4 December 2007, the OAuth Core 1.0 final draft was released.<sup>[2]</sup>

At the 73rd Internet Engineering Task Force (IETF) meeting in Minneapolis in November 2008, an OAuth BoF was held to discuss bringing the protocol into the IETF for further standardization work. The event was well attended and there was wide support for formally chartering an OAuth working group within the IETF.

The OAuth 1.0 protocol was published as RFC 5849, an informational Request for Comments, in April 2010. Since 31 August 2010, all third party Twitter applications have been required to use OAuth.<sup>[8]</sup>

The OAuth 2.0 framework was published considering additional use cases and extensibility requirements gathered from the wider IETF community. Albeit being built on the OAuth 1.0 deployment experience, OAuth 2.0 is not backwards compatible with OAuth 1.0. OAuth 2.0 was published as RFC 6749 and the Bearer Token Usage as RFC 6750, both standards track Requests for Comments, in October 2012.<sup>[2][9]</sup>

The OAuth 2.1 Authorization Framework is in draft stage and consolidates the functionality in the RFCs OAuth 2.0, OAuth 2.0 for Native Apps, Proof Key for Code Exchange, OAuth 2.0 for Browser-Based Apps, OAuth Security Best Current and Bearer Token Usage.<sup>[10]</sup>

## Version History Security issues

### OAuth 1.0

On 23 April 2009, a session fixation security flaw in the 1.0 protocol was announced. It affects the OAuth authorization flow (also known as "3-legged OAuth") in OAuth Core 1.0 Section 6.<sup>[11]</sup> Version 1.0a of the OAuth Core protocol was issued to address this issue.<sup>[12]</sup>

### OAuth 2.0

In January 2013, the Internet Engineering Task Force published a threat model for OAuth 2.0.<sup>[13]</sup> Among the threats outlined is one called "Open Redirector"; in early 2014, a variant of this was described under the name "Covert Redirect" by Wang Jing.<sup>[14][15][16][17]</sup>

OAuth 2.0 has been analyzed using formal web protocol analysis. This analysis revealed that in setups with multiple authorization servers, one of which is behaving maliciously, clients can become confused about the authorization server to use and may forward secrets to the malicious authorization server (AS Mix-Up Attack).<sup>[18]</sup> This prompted the creation of a new best current practice internet draft that sets out to define a new security standard for OAuth 2.0.<sup>[19]</sup> Assuming a fix against the AS Mix-Up Attack in place, the security of OAuth 2.0 has been proven under strong attacker models using formal analysis.<sup>[18]</sup>

One implementation of OAuth 2.0 with numerous security flaws has been exposed.<sup>[20]</sup>

In April and May 2017, about one million users of Gmail (less than 0.1% of users as of May 2017) were targeted by an OAuth-based phishing attack, receiving an email purporting to be from a colleague, employer or friend wanting to share a document on Google Docs.<sup>[21]</sup> Those who clicked on the link within the email were directed to sign in and allow a potentially malicious third-party program called "Google Apps" to access their "email account, contacts and online documents".<sup>[21]</sup> Within "approximately one hour",<sup>[21]</sup> the phishing attack was stopped by Google, who advised those who had given "Google Apps" access to their email to revoke such access and change their passwords.

In the draft of OAuth 2.1 the use of the PKCE extension for native apps has been recommended to all kinds of OAuth clients, including web applications and other confidential clients in order to avoid malicious browser extensions to perform OAuth 2.0 code injection attack.<sup>[10]</sup>

## Uses

Facebook's [Graph API](#) only supports OAuth 2.0.<sup>[22]</sup> [Google](#) supports OAuth 2.0 as the recommended authorization mechanism for all of its [APIs](#).<sup>[23]</sup> [Microsoft](#) also supports OAuth 2.0 for various APIs and its Azure Active Directory service,<sup>[24]</sup> which is used to secure many Microsoft and third party APIs.

OAuth can be used as an authorizing mechanism to access secured [RSS/Atom](#) feeds. Access to RSS/ATOM feeds that require authentication has always been an issue. For example, an RSS feed from a secured [Google Site](#) could not have been accessed using [Google Reader](#). Instead, three-legged OAuth would have been used to authorize that RSS client to access the feed from the Google Site.

## OAuth and other standards

OAuth is a service that is complementary to and distinct from [OpenID](#). OAuth is unrelated to [OATH](#), which is a reference architecture for authentication, not a standard for authorization. However, OAuth is directly related to [OpenID Connect](#) (OIDC), since OIDC is an authentication layer built on top of OAuth 2.0. OAuth is also unrelated to [XACML](#), which is an authorization policy standard. OAuth can be used in conjunction with XACML, where OAuth is used for ownership consent and access delegation whereas XACML is used to define the authorization policies (e.g., managers can view documents in their region).

## OpenID vs. pseudo-authentication using Oauth

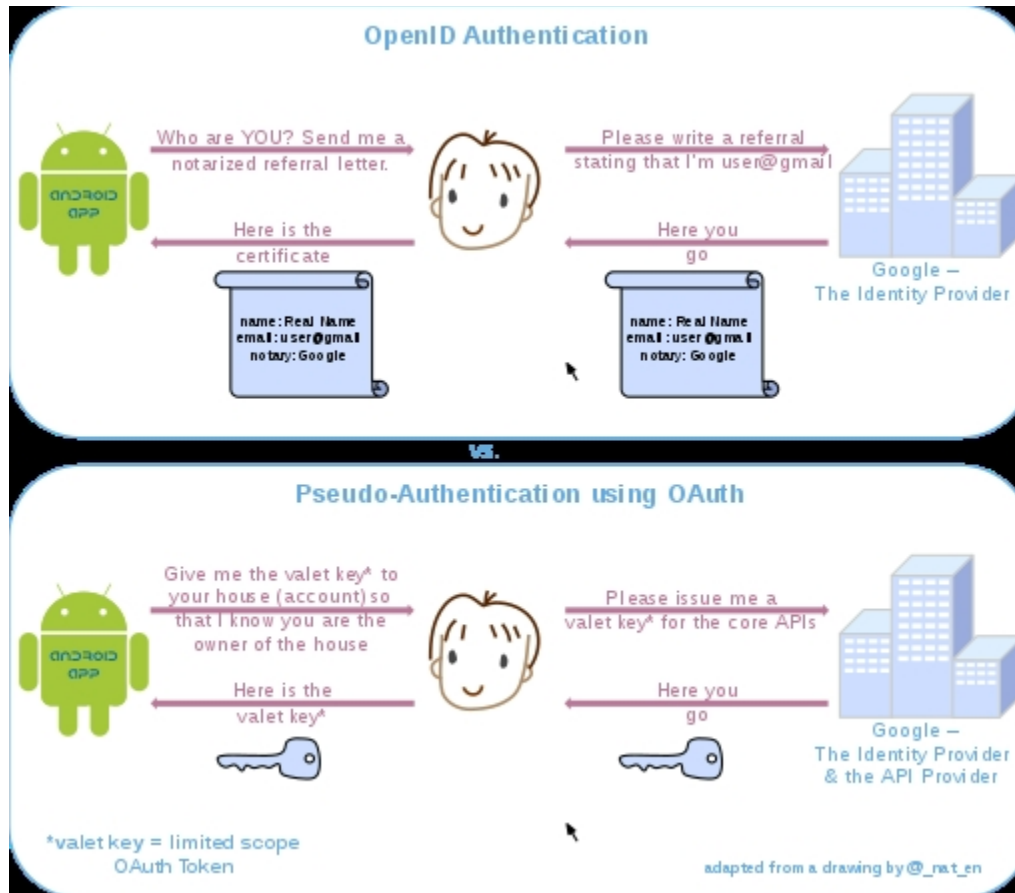
OAuth is an *authorization* protocol, rather than an *authentication* protocol. Using OAuth on its own as an authentication method may be referred to as pseudo-authentication. The following diagrams highlight the differences between using [OpenID](#) (specifically designed as an authentication protocol) and OAuth for authorization.

The communication flow in both processes is similar:

1. (Not pictured) The user requests a resource or site login from the application.
2. The site sees that the user is not authenticated. It formulates a request for the identity provider, encodes it, and sends it to the user as part of a redirect URL.
3. The user's browser makes a request to the redirect URL for the identity provider, including the application's request
4. If necessary, the identity provider authenticates the user (perhaps by asking them for their username and password)
5. Once the identity provider is satisfied that the user is sufficiently authenticated, it processes the application's request, formulates a response, and sends that back to the user along with a redirect URL back to the application.
6. The user's browser requests the redirect URL that goes back to the application, including the identity provider's response
7. The application decodes the identity provider's response, and carries on accordingly.
8. (OAuth only) The response includes an access token which the application can use to gain direct access to the identity provider's services on the user's behalf.

The crucial difference is that in the OpenID *authentication* use case, the response from the identity provider is an assertion of identity; while in the OAuth *authorization* use case, the identity provider is also an [API](#) provider, and the response from the identity provider is an access token that may grant the application ongoing access to some of the identity provider's APIs, on the user's behalf. The access token acts as a kind of "valet key" that the application can include with its requests to the identity provider, which prove that it has permission from the user to access those [APIs](#).

Because the identity provider typically (but not always) authenticates the user as part of the process of granting an OAuth access token, it is tempting to view a successful OAuth access token request as an authentication method itself. However, because OAuth was not designed with this use case in mind, making this assumption can lead to major security flaws.<sup>[25]</sup>



## OAuth and XACML

XACML is a policy-based, attribute-based access control authorization framework. It provides:

- An access control architecture.
- A policy language with which to express a wide range of access control policies including policies that can use consents handled / defined via OAuth.
- A request / response scheme to send and receive authorization requests.

XACML and OAuth can be combined to deliver a more comprehensive approach to authorization. OAuth does not provide a policy language with which to define access control policies. XACML can be used for its policy language.

Where OAuth focuses on delegated access (I, the user, grant Twitter access to my Facebook wall), and identity-centric authorization, XACML takes an attribute-based approach which can consider attributes of the user, the action, the resource, and the context (who, what, where, when, how). With XACML it is possible to define policies such as

- Managers can view documents in their department

- Managers can edit documents they own in draft mode

XACML provides more fine-grained access control than OAuth does. OAuth is limited in granularity to the coarse functionality (the scopes) exposed by the target service. As a result, it often makes sense to combine OAuth and XACML together where OAuth will provide the delegated access use case and consent management and XACML will provide the authorization policies that work on the applications, processes, and data.

Lastly, XACML can work transparently across multiple stacks (APIs, web SSO, ESBs, home-grown apps, databases...). OAuth focuses exclusively on HTTP-based apps.

## Controversy

Eran Hammer resigned from his role of lead author for the OAuth 2.0 project, withdrew from the IETF working group, and removed his name from the specification in July 2012. Hammer cited a conflict between web and enterprise cultures as his reason for leaving, noting that IETF is a community that is "all about enterprise use cases" and "not capable of simple". "What is now offered is a blueprint for an authorization protocol", he noted, "that is the enterprise way", providing a "whole new frontier to sell consulting services and integration solutions".<sup>[26]</sup> In comparing OAuth 2.0 with OAuth 1.0, Hammer points out that it has become "more complex, less interoperable, less useful, more incomplete, and most importantly, less secure". He explains how architectural changes for 2.0 unbound tokens from clients, removed all signatures and cryptography at a protocol level and added expiring tokens (because tokens could not be revoked) while complicating the processing of authorization. Numerous items were left unspecified or unlimited in the specification because "as has been the nature of this working group, no issue is too small to get stuck on or leave open for each implementation to decide."<sup>[26]</sup>

David Recordon later also removed his name from the specifications for unspecified reasons.<sup>[citation needed]</sup> Dick Hardt took over the editor role, and the framework was published in October 2012.<sup>[2]</sup>

An email software developer has criticised OAuth 2.0 as "an absolute dog's breakfast", requiring developers to write custom modules specific to each service (Gmail, Microsoft Mail services, etc.), and to register specifically with them.<sup>[27]</sup>

## See also

- List of OAuth providers
- Data portability
- IndieAuth
- Mozilla Persona
- OpenID
- SAML
- XACML
- User-Managed Access

## References

1. <sup>^</sup> "Open Authorization - Glossary | CSRC" csrc.nist.gov.
2. <sup>^</sup> Jump up to:<sup>a b c d</sup> Hardt, Dick (October 2012). "RFC6749 - The OAuth 2.0 Authorization Framework". *Internet Engineering Task Force*. Archived from the original on 15 October 2012. Retrieved 10 October 2012.

3. [Whitson, Gordon. "Understanding OAuth: What Happens When You Log Into a Site with Google, Twitter, or Facebook". Lifehacker. Archived from the original on 24 April 2014. Retrieved 15 May 2016.](#)
4. [Henry, Gavin \(January 2020\). "Justin Richer on OAuth". IEEE Software. 37 \(1\): 98–100. doi:10.1109/MS.2019.2949648. ISSN 0740-7459.](#)
5. ["Amazon & OAuth 2.0". Archived from the original on 8 December 2017. Retrieved 15 December 2017.](#)
6. ["Introduction" oauth.net. Archived from the original on 21 November 2018. Retrieved 21 November 2018.](#)
7. ["OAuth Core 1.0". 4 December 2007. Archived from the original on 25 November 2015. Retrieved 16 October 2014.](#)
8. [Chris Crum \(31 August 2010\). "Twitter Apps Go OAuth Today" WebProNews.com. Archived from the original on 31 July 2017. Retrieved 31 July 2017.](#)
9. [Jones, Michael; Hardt, Dick \(October 2012\). "RFC6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage". Internet Engineering Task Force. Archived from the original on 15 October 2012. Retrieved 10 October 2012.](#)
10. [Jump up to:<sup>a</sup> <sup>b</sup> Lodderstedt, Torsten; Hardt, Dick; Parecki, Aaron. "The OAuth 2.1 Authorization Framework" tools.ietf.org. Retrieved 22 November 2020.](#)
11. ["OAuth Security Advisory: 2009.1" oauth.net. 23 April 2009. Archived from the original on 27 May 2016. Retrieved 23 April 2009.](#)
12. ["OAuth Core 1.0a" oauth.net. Archived from the original on 30 June 2009. Retrieved 17 July 2009.](#)
13. [Lodderstedt, Torsten; McGloin, Mark; Hunt, Phil \(January 2013\). "RFC6819 - OAuth 2.0 Threat Model and Security Considerations". Internet Engineering Task Force. Archived from the original on 30 June 2020. Retrieved 29 June 2020. \[rfc:6819 OAuth 2.0 Threat Model and Security Considerations\]. Internet Engineering Task Force. Accessed January 2015.](#)
14. ["OAuth Security Advisory: 2014.1 "Covert Redirect"" oauth.net. 4 May 2014. Archived from the original on 21 November 2015. Retrieved 10 November 2014.](#)
15. ["Serious security flaw in OAuth, OpenID discovered". CNET. 2 May 2014. Archived from the original on 2 November 2015. Retrieved 10 November 2014.](#)
16. ["Math student detects OAuth, OpenID security vulnerability". Phys.org. 3 May 2014. Archived from the original on 6 November 2015. Retrieved 11 November 2014.](#)
17. ["Covert Redirect". Tetrapph. 1 May 2014. Archived from the original on 10 March 2016. Retrieved 10 November 2014.](#)
18. [Jump up to:<sup>a</sup> <sup>b</sup> Fett, Daniel; Küsters, Ralf; Schmitz, Guido \(2016\). "A Comprehensive Formal Security Analysis of OAuth 2.0". Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16. New York, New York, USA: ACM Press: 1204–1215. arXiv:1601.01229. Bibcode:2016arXiv160101229F. doi:10.1145/2976749.2978385. ISBN 9781450341394. S2CID 1723789.](#)
19. [Bradley, John; Labunets, Andrey; Lodderstedt, Torsten; Fett, Daniel. "OAuth 2.0 Security Best Current Practice". Internet Engineering Task Force. Archived from the original on 17 January 2020. Retrieved 29 July 2019.](#)
20. ["Hacking Facebook with OAuth 2.0 and Chrome". 12 February 2013. Archived from the original on 23 April 2016. Retrieved 6 March 2013.](#)
21. [Jump up to:<sup>a</sup> <sup>b</sup> <sup>c</sup> "Google Docs phishing email 'cost Minnesota \\$90,000". BBC News. 8 May 2017. Archived from the original on 30 June 2020. Retrieved 29 June 2020.](#)
22. ["Authentication - Facebook Developers". Facebook for Developers. Archived from the original on 23 January 2014. Retrieved 5 January 2020.](#)
23. ["Using OAuth 2.0 to Access Google APIs | Google Identity Platform". Google Developers. Archived from the original on 4 January 2020. Retrieved 4 January 2020.](#)
24. ["v2.0 Protocols - OAuth 2.0 Authorization Code Flow". Microsoft Docs. Archived from the original on 29 June 2020. Retrieved 29 June 2020.](#)
25. ["End User Authentication with OAuth 2.0" oauth.net. Archived from the original on 19 November 2015. Retrieved 8 March 2016.](#)



26. ^ Jump up to:<sup>a</sup> <sup>b</sup> Hammer, Eran (28 July 2012). "[OAuth 2.0 and the Road to Hell](#)". Hueniverse. Archived from [the original](#) on 25 March 2013. Retrieved 17 January 2018.
27. ^ Harris, David (October 2021). "[Pegasus Mail and Mercury Developer News](#)". Pegasus Mail.

## External links

- [Official website](#)
- [The Complete Guide to OAuth 2.0 and OpenID Connect Protocols](#)
- [OAuth Working Group's Mailing List](#)
- [The OAuth 1.0 Protocol \(RFC 5849\)](#)
- [The OAuth 2.0 Authorization Framework \(RFC 6749\)](#)
- [The OAuth 2.0 Authorization Framework: Bearer Token Usage \(RFC 6750\)](#)
- [The OAuth 2.1 Authorization Framework draft-ietf-oauth-v2-1-00](#)
- [OAuth 2.0 Authorization Flows diagrams](#)
- [OAuth Beginner's Guide and Resource Center by Hueniverse at the Wayback Machine](#) (archived February 20, 2017)
- [OAuth end points cheat sheet](#)
- [OAuth with Spring framework integration](#)
- [Illustration of OAuth 2.0 code injection attack](#)

of authentication technologies, with the aim of lowering costs and simplifying their functions.

# GREEN BUTTON COST-BENEFIT ANALYSIS REPORT



Submitted to: **ONTARIO MINISTRY OF ENERGY**  
Conservation and Energy Efficiency Branch

Prepared by:



Revised: October 2017



## TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>1</b>
<b>COST-BENEFIT ANALYSES .....</b>	<b>2</b>
OVERVIEW .....	2
BENEFIT-COST RATIOS .....	3
ALTERNATIVES .....	3
LIMITATIONS .....	3
<i>Benefit-Cost Ratios</i> .....	3
<i>Level of Granularity</i> .....	4
<i>Research Sources</i> .....	4
<b>GREEN BUTTON COST-BENEFIT ANALYSIS .....</b>	<b>9</b>
STAKEHOLDER GROUPS .....	9
QUANTITATIVE AND QUALITATIVE BENEFITS .....	10
SCENARIOS.....	10
GENERAL INPUTS AND ASSUMPTIONS.....	11
<i>Utility Type</i> .....	11
<i>Additional Inputs</i> .....	13
<i>A Note About Net-Present Value Calculations and Societal Discount Rate</i> .....	13
COSTS OF A GREEN BUTTON IMPLEMENTATION.....	16
<i>Cost Categories, Definitions and Applicability</i> .....	17
<i>Cost Inputs, Sources and Assumptions</i> .....	20
BENEFITS OF A GREEN BUTTON IMPLEMENTATION.....	24
<i>Benefit Categories, Definitions and Applicability</i> .....	24
<i>Benefit Inputs, Sources and Assumptions</i> .....	27
<i>Penetration Level</i> .....	33
<b>RESULTS OF THE ANALYSIS.....</b>	<b>35</b>
<i>Green Button Options</i> .....	35
<i>Utility Type</i> .....	36
<i>Implementation Type</i> .....	37
<b>KEY SCENARIOS.....</b>	<b>40</b>
SCENARIO 1: SINGLE INTEGRATED/MULTI-INTEGRATED HOSTED DMD/CMD (ELECTRICITY AND NATURAL GAS ONLY) .....	40
<i>Scenario 1A: Single Integrated Hosted DMD/CMD (Electricity and Natural Gas Utilities Only)</i> .....	41
<i>Scenario 1B: Multi-Integrated Hosted DMD/CMD (Electricity and Natural Gas Utilities Only)</i> .....	45
SCENARIO 2: SINGLE INTEGRATED/MULTI-INTEGRATED HOSTED DMD/CMD: ELECTRICITY, NATURAL GAS AND WATER .....	49
<i>Scenario 2A: Single Integrated Hosted DMD/CMD (All Utility Types)</i> .....	50
<i>Scenario 2B: Multi-Integrated Hosted DMD/CMD (All Utility Types)</i> .....	54
DIRECT AND INDIRECT COSTS.....	58
QUALITATIVE BENEFITS.....	63
<b>CONCLUSION .....</b>	<b>65</b>
<b>APPENDIX A: COST-BENEFIT ANALYSIS RESULTS SLIDE DECK.....</b>	<b>66</b>

**APPENDIX B: COST-BENEFIT ANALYSIS INPUT ASSUMPTIONS..... 67**

**APPENDIX C: COSTS AND BENEFITS OVERVIEW TABLE ..... 68**

**APPENDIX D: CONSERVATION METHODOLOGY ..... 69**

**APPENDIX E: ADDITIONAL SCENARIO ANALYSIS ..... 70**

    SCENARIO 1B: MULTI-INTEGRATED HOSTED DMD/CMD (ELECTRICITY AND NATURAL GAS UTILITIES ONLY). **ERROR! BOOKMARK NOT DEFINED.**

    SCENARIO 2B: MULTI-INTEGRATED HOSTED DMD/CMD (ALL UTILITY TYPES)..... **ERROR! BOOKMARK NOT DEFINED.**

    DIRECT AND INDIRECT COSTS..... **ERROR! BOOKMARK NOT DEFINED.**

    ADDITIONAL COST-BENEFIT RATIO RESULTS FOR THE MULTI-INTEGRATED HOSTED SCENARIOS ..... **ERROR! BOOKMARK NOT DEFINED.**

**LIST OF FIGURES**

Figure 1. Cost-Benefit Analysis Scenarios ..... 11

Figure 2. Adoption curves based on Rogers’ Diffusion of Innovation Algorithm ..... 33

**LIST OF TABLES**

Table 1. Grouping of Costs and Benefits..... 10

Table 2. Green Button Option Definitions ..... 10

Table 3. Utility Input Assumptions..... 12

Table 4. General Inputs..... 14

Table 5. Cost Categories, Definitions and Applicability ..... 18

Table 6. Cost Inputs, Sources and Assumptions ..... 21

Table 7. Benefit Categories, Definitions and Applicability..... 25

Table 8. Benefit Inputs, Sources and Assumptions..... 28

Table 9. Penetration curves included in the analysis..... 34

Table 10. Green Button DMD Scenario Cost-Benefit Results ..... 35

Table 11. Green Button DMD/CMD Scenario Cost-Benefit Results..... 36

Table 12. Green Button Implementation for Water Utilities Only ..... 37

Table 14. Green Button Implementation Type Cost-Benefit Results..... 39

Table 15. Scenario 1A Cost Details..... 41

Table 16. Scenario 1A Benefits Details ..... 42

Table 17. Scenario 1A Benefit-Cost Ratios..... 43

Table 18. Scenario 1A Energy and GHG Cumulative Impacts ..... 43

Table 19. Scenario 1A Costs by Stakeholder Groups (5-year horizon) ..... 43

Table 20. Scenario 1A Benefits by Stakeholder Group (5-year horizon) ..... 44

Table 21. Scenario 1B Cost Details..... 45

Table 22. Scenario 1B Benefits Details..... 46

Table 23. Scenario 1B Benefit-Cost Ratios ..... 47

Table 24. Scenario 1B Energy and GHG Cumulative Impacts ..... 47

Table 25. Scenario 1B Costs by Stakeholder Group (5-year horizon) ..... 47

Table 26. Scenario 1B Benefits by Stakeholder Group (5-year horizon)..... 48

Table 27. Scenario 2A Cost Details..... 50

Table 28. Scenario 2A Benefits Details ..... 51

Table 29. Scenario 2A Benefit-Cost Ratios.....	52
Table 30. Scenario 2A Energy and GHG Cumulative Impacts .....	52
Table 31. Scenario 2A Costs by Stakeholder Group (5-year horizon) .....	53
Table 32. Scenario 2A Benefits by Stakeholder Group (5-year horizon) .....	53
Table 33. Scenario 2B Cost Details.....	54
Table 34. Scenario 2B Benefits Details.....	55
Table 35. Scenario 2B Benefit-Cost Ratios .....	55
Table 36. Scenario 2B Energy and GHG Cumulative Impacts .....	56
Table 37. Scenario 2B Costs by Stakeholder Group (5-year horizon) .....	56
Table 38. Scenario 2B Benefits by Stakeholder Group (5-year horizon).....	57
Table 39. Total Benefits and Costs, Combining Direct and Indirect (5-year horizon).....	59
Table 40. Breakout of Direct and Indirect Benefits and Costs, Single- and Multi-Integrated (5-year horizon).....	60
Table 41. Breakout of Direct and Indirect Benefits and Costs, Non-Integrated and In-House (5-year horizon).....	60
Table 42. Total Benefits and Costs, Combining Direct and Indirect (10-year horizon).....	61
Table 43. Breakout of Direct and Indirect Benefits and Costs, Single and Multi-Integrated (10-year horizon).....	62
Table 44. Breakout of Direct and Indirect Benefits and Costs, Non-Integrated and In-House (10-year horizon).....	62
Table 44. Scenario 1B Cost Details.....	<b>Error! Bookmark not defined.</b>
Table 45. Scenario 1B Benefits Details.....	<b>Error! Bookmark not defined.</b>
Table 46. Scenario 1B Benefit-Cost Ratios .....	<b>Error! Bookmark not defined.</b>
Table 47. Scenario 1B Costs by Stakeholder Group (5-year horizon) .....	<b>Error! Bookmark not defined.</b>
Table 48. Scenario 1B Benefits by Stakeholder Group (5-year horizon).....	<b>Error! Bookmark not defined.</b>
Table 49. Scenario 2B Cost Details.....	<b>Error! Bookmark not defined.</b>
Table 50. Scenario 2B Benefits Details.....	<b>Error! Bookmark not defined.</b>
Table 51. Scenario 2B Benefit-Cost Ratios .....	<b>Error! Bookmark not defined.</b>
Table 52. Scenario 2B Costs by Stakeholder Group (5-year horizon) .....	<b>Error! Bookmark not defined.</b>
Table 53. Scenario 2B Benefits by Stakeholder Group (5-year horizon).....	<b>Error! Bookmark not defined.</b>
Table 54. Breakout of Direct and Indirect Benefits and Costs, Single and Multi-Integrated (10-year horizon).....	<b>Error! Bookmark not defined.</b>
Table 55. Green Button DMD/CMD Multi-Integrated Scenario Cost-Benefit Results..	<b>Error! Bookmark not defined.</b>



## INTRODUCTION

Ontario's Ministry of Energy has hired Dunsky Energy Consulting to support its efforts in developing policy recommendations for the potential implementation of Green Button for electricity, natural gas, and water utilities in Ontario. Specifically, our team is conducting a cost-benefit analysis and facilitating stakeholder consultations on behalf of the Ministry. The Ministry is taking on an exciting leadership role in this area, as no jurisdiction has attempted a quantified cost-benefit analysis of the Green Button standard to date.

This report includes the following information:

- The **cost-benefit analysis report**, which outlines how the Green Button cost-benefit analysis was developed including:
  - **Overview of cost-benefit analyses in general:** principles, strengths, and limitations of cost-benefit analyses (not Green-Button-specific);
  - **Green-Button cost-benefit analysis assumptions:** generic assumptions and inputs used in our modelling (not scenario-specific); and
  - **Key scenarios:** assumptions and inputs used in our modelling related to specific scenarios.
- **Appendix A** includes the Cost-Benefit Analysis slide deck, which was presented to stakeholders during the second round of consultations, held July 18<sup>th</sup> to 27<sup>th</sup>.
- **Appendix B** includes descriptions of, and sources for, the assumptions built into the cost-benefit analysis model and is designed to provide the Ministry with an understanding of how our research informed the analysis and the inclusions therein.
- **Appendix C** provides an overview of the components of the costs and benefits that are included in the model. To avoid double-counting costs and benefits, many important considerations of a Green Button initiative were required to be rolled up into larger categories. This table is intended to demonstrate that these costs and benefits have not been excluded from the analysis; rather, they have been included at a higher level.
- **Appendix D** explains the methodology, assumptions, and inputs used to estimate the conservation costs and benefits, including greenhouse gas reductions, related to the implementation of Green Button.
- **Appendix E** includes additional scenario analyses using a real societal discount rate of 3.5%, which has been used by the Ministry of Energy in other recent analyses.



## COST-BENEFIT ANALYSES

This section explains how cost-benefit analyses in general are structured, as well as alternatives and limitations.

### OVERVIEW

The cost-benefit analysis (CBA) developed to assess the potential implementation of Green Button in Ontario follows the general principles of cost-benefit analyses: it provides a common ground to compare the costs incurred by each scenario under consideration to the potential benefits that are expected to materialize as a consequence of that scenario. One of the key strengths of a CBA analysis is that it provides a coherent and consistent view of benefits and costs using a common expression. In most cases the common expression is monetary value, which means that all costs and benefits in the analysis must be expressed as a monetary value. If they cannot be expressed in this way, they cannot be included in the analysis. For example, time can be converted by utilizing assumptions for hourly or daily labour costs.

CBA analyses are based on a set of fundamental parameters and considerations. Some of the key ones are the following:

- Benefits and costs are expressed in constant dollars, taking into consideration the time-value of monetary flows.
- CBA analyses must be balanced (i.e., the analysis should strive to account for all costs and benefits of any specific component).
- Its boundaries must be clearly defined, to capture and express costs and benefits within these boundaries.
- Double counting of costs and benefits must be avoided. This can be challenging when benefits can be expressed in different fashions or accrue to different stakeholders (i.e., if any components are included at a more granular population than the general boundary of the analysis, they should not be included in a broader stakeholder category).
- CBA analyses cannot provide a perfect appraisal of all present and future costs and benefits. Recognizing this, effort should be focused on the evaluation of costs and benefits with a material impact on the expected results.
- CBA outcomes rely on the accuracy and quality of the inputs used. Data quality can be higher when it is possible to draw from similar types of analyses conduct in other jurisdictions or when detailed, market-specific data is available.

## BENEFIT-COST RATIOS

Benefit-cost ratios are the result of a cost-benefit analysis. To calculate them, total benefits (in dollars) are divided by total costs in the following way:

$$R = \frac{B}{C}$$

If the ratio is positive, it means that the benefits outweigh the costs, so the initiative being analyzed is cost-effective. If it is negative, the costs exceed the benefits and the initiative is not cost-effective.

Here is an example:

$$B \quad C \quad R = \frac{\$4,000,000}{\$1,000,000} = 4$$

In this example, the benefits outweigh the costs by 4 to 1, so the initiative being analyzed is cost-effective.

## ALTERNATIVES

Alternatives to CBA exist that use a different denominator for the benefits where appropriate. As an example, cost-effectiveness analyses for energy efficiency programs can be expressed in \$/unit of energy saved, and similar constructs are used for economic analysis in other spheres (\$ per life-year saved, \$ per GHG emissions reduction, etc.). When assessing the potential implementation of a Green Button policy, since the vast majority of benefits can be readily expressed in a monetary figure, this is the most appropriate denominator to be used for a CBA analysis.

## LIMITATIONS

### BENEFIT-COST RATIOS

The cost-benefit results (in the form of benefit-cost ratios) are presented at the societal level, not for individual sectors or customer groups. This is because there are numerous overlapping and multi-tiered costs and benefits that cannot be broken out. For example, setup costs are incurred at the utility level (therefore all customers), but only a subset of customers see associated process efficiencies. Conversely, some customers will incur costs, but other customers will receive benefits related to that investment.

While we are unable to present balanced cost-benefit ratios at the sector or customer-group level, the results have been built up from inputs at those levels rather than developed from a top-down approach. We are therefore able to present the dollar values used as inputs in key scenarios to provide a sense of scale.

---

## LEVEL OF GRANULARITY

CBA analyses provide a reasonable estimate of the best alternatives to be considered. However, they should be used to inform and guide decisions, not to dictate them. Components and considerations not included in the CBA analysis (including qualitative benefits) should also be accounted for in the decision-making process.

It is also important to note that Green Button is a relatively new opportunity, and little documented and verified data exists at the granularity that exists for other types of CBAs. The information we gathered was largely new and primary-source based, and data for some sectors, costs and benefits is more widely available than others. Where detailed, granular data does not exist, or the project scope did not allow for in-depth research, our team therefore developed assumptions and proxies.

For this reason, the analysis highlights scenarios that are cost-effective and ones that are not. However, the results should not be interpreted as exact; they should be interpreted as indicative. The inputs we gathered and developed are appropriate for a policy-level analysis designed to determine whether the benefits of a Green Button implementation outweigh the potential costs. However, they are not developed at the granularity that an actual implementation plan would require.

Where costs and benefits have been broadly quantified based on limited data availability, we recommend caution in the interpretation of the results. This is especially the case with results for which the benefit-to-cost ratio is close to one, as small deviations from the assumptions used can lead to different conclusions (e.g., the benefit/cost ratio can fall or rise above one if assumptions change).

---

## RESEARCH SOURCES

Our team conducted secondary research and literature reviews that included evaluation and research reports, utility filings and reports, Statistics Canada data, conservation and demand management (CDM) and demand-side management (DSM) programs, and other sources.

We also generated key inputs and assumptions through a series of consultations, surveys and interviews with stakeholders. Information on this source of primary data is provided below, and the assumptions developed from each source is provided in Appendix B.

### ***STAGE ONE CONSULTATIONS***

We obtained initial input from stakeholders on general costs and benefits they could experience from a Green Button implementation. This stage was designed to ensure we research the appropriate topics and details. Eighty-nine organizations attended these sessions, with the breakout by stakeholder group provided below.

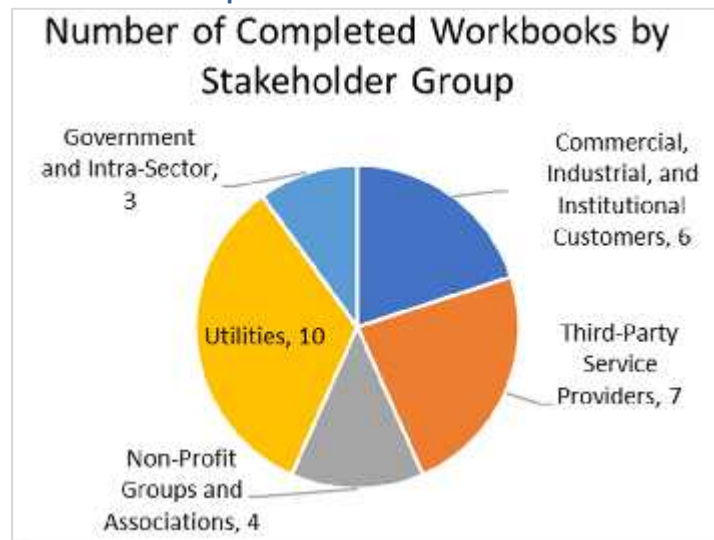
**Figure 1. Breakdown of Stakeholder Groups Attending Stage One Consultations**



**STAGE ONE WORKBOOKS**

We asked a series of questions asking stakeholders to quantify costs and benefits they could see as a result of a Green Button implementation. Questions focused on how and for what purposes utility data is requested or shared, challenges with accessing or providing data, time and effort that could be saved by accessing data via Green Button, and other potential benefits such as access to additional insights in energy or water use, greater potential for taking action to save energy or water, and other outcomes. We received thirty workbooks in total, with the cross-section of stakeholder groups provided in figure 2 below.

**Figure 2. Breakdown of Completed Workbooks by Stakeholder Group**



## INTERVIEWS

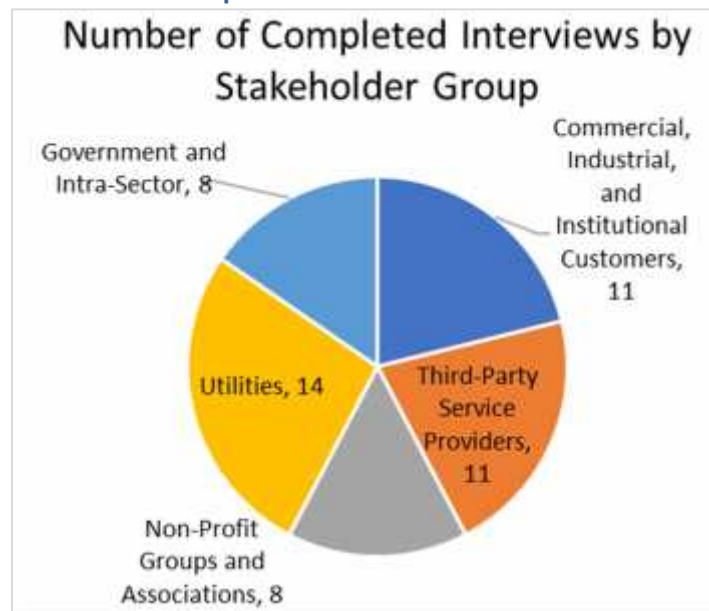
The Stage One Consultations and workbooks were designed to ensure we understood the potential scope of costs and benefits for a Green Button implementation. However, to obtain more granular data and inputs with which to assess the costs and benefits, our team conducted interviews with multiple organizations in each stakeholder group.

For interviews with utilities:

- We interviewed small, medium, and large electricity and water utilities as well as both large natural gas utilities to ensure we captured differences between how each size and type would be impacted by a Green Button implementation.
- We interviewed both utilities involved in Ontario’s Green Button Connect My Data Pilot in order to obtain as much detail as possible on the actual implementation experience in Ontario, in particular for the costs of implementing Green Button Connect My Data (including Extract, Transform, and Load (ETL) protocols, integration with customer portals, meter data, external testing and validation, etc.).

These semi-structured interviews went into more detail in terms of quantifying the costs and benefits identified in the earlier consultations and workbooks. Our team completed 52 interviews across the range of stakeholder groups, with a higher percentage completed with groups identified as having the greatest potential benefits and/or costs: Commercial, Industrial and Institutional customers, utilities, and third-party service providers (consultants, energy efficiency services organizations, app developers, and hosted solution providers), as highlighted in figure 3 below.

**Figure 3. Breakdown of Completed Interviews by Stakeholder Group**



**UTILITY INFORMATION TECHNOLOGY SURVEY**

An important component of the cost-benefit analysis was understanding the information technology (IT) infrastructure of utilities. Because benefits arising from Green Button change based on the type and frequency of utility metering and meter reads and other utility IT considerations, we sent surveys to electricity, natural gas, and water utilities. The surveys included the following question categories:

Category Type	Information Sought
<b>Consumption Data</b>	Type of metering infrastructure by customer segment
	Number of installed meters and sub-meters by customer segment
	Typical time intervals for meter reads and whether estimates are used, by customer segment
	How meter data is managed for General Service and Large User customers (specifically whether or not it is outsourced or done in-house)
	Availability and frequency of access of online customer portals
	Billing frequency and format
	Billing processes including whether or not it is conducted by a third party
	Customer access to consumption data, including availability, format, process, granularity, frequency, and cost
	Processes for authorized third-party access to customer utility data, including time and effort required to grant approvals
<b>Generation Data</b>	Availability of customer generation data (for applicable customers), by customer segment
	Level of granularity and frequency of customer generation data
	Percentage of customers requesting access to their generation data in a machine-readable form, by customer segment, and the cost and effort of fulfilling such requests
<b>Additional Questions</b>	Current investment in smart meters, by customer segment
	Planned meter and IT investment, including smart meters (by customer segment), meter data management infrastructure, billing, customer portals

These surveys were used, in combination with other sources, to develop estimates of the number of water utilities with metering infrastructure, accounts by utility type and customer segment, penetration of submeters in buildings and facilities, percentage of customers currently accessing utility data in electronic format, and annual cost reductions by utility type and size.

Overall, our team received 61 completed surveys, broken down as follows:

- 33 electricity utilities (46 percent of possible utilities);
- 2 natural gas utilities (67 percent of possible utilities); and
- 26 water utilities (5 percent of possible utilities).

### ***SOLUTION PROVIDER SURVEY***

Additional data was also required to estimate the costs for developing, hosting, and maintaining the Green Button platforms. Because we required detailed cost information that is difficult to gather via phone interview, we sent surveys to eleven solution providers, from which we received two submissions. The surveys asked for estimates of the following costs for each of two scenarios:

#### **Scenarios:**

1. Implementing Green Button Connect My Data as a hosted solution for each utility (e.g. if each utility was responsible for hiring a firm to implement Green Button Connect My Data).
2. Implementing Green Button Connect My Data as a hosted solution for a group of utilities (e.g. if a hosted solution provider were hired to implement it for a group of utilities or for the entire province).

#### **Information Requested:**

- Fixed and variable costs for each utility if hired on an individual basis, by utility type, size (small, medium, or large), or group;
- Time required to set up and launch the platform; and
- Assumptions, including whether or not the provider is hosting Connect My Data or is installing Connect My Data software.

This information was used to develop estimates for the costs of developing and hosting a Green Button Platform. Rolled-up, not itemized, costs were requested; they included front-end solutions, cloud services, platform costs, development and testing, and registration.

## GREEN BUTTON COST-BENEFIT ANALYSIS

The following sections describe 1) the general assumptions used in the Green Button cost-benefit analysis and 2) inputs and assumptions used in modelling specific scenarios.

### STAKEHOLDER GROUPS

There are five key stakeholder groups involved in the analysis, with further categorization within the groups, as outlined below<sup>1</sup>:

Stakeholder Group	Stakeholder Sub-Group	Additional Considerations (if applicable)		
Customers	Commercial	Large	Owners/Managers; Tenants	Existing users of utility data; New users of utility data
		Small	Owners/Managers; Tenants	Existing users of utility data; New users of utility data
	Large Industrial		Owners/Managers; Tenants	Existing users of utility data; New users of utility data
	Institutional		Owners/Managers; Tenants	Existing users of utility data; New users of utility data
	Residential		Owners/Managers; Tenants	Existing users of utility data; New users of utility data
Third-Party Service Providers	Energy Efficiency Services			
	Hosted Solution Providers			
	Application Developers			
	Consultants			
	Renewables			
Non-Profit Groups and Associations	Associations			
	Non-Profit Organizations			
Utilities	Electricity Utilities	Large; Medium, Small		
	Natural Gas Utilities	Large; Medium, Small		
	Water Utilities	Large; Medium, Small		
Government and Intra-Sector				

<sup>1</sup> Note that stakeholder groups do not necessarily align with higher-level groups used for stakeholder consultations and workshops – these sub-groups align with how research for the cost-benefit analysis was conducted.



## QUANTITATIVE AND QUALITATIVE BENEFITS

We considered multiple costs and benefits in our analysis, some of which are direct results of a Green Button implementation, others that are prompted by (but not automatically resulting from) Green Button, and others that are important but cannot be quantified. For this reason, we group them in the following way:

**Table 1. Grouping of Costs and Benefits**

QUANTITATIVE		QUALITATIVE
Direct (Layer 1A)	Indirect (Layer 2A)	(Layer 2B)
Benefits and costs are a direct result of Green Button implementation  Monetary value can be estimated based on available information	Indirect consequence of Green Button implementation  Require an additional external influence or decision point in order to materialize  Monetary value can be estimated based on available information	Not included in Cost-Benefit Model  Reported as “additional costs/benefits”  Used in overall analysis and policy recommendations

## SCENARIOS

Two core considerations in the Green Button Cost-Benefit Analysis were the potential implementation of either Green Button Download my Data (DMD) or the implementation of both Download my Data and Connect my Data (CMD). For clarity, these are the definitions we used, per the Ministry’s definition:

**Table 2. Green Button Option Definitions**

Option	Details
<b>Green Button Download My Data (DMD)</b>	<ul style="list-style-type: none"> <li>Provides customers with the ability to download their utility data directly, through their utilities’ websites</li> <li>Data is downloaded in XML and is provided in a consistent format</li> </ul>
<b>Green Button Connect My Data (CMD)</b>	<ul style="list-style-type: none"> <li>Provides customers with the ability to share their data with solution providers/app developers and compatible databases in an automated way, based on consumer authorization</li> <li>Process follows Privacy By Design principles</li> </ul>

For each of these options, we then layered additional dimensions:

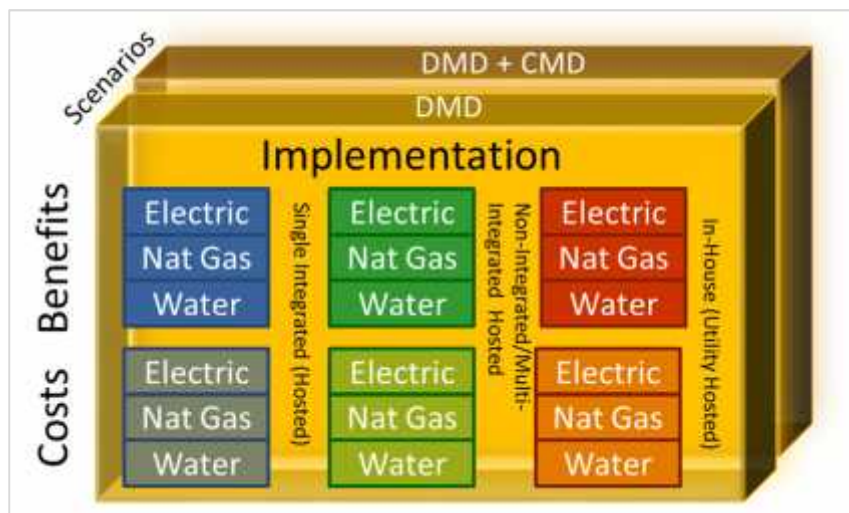
- **Utility Type:** Electricity, Natural Gas, Water
- **Implementation Type:** Single Integrated (Hosted), Multi-Integrated (Hosted), Non-Integrated (Hosted), In-House

For the implementation types, we used the following definitions:

- **Single Integrated (Hosted):** One Hosted Software as a Service (SaaS) provider implements Green Button for all utilities, incorporating one platform for each utility type (three platforms in total).
- **Multi-Integrated (Hosted):** A limited number of Green Button hosted SaaS platforms are used by all utilities.<sup>2</sup> This implementation assumed five implementation platforms for electricity and water utilities and two for natural gas utilities.
- **Non-Integrated (Hosted):** Each utility has the option to develop/procure its own Green Button SaaS hosted platform. One platform per utility was assumed, for 591 platforms in total.
- **In-House:** Each utility develops its own platform on its own IT systems. One platform per utility was assumed, for 591 platforms in total.

Overall, the layering (and resulting combinations of scenarios) can be conceptualized in the following way:

Figure 4. Cost-Benefit Analysis Scenarios



## GENERAL INPUTS AND ASSUMPTIONS

### UTILITY TYPE

The inputs for each utility type (electricity, natural gas, and water) are critical because Green Button would be implemented by utilities. Our general assumptions are:

<sup>2</sup> This was a hypothetical scenario to demonstrate potential synergies in limiting the number of providers; the same assumptions were used for this scenario as for the non-integrated, with the difference being the number of platforms developed and integrated.

**Table 3. Utility Input Assumptions**

Utility Type	Key Factors in Analysis	Details	Source (if applicable)
<b>Electricity</b>	Utility Population/Sizes	<ul style="list-style-type: none"> <li>7 Large, 21 Medium, 44 Small</li> </ul>	<ul style="list-style-type: none"> <li>OEB 2014 Yearbook of Electricity Distributors</li> </ul>
	Metering Infrastructure	<ul style="list-style-type: none"> <li>All are metered</li> <li>Most have completed smart meter implementation for Residential and Small Commercial</li> <li>Sub meters exist for many buildings (but unknown to what extent by utilities)</li> </ul>	<ul style="list-style-type: none"> <li>Utility IT survey</li> <li>Interviews with stakeholders</li> </ul>
	Total Number of Accounts	<ul style="list-style-type: none"> <li>5,162,768 accounts</li> </ul>	<ul style="list-style-type: none"> <li>OEB 2014 Yearbook of Electricity Distributors</li> <li>Utility IT survey</li> </ul>
<b>Natural Gas</b>	Utility Population and Sizes	<ul style="list-style-type: none"> <li>2 Large, 1 Small</li> </ul>	<ul style="list-style-type: none"> <li>OEB 2014 Yearbook of Natural Gas Distributors</li> </ul>
	Metering Infrastructure	<ul style="list-style-type: none"> <li>All are metered</li> <li>Combination of Automatic Meter Reading (AMR) and analog meters</li> </ul>	<ul style="list-style-type: none"> <li>Consultations with utilities</li> </ul>
	Total Number of Accounts	<ul style="list-style-type: none"> <li>3,423,622 accounts</li> </ul>	<ul style="list-style-type: none"> <li>Utility scorecards – Ontario Energy Board</li> <li>Union Gas and Enbridge Gas filings</li> </ul>
<b>Water</b>	Utility Population and Sizes	<ul style="list-style-type: none"> <li>39 Large, 91 Medium, 385 Small (only metered utilities were included in the analysis)</li> </ul>	<ul style="list-style-type: none"> <li>Watertap Ontario</li> </ul>
	Metering infrastructure	<ul style="list-style-type: none"> <li>All large and medium utilities metered</li> <li>70% of Ontario’s 550 small water utilities assumed to be metered (resulting in the 385 indicated above)</li> <li>Analog meters</li> </ul>	<ul style="list-style-type: none"> <li>Utility IT Survey</li> </ul>
	Total Number of Metered Accounts	<ul style="list-style-type: none"> <li>4,955,366 metered accounts</li> </ul>	<ul style="list-style-type: none"> <li>Residential: based on population in each municipality and average number of individuals per household in Ontario (Statistics Canada)</li> <li>Commercial: based on proportion of electricity to water accounts</li> </ul>

---

## ADDITIONAL INPUTS

Separate from the utility types, our team had to make decisions as to the information and inputs to include in the analysis based on the data available or accessible through research and interviews, as well as the requirements of the analysis. These types of inclusions (and exclusions, as applicable) are provided in Table 4: General Inputs.

---

## A NOTE ABOUT NET-PRESENT VALUE CALCULATIONS AND SOCIETAL DISCOUNT RATE

The economic analysis of Green Button was conducted based on the net present value of the benefits and costs streams generated by the program. All benefits and costs monetary streams were assessed in real values to isolate them from the impacts of inflation and to account for the uncertain timing of the Green Button implementation. Conducting cost-effectiveness analysis using real values is a leading industry practice and recommended in the IESO Conservation & Demand Management Energy Efficiency Cost Effectiveness Guide of June 2015.

The monetary streams were then discounted to the first year of implementation, using a real social discount rate of 2%. The proposed discount rate was informed by the long-term Ontario Global bonds maturing in December 2046 (Series no. DMTN228) with an interest rate of 2.9%, the inflation rate in June 2016 of 1.7%, and the IESO real social discount rate of 4% applied for utilities' CDM initiatives. Monetary values are expressed in 2016 dollars.

Although there are no set criteria to define an appropriate discount rate for government-led energy efficiency initiatives, the public benefit perspective of Green Button advocates for the use of a long-term, risk-free discount rate attuned to the provincial government's long-term interest rates. However, considering that this would translate into a real discount rate of 1.2%, and considering the discount rates used for CDM initiatives of 4%, a more conservative real discount rate of 2% was applied to the Green Button economic analysis.

Relevant sources are as follows:

- Province of Ontario Bond Issues Details: [http://www.ofina.on.ca/pdf/bond\\_issue\\_details\\_DMTN228\\_to\\_R19.pdf](http://www.ofina.on.ca/pdf/bond_issue_details_DMTN228_to_R19.pdf)
- 2016 Consumer Price Index and Inflation Rates for Ontario: <http://inflationcalculator.ca/2016-cpi-and-inflation-rates-for-ontario/>
- Conservation and Demand Management Energy Efficiency Cost Effectiveness Guide: <http://www.ieso.ca/-/media/files/ieso/document-library/conservation/ldc-toolkit/cdm-ee-cost-effectiveness-test-guide-v2-20150326.pdf?la=en>

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

**Table 4. General Inputs**

Category	Assumption/Consideration	Status	Rationale	Source (if applicable)
<b>General Inputs</b>	Metered utility types beyond electricity, natural gas, and water	Excluded	Lack of data	
	Societal discount rate	Included	The final policy will provide benefits and costs for Ontario as a whole.	Adjustment to IESO real discount rate (CDM EE Cost-Effectiveness Test Guide) to reflect conservative view of 30-year Ontario real bond rates of 1.2%) <sup>3</sup>
	Participation in Green Button based on Rogers' Diffusion of Innovation (varies by cost/benefit category)	Included	Used in Energy Efficiency Forecasting. Parameters fitted to observed and expected behaviours	Rogers' Diffusion of Innovation
<b>Green Button Standard</b>	Updates to Ontario Green Button architecture	Excluded	Out of scope	
	Single version of the standard for deployment	Included	Ensures consistency among utility implementations	
	Green Button certification costs (utility or solution provider/app developer)	Excluded	Lack of data, certification approach and costs under development at time of analysis	
	Application registration platform costs	Excluded	Not a fundamental requirement and lack of data	
<b>Metering Infrastructure</b>	Infrastructure upgrades (i.e., upgrading to smart meters or installing meters)	Excluded	Out of scope	
	Existing sub-meters: benefits	Included	Small, but quantifiable	Interviews with stakeholders
	Existing sub-meters: costs	Excluded	Initial research indicates lack of additional costs to implement Green Button for existing sub-meters	Interviews with stakeholders

<sup>3</sup> For additional analyses using a real societal discount rate of 3.5%, which has been used by the Ministry of Energy in other recent analyses, please see Appendix E.

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

Category	Assumption/Consideration	Status	Rationale	Source (if applicable)
Energy Inputs	Duration limited to analysis periods of 5 and 10 years (no end effects)	Included	Conservative assessment and unknown lifetime for retrofit measures	
	Energy retrofit costs (\$/kWh or \$/annual m <sup>3</sup> saved) accrued at the same time as benefits materialize	Included	Aligns benefits and costs for a more consistent reporting of results	Ontario gas utility's DSM Plan; Canadian Jurisdictions' Electricity DSM Plans (e.g. New Brunswick, Nova Scotia)/Potential Studies

## COSTS OF A GREEN BUTTON IMPLEMENTATION

Quantitative costs of implementing and managing a Green Button Connect My Data solution, whether direct or indirect, can be categorized into three main components:

1. **Set-up:** Costs required to develop the Green Button platform (setup can be administered either by utilities or third parties).
  - Setup costs are largely related to developing the Green Button platform, so the costs are incurred for each platform developed. This means they vary based on the implementation model selected (single-integrated hosted, multi-integrated hosted, non-integrated hosted, and in-house), but not by utility size, type, or other consideration.
2. **Integration:** Costs incurred to integrate Green Button with utilities' data systems and processes.
  - These costs vary based on the utility size, reflecting the complexity of systems required to integrate with the Software as a Service (SaaS) hosted implementation platform. As part of the analysis, we also assumed the integration costs would vary based on the implementation scenario being assessed, with increased costs if utilities are required to develop and test all solutions without guidance from a SaaS hosted implementation provider.
3. **Ongoing annual costs:** Costs, expressed as a unit cost (cost per participating account) required to maintain the system and manage third-party solution provider application registration.
  - Similar to integration costs, the analysis assumes that annual costs vary based on the type of implementation model selected (single-integrated hosted, multi-integrated hosted, non-integrated hosted, and in-house). This reflects the range of values reported by third-party hosted solutions providers, with a lower unit cost (cost per participating account) for fewer SaaS platforms and a higher unit cost for individual in-house implementations. Details are provided in the Costs table below.
  - Retrofit costs are also included in this category as an indirect cost, since increased access to utility data is expected to drive interest in energy efficiency. The analysis is agnostic as to whether the retrofits occur outside of or through utility CDM programs, as total costs (whether incurred by the utility or the participant) are included, regardless of the source of funds.

**These costs are incurred regardless of specific implementation scenario**, although their magnitude changes based on the particular scenario being analyzed. In this section, we provide individual cost inputs to the analysis. Costs associated with specific implementation scenarios (combinations of inputs) are provided in the following section.

---

COST CATEGORIES, DEFINITIONS AND APPLICABILITY

Table 5 provides an overview and clarifying information regarding the various categories of costs, including definitions and the groups to which the costs apply.



**Table 5. Cost Categories, Definitions and Applicability**

Category	Cost	Definition	Impacted Groups <sup>4</sup>	Grouping
<b>Platform Setup Costs</b>	Front-end solutions	Interfaces and applications that users interact with directly	Utilities (can be via Software as a Service Green Button Implementation Providers)	Direct, Quantified
	Cloud services	Computing resources and services that support the deployment of Green Button and provide access to its applications, resources and services	Utilities (can be via Software as a Service Green Button Implementation Providers)	Direct, Quantified
	Green Button platform	The technical foundation that allows multiple products (such as Green Button applications) to be built within the same framework and execute successfully	Utilities (can be via Software as a Service Green Button Implementation Providers)	Direct, Quantified
	Development and testing of the services to manage third-party (solution provider) applications	Management of integration, registration, risk assessment, issues, etc.	Utilities (can be via Software as a Service Green Button Implementation Providers)	Direct, Quantified
	Testing of required security and privacy mechanisms and protocols	Required for ensuring mechanisms and protocols are acceptable	Utilities (can be via Software as a Service Green Button Implementation Providers)	Direct, Quantified

<sup>4</sup> Party incurring the costs

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

Category	Cost	Definition	Impacted Groups <sup>4</sup>	Grouping
<b>Utility Integration Costs</b>	Customer information system extract, transform and load (ETL) protocols	Protocols for the functions required to pull data from a utility's database into another database	Utilities (can be via SaaS Green Button Implementation Provide)	Direct, Quantified
	Other integration costs such as integration with customer portals, meter data, external testing and validation, etc.	Testing and resolving issues with the connections between utility data systems and external systems via Green Button	Utilities	Direct, Quantified
<b>Annual Variable Costs by Participating Customer</b>	Maintenance and ongoing operations	Ongoing modification to address issues, improve performance, or incorporate changes to the standard	Utilities	Direct, Quantified
<b>Retrofit Costs</b>	Unit Costs of Retrofit Activity (\$/conservation benefit)	Unit costs are the costs of an activity (e.g. retrofits) divided by the energy saved. Increased energy efficiency retrofits are expected to occur with a Green Button implementation, so related costs must be included to provide a balanced analysis.	Customers	Indirect, Quantified

---

## COST INPUTS, SOURCES AND ASSUMPTIONS

Table 6 includes key inputs for each cost component, including sources and assumptions our team used to develop them.

Costs associated with solution provider/app developer registration with utilities were excluded because they were outside of cost-effectiveness testing parameters (they are built into the solution providers' costs).

**Table 6. Cost Inputs, Sources and Assumptions**

Cost Component	Unit Cost	Assumption/Considerations	Sources <sup>5</sup>
<b>Platform Setup Costs – Green Button Platform</b>	\$50,000/ platform	<ul style="list-style-type: none"> <li>Assumes fixed cost per CMD implementation platform for setup (number of platforms drives costs).</li> <li>Significant differences in values were quoted by different providers (from \$0 to \$50,000), but the value selected is a reasonable representation because it includes all services, including third-party registration.</li> </ul>	<ul style="list-style-type: none"> <li>Based on discussions with hosted Software as a Service (SaaS) providers and solution provider survey.</li> </ul>
<b>Utility Integration Costs – Hosted Solution Implementation Scenarios (Multi-Integrated, Single Integrated, and Non-Integrated)</b>	Large Utilities: \$225,000/utility	<ul style="list-style-type: none"> <li>Costs vary based on utility size, which reflects complexity of utilities’ IT infrastructure.</li> <li>Utility type does not alter the assumptions as it is IT, not energy, factors that impact the costs.</li> </ul>	<ul style="list-style-type: none"> <li>Based on stakeholder interviews (specifically on Ontario’s CMD pilot project experience).</li> </ul>
	Medium Utilities: 72,000\$/utility		
	Small Utilities: 22,500\$/utility		
<b>Utility Integration Costs – Impact of in-house Implementation Model</b>	Integration costs increase by 33% in comparison to the Single Integrated Hosted Solution implementation scenario	<ul style="list-style-type: none"> <li>Costs vary based on utility size, which reflects complexity of utilities’ IT infrastructure.</li> <li>Cost inefficiencies occur because software hosting is not part of utilities’ core business.</li> </ul>	<ul style="list-style-type: none"> <li>Based on stakeholder interviews (specifically on Ontario’s CMD pilot project experience).</li> </ul>

<sup>5</sup> When interviewees provided a range of responses our team used the mid-range unless, based on our experience and knowledge, it appeared overly optimistic, in which case we selected a higher end of the range.

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

Cost Component	Unit Cost	Assumption/Considerations	Sources <sup>5</sup>
Annual Variable Costs by Participating Customers	<b>SaaS Multi- and Non-Integrated Hosted Implementations:</b> \$1/participating customer	<ul style="list-style-type: none"> <li>Fixed costs per participant vary by implementation scenario: assumes economies of scale between implementation scenarios (the fewer the number of platforms, the greater the cost efficiencies related to management of the platform and system).</li> <li>Assumes mid-range of information provided by Software as-a-Service providers.</li> <li>Includes general operational costs and costs to support solution provider/app developer registration.</li> </ul>	<ul style="list-style-type: none"> <li>Professional judgment based on information provided by SaaS providers during stakeholder interviews.</li> </ul>
	<b>SaaS Single Integrated Hosted Implementation:</b> \$0.80/participating customer	<ul style="list-style-type: none"> <li>Fixed costs per participant vary by implementation scenario: assumes economies of scale between implementation scenarios (the fewer the number of platforms, the greater the cost efficiencies related to management of the platform and system).</li> <li>Includes general operational costs and costs to support solution provider/app developer registration.</li> <li>The input selected reflects operational maintenance efficiencies compared with the multi- and non-integrated implementations.</li> </ul>	<ul style="list-style-type: none"> <li>Representative of information provided by SaaS providers during stakeholder interviews.</li> </ul>

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

Cost Component	Unit Cost	Assumption/Considerations	Sources <sup>5</sup>
	<p><b>In-House Utility Implementations:</b>                      \$1.20/participating customer</p>	<ul style="list-style-type: none"> <li>Fixed costs per participant vary by implementation scenario: assumes economies of scale between implementation scenarios (the fewer the number of platforms, the greater the cost efficiencies related to management of the platform and system).</li> <li>Analysis assumes high range of information provided by Software as-a-Service providers in order to be conservative and based on professional judgment.</li> </ul>	<ul style="list-style-type: none"> <li>High range of information provided by SaaS providers during stakeholder interviews.</li> </ul>
<p><b>Retrofit Costs – Customers’ energy efficiency upgrades resulting from access to data</b></p>	<p><b>Residential Electricity Customers:</b> \$0.65/\$ value of benefits  <b>Residential Natural Gas and Customers:</b> \$0.69/\$ value of benefits  <b>Non-Residential Customers (all utility types):</b> \$0.50/\$ value of benefits</p>	<ul style="list-style-type: none"> <li>Annual levelized costs.</li> <li>Costs are in relation to level and extent of retrofit activity.</li> <li>Full retrofit costs are included regardless of whether customers participate in a CDM/DSM program or not (i.e. if costs are partially paid by the utility or fully by the customer).</li> <li>Behavioural and operational savings are assumed to be implemented by the customer at no cost because they result from a change in procedures or behaviour rather than a solution that requires a capital outlay.<sup>6</sup></li> </ul>	<ul style="list-style-type: none"> <li>Ontario utility and other Canadian CDM/DSM Plans (e.g. New Brunswick, Nova Scotia); Potential Studies</li> </ul>

<sup>6</sup> Some process efficiencies could require additional resources or labour, but this is expected to be minimal and has therefore been excluded from the analysis.

## BENEFITS OF A GREEN BUTTON IMPLEMENTATION

Quantified benefits from a Green Button implementation can be categorized into **two main categories**:

- **Operational Efficiencies**
  - Process efficiencies in accessing consumption, billing and generation utility data;
  - Reduced customer care effort; and
  - CDM/DSM program efficiencies and innovations.
  
- **Conservation / Energy Efficiency.**
  - Energy and water savings from behavioural changes resulting from additional access to utility data; and
  - Energy efficiency retrofit improvements resulting from additional access to utility data.

These benefits are incurred regardless of specific implementation scenarios, although their magnitude will change based on the particular scenario being analyzed. Benefits associated with specific implementation scenarios (combination of inputs) are provided in the following section.

---

## BENEFIT CATEGORIES, DEFINITIONS AND APPLICABILITY

Table 7 on the following page provides an overview and clarifying information regarding the various categories of benefits included in the analysis, including definitions and the groups to which they apply.

**Table 7. Benefit Categories, Definitions and Applicability**

Category	Benefit	Definition	Impacted Groups <sup>7</sup>	Grouping
Operational Efficiencies	Utility consumption, billing and generation data process efficiencies and Ongoing utility consumption monitoring and benchmarking	<ul style="list-style-type: none"> <li>Process efficiencies for customers and consultants/service providers include efficiencies in energy audits; reduced effort/cost for energy tracking, reporting, and benchmarking; reduced effort to consolidate/ standardize data across facilities; reduced effort to “clean” and quality-check data; reduced effort to authorize data sharing; and access to increased frequency and granularity of utility data.</li> <li>The benefits relate to customers who require data for their own internal use (e.g. for internal benchmarking or operational requirements) or who will need to comply with the Ministry of Energy’s Large Building Energy and Water Reporting and Benchmarking initiative under <i>Ontario Regulation 20/17, Ontario Reporting of Energy Consumption and Water Use</i>.</li> <li>Benefits to utilities include increased operational efficiencies from improvements to IT systems resulting from preparing systems to meet Green Button requirements.</li> </ul>	Customers, Consultants/Service Providers, Utilities	Direct, Quantified
	Reduced customer care effort	<ul style="list-style-type: none"> <li>The benefit results from a reduction in the time required to provide consumption information to utility customers.</li> </ul>	Utilities	Indirect, Quantified
	CDM/DSM program efficiencies and innovations	<ul style="list-style-type: none"> <li>Efficiencies resulting from streamlined CDM/DSM program implementation (e.g., easier access to data to conduct audits) and program evaluation (e.g. less resource time to gain access to billing data).</li> <li>Innovations to existing programs based on increased customer access to utility data.</li> </ul>	Utilities	Indirect, Quantified

<sup>7</sup> Who receives the benefits



Category	Benefit	Definition	Impacted Groups <sup>7</sup>	Grouping
<b>Energy Efficiency and Conservation</b>	Energy savings from behavioural and retrofit improvements resulting from additional access to utility data	Behavioural benefits include conservation behaviours resulting from increased access to utility data, greater operational savings in commercial/industrial buildings, and increased participation in CDM/DSM programs. Examples of behavioural/ operational efficiencies include turning lights off or optimizing equipment schedules to minimize energy use. <ul style="list-style-type: none"> <li>• Energy Efficiency retrofit benefits include increased implementation of energy efficiency measures (e.g. purchasing and installing energy efficient measures, conducting building audits and implementing recommendations, etc.). Measures could be implemented through participation in existing CDM/DSM programs or outside of utility programs.</li> </ul>	Customers <sup>8</sup>	Indirect, Quantified

---

<sup>8</sup> Energy efficiency benefits were not applied to utilities to avoid double-counting the benefits

---

## BENEFIT INPUTS, SOURCES AND ASSUMPTIONS

Table 8 includes key inputs for each benefit, including sources and assumptions our team used to develop them.

Benefits of increased real estate value were excluded from the analysis because the impact is diffuse and not material in the analysis: only a certain percentage of homes would be sold during the study period, of which only a certain percentage would access GB data, of which only a certain percentage would retrofit their homes to increase the value, of which a low percentage would see an increase in value because purchasers would not likely have comparable data for other homes.

**Table 8. Benefit Inputs, Sources and Assumptions**

Benefit Component	Unit Benefit	Assumptions/Considerations	Sources
<b>Utility consumption, Billing and Generation Data Process Efficiencies and Ongoing Utility Consumption Monitoring and Benchmarking</b>	<b>Large commercial/ industrial customers (above 10,000 sq. feet):</b> <ul style="list-style-type: none"> <li>\$180 in avoided costs annually per building (6 hours of effort at \$30/hr)</li> </ul>	<ul style="list-style-type: none"> <li>Benefits reflect total budget impact for a portfolio of buildings as well as effort required to collect and analyze data for a single building.</li> <li>The benefits were distributed among each utility type (64% electricity, 22% natural gas, 14% water), based on stakeholder input as to the type of utility from which they would receive the most Green Button-related benefits, the frequency of billing by the utilities, and the granularity of data available.</li> <li>Direct benefit of implementing Green Button.</li> </ul>	<ul style="list-style-type: none"> <li>Stakeholder consultations and interviews</li> </ul>
	<b>Small commercial/ industrial customers:</b> <ul style="list-style-type: none"> <li>\$198 in avoided costs annually per building</li> </ul>	<ul style="list-style-type: none"> <li>Benefits reflect total budget impact for a portfolio of buildings as well as effort required to collect and analyze data for a single building.</li> <li>Assumption that small buildings (less than 10,000 sq. feet) would experience higher benefits than larger buildings because owners of smaller buildings have less sophisticated processes to collect and manage consumption data.</li> <li>A 10% increase for this benefit category was attributed to the owners of small buildings category (in comparison to the avoided costs for large buildings), based on professional judgement.</li> <li>Direct benefit of implementing Green Button.</li> </ul>	<ul style="list-style-type: none"> <li>Stakeholder consultations and interviews</li> </ul>
	<b>Building Owners &amp; Residential Customers:</b> <ul style="list-style-type: none"> <li>Annual benefit (variable based on descriptions in Assumptions column)</li> </ul>	<ul style="list-style-type: none"> <li>Benefits vary by implementation (DMD/CMD), new vs. current users of electronic data format, customer type, and building ownership status.</li> <li>Greater value to customers not currently accessing data electronically.</li> <li>Direct benefit of implementing Green Button.</li> </ul>	<ul style="list-style-type: none"> <li>Stakeholder consultations and interviews</li> </ul>

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

Benefit Component	Unit Benefit	Assumptions/Considerations	Sources
<p><b>Utility consumption, Billing and Generation Data Process Efficiencies and Ongoing Utility Consumption Monitoring and Benchmarking (continued)</b></p>	<p><b>Consultants/service providers (cleaning and consolidating data)</b></p> <ul style="list-style-type: none"> <li>• Annual benefit</li> <li>• 6 hours of effort at \$50/hour (1 hour for Natural Gas and Water)</li> </ul> <p><b>Consultants/service providers (conducting audits)</b></p> <ul style="list-style-type: none"> <li>• Annual benefit</li> <li>• \$150 (electricity only)</li> <li>• \$175 (electricity and Natural Gas)</li> <li>• \$190 (all three utility types)</li> </ul>	<ul style="list-style-type: none"> <li>• Consultants/service providers would experience easier access to data and reduced effort for data cleaning and validation.</li> <li>• Benefits are per building using these services.</li> <li>• Assume 2% of commercial building stock uses these services.</li> <li>• Direct benefit of implementing Green Button.</li> </ul>	<ul style="list-style-type: none"> <li>• Stakeholder consultations and interviews</li> </ul>
<p><b>CDM/DSM Program Efficiencies and Innovations</b></p>	<ul style="list-style-type: none"> <li>• <b>Large LDC:</b> \$10,000/year avoided costs</li> <li>• <b>Medium LDC:</b> \$5,000/year avoided costs</li> <li>• <b>Small LDC:</b> \$2,500/year avoided costs</li> <li>• <b>Large Natural Gas utility:</b> \$5,000/year avoided costs</li> <li>• <b>Small Natural Gas utility:</b> \$2,500/year avoided costs</li> </ul>	<ul style="list-style-type: none"> <li>• Most utilities reported they do not perceive the value proposition that Green Button could provide for their CDM/DSM program design and delivery models. However, they recognize it can bring some benefit to their operations (e.g. through applications that promote CDM/DSM programs or energy savings tips, through increased efficiencies for gathering consumption data for program delivery, customer negotiations, or evaluation).</li> <li>• The analysis therefore included a conservative estimate, based on experience evaluating CDM/DSM programs for electricity and natural gas utilities. While the estimate reflects a lack of specific data, it also reflects our understanding that the value is not zero.</li> <li>• No benefits were attributed to water utilities, considering their earlier stages in conservation program development compared to energy utilities.</li> <li>• Indirect benefit of implementing Green Button.</li> </ul>	<ul style="list-style-type: none"> <li>• Estimates based on utility interviews</li> </ul>

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

Benefit Component	Unit Benefit	Assumptions/Considerations	Sources
<p><b>Behaviour-Based Efficiency and Conservation</b></p>	<p><b>Non-Residential Customers:</b></p> <ul style="list-style-type: none"> <li>2% electricity and natural gas savings for participating customers (non-residential)</li> </ul> <p><b>Residential Customers:</b></p> <ul style="list-style-type: none"> <li>1% electricity and natural gas savings for participating customers (residential)</li> </ul> <p><b>Water Utility Customers:</b></p> <ul style="list-style-type: none"> <li>1% water savings for participating customers (residential and non-residential)</li> </ul>	<ul style="list-style-type: none"> <li>Benefits allocated between utility types based on average energy consumption by sub-sector (residential, small commercial, large commercial, large industrial, and institutional).</li> <li>Based on a conservative reduction of energy savings found to result from behavioural conservation programs designed around access to utility consumption data (access to data typically achieves between 4-12%).</li> <li>Recognizes that savings achieved as a result of Green Button access to data may not achieve the same results as a utility-driven CDM/DSM program (utilities would not have control over all the solutions developed, quality of advice, and other factors). Behavioural-only programs typically achieve between 1 and 3%.<sup>9</sup></li> <li>Benefits assumed to be achieved either through existing CDM/DSM programs or outside of them (e.g. customers make the changes without receiving an incentive). The analysis does not differentiate between whether the savings are generated through utility program participation or not, as behavioural/operational benefits are assumed to require no cost/investment.</li> <li>Benefits assume that utilities would have an opportunity to recruit participants to existing programs (whether or not customers take advantage of the opportunity) rather than assuming new programs will necessarily be developed that could duplicate/compete with existing savings opportunities.             <ul style="list-style-type: none"> <li>This is a conservative assumption – new programs could improve the results.</li> </ul> </li> <li>New programs were excluded due to lack of information on the costs of new DSM/CDM programs based on Green Button information and because of concerns reported by electricity utilities with regards to behavioural savings and their potential contribution to Conservation First Framework 2020 savings targets.</li> <li>Indirect benefit of implementing Green Button.</li> </ul>	<ul style="list-style-type: none"> <li>Professional judgment applied to Murray, M. and J. Hawley. 2016. <i>Got Data? The Value of Energy Data Access to Consumers</i>. Mission:Data</li> <li>Evaluation experience and research into behaviour-based energy savings.<sup>8</sup></li> </ul>

<sup>9</sup> See, for example: [http://ilsagfiles.org/SAG\\_files/Evaluation\\_Documents/ComEd/ComEd\\_EPY7\\_Evaluation\\_Reports/ComEd\\_HER\\_Opower\\_PY7\\_Evaluation\\_Report\\_2016-02-15\\_Final.pdf](http://ilsagfiles.org/SAG_files/Evaluation_Documents/ComEd/ComEd_EPY7_Evaluation_Reports/ComEd_HER_Opower_PY7_Evaluation_Report_2016-02-15_Final.pdf) (average of 1.15% - depending on cohort, savings range from 0.53% to 2.83% electrical savings) [http://www2.opower.com/l/17572/2013-08-22/bvhvp/17572/49284/25\\_ODC\\_Navigant\\_MA\\_Four\\_Year\\_Cross\\_Cutting.pdf](http://www2.opower.com/l/17572/2013-08-22/bvhvp/17572/49284/25_ODC_Navigant_MA_Four_Year_Cross_Cutting.pdf) (presents the findings of behavioural programs of Massachusetts program administrators for electricity and natural gas, which were typically around 1.5%)

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

Benefit Component	Unit Benefit	Assumptions/Considerations	Sources
<p><b>Retrofit-Based Efficiency and Conservation</b></p>	<p><b>Electricity customers:</b></p> <ul style="list-style-type: none"> <li>10% electricity savings per building for participating customers (residential and non-residential)</li> </ul> <p><b>Natural Gas customers:</b></p> <ul style="list-style-type: none"> <li>4% natural gas savings per building for participating customers (residential and non-residential)</li> </ul> <p><b>Water customers:</b></p> <ul style="list-style-type: none"> <li>3% water savings per building for participating customers (residential and non-residential)</li> </ul>	<ul style="list-style-type: none"> <li>Based on conservative reduction of typical energy efficiency evaluation results (not measure-specific), in which energy savings from deeper retrofits (e.g. insulation or building-envelope based) are often 20% or higher.</li> <li>Savings estimated to be incremental to Conservation First Framework/Industrial Accelerator Program and DSM Framework targets.</li> <li>Participation varies by sub-sector based on application of adoption curves (refer to Table 9).</li> <li>We reduced utility results to account for a wide range of measures and retrofits, from simple measures such as selecting a more efficient appliance to a retrofit that improves the insulation level of the building. Therefore, overall savings would be expected to be lower than from a retrofit-only solution.</li> <li>Benefits allocated between utility types based on average energy consumption by sub-sector (residential, small commercial, large commercial, large industrial, and institutional).</li> <li>The analysis of retrofit benefits accounts for utility savings that occur only during the study period (5 years or 10 years, depending on the specific scenario), even though retrofit measures can produce savings over a much longer period.             <ul style="list-style-type: none"> <li>This is a conservative estimate. While it reduces the potential benefits, it limits the risk of overstating the indirect benefits of Green Button and eliminates the uncertainty of the duration of those energy savings.</li> </ul> </li> <li>Benefits were assumed to be achieved either through existing CDM/DSM programs or outside of them (e.g. customers make the changes without receiving an incentive).</li> <li>Indirect benefit of implementing Green Button.</li> </ul>	<ul style="list-style-type: none"> <li>Estimates based on Ontario utility and other Canadian CDM/DSM Plans (e.g. New Brunswick and Nova Scotia) and average Ontario energy rates.</li> </ul>

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

Benefit Component	Unit Benefit	Assumptions/Considerations	Sources
<p><b>Reduced Utility Customer Care Efforts</b></p>	<ul style="list-style-type: none"> <li>• <b>Large LDC:</b> \$10,000/year avoided costs</li> <li>• <b>Medium LDC:</b> \$5,000/year avoided costs</li> <li>• <b>Small LDC:</b> \$2,500/year avoided costs</li> <li>• <b>Large Natural Gas utility:</b> \$5,000/year avoided costs</li> <li>• <b>Small Natural Gas utility:</b> \$2,500/year avoided costs</li> </ul>	<ul style="list-style-type: none"> <li>• Applied to DMD/CMD (not DMD only) since bulk of customer care is for Residential customers who are not expected to participate in a DMD-only implementation to an extent that would demonstrate impact.</li> <li>• Annual cost savings per utility type and size.</li> <li>• Green Button can support new conservation programs based on easier and more streamlined access to consumption data and can reduce cost to procure such services through a single bridge to consumers' utility data.</li> <li>• Direct benefit of implementing Green Button.</li> </ul>	<ul style="list-style-type: none"> <li>• Stakeholder consultations and interviews</li> </ul>

PENETRATION LEVEL

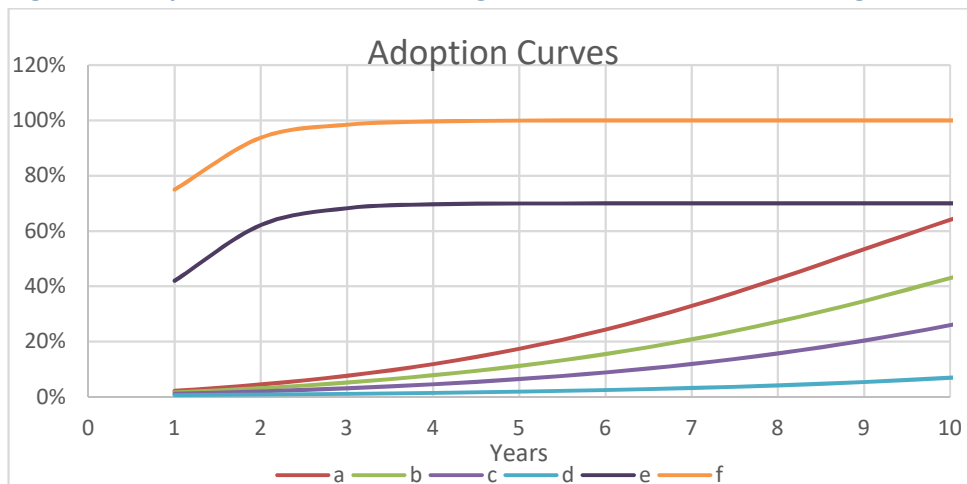
Everett Rogers, whose Diffusion of Innovation theory is used extensively in behavioural and technology-related research, identified that people will adopt new ideas or technologies at different stages, even though benefits may exist from inception. Green Button is no different: despite the benefits that increased access to utility data may have for all customers, some customers will adopt it early in the process (as was seen in the Green Button pilots), others will adopt it over time as it becomes more common and mainstream, and yet others likely never will. These trends are known as adoption curves.

The shape of adoption curves and rate of adoption however, can be different for different technologies and groups. For example, how quickly Green Button is used by a significant number or majority of customers will likely be different by customer group, depending on their individual data needs and requirements. For example, with the Large Building Energy and Water Reporting and Benchmarking initiative, we would expect large commercial, institutional, and industrial customers to adopt Green Button for data access purposes relatively sooner than a majority of residential customers.

For this reason, we developed individual adoption curves to represent the potential adoption of Green Button in the province, varying by benefit and cost category, but also by building type.

The following graph presents the different adoption curves that we applied to different groups using Rogers' Diffusion of Innovation theory, which outlines different ways in which innovations can be adopted based on the innovation itself, communications channels, time, and applicable social systems. The various curves (labelled with the letters a-f) have been applied to different stakeholder groups and benefits, as explained in Table 3 below the graph.

**Figure 5. Adoption curves based on Rogers' Diffusion of Innovation Algorithm**



The above penetration curves have been used for different benefits and building categories included in the model. The specific curves and rationales are outlined in Table 9 below.



**Table 9. Penetration curves included in the analysis**

Benefit/stakeholder	Category	Curve	Rationale
New users of utility data, owners/ managers of large and institutional facilities	Operational Efficiencies	a	Needs expressed during the consultation process were considerable; owner sophistication supports high penetration of Green Button
Retrofits to large commercial and institutional facilities	Increased conservation and energy efficiency	b	Limited to 25% of the building stock undergoing retrofits <sup>10</sup>
Operational benefits for large commercial and institutional facilities	Increased conservation and energy efficiency	c	Significant potential for building managers, resources available to actively manage utility consumption
Retrofits to small commercial buildings	Increased conservation and energy efficiency	c	Limited to 25% of the building stock undergoing retrofits <sup>11</sup>
New small commercial and residential users of utility data	Operational Efficiencies	d	Lower sophistication and availability to manage utility consumption data
Behavioural benefits for small commercial and residential buildings	Increased conservation and energy efficiency	d	Lower sophistication and availability to manage utility consumption
Retrofits to residential buildings	Increased conservation and energy efficiency	d	Limited to 25% of the building stock undergoing retrofits <sup>12</sup>
Large Building Energy and Water Reporting and Benchmarking (O.Reg. 20/17)	Operational Efficiencies	e	Assumes 35% would comply with regulations through means other than Green Button, such as hiring third-party consultants to capture, clean, and consolidate data (so a lower adoption curve has been selected than could be achieved from a technical perspective).
Current users of data (commercial, institutional, and industrial)	Operational Efficiencies	f	Automatic adoption of GB solution by proportion of customers accessing data as indicated by IT survey and interviews.

<sup>10</sup> Calculated based on common values for retrofit savings and research on additional savings (Hummer, J. and D. Brannan. 2014. *Quantifying Behavioral Spillover: The Overlooked, Uncounted Source of Program-Influenced Savings.* Behavior, Energy & Climate Change Conference.)

<sup>11</sup> Ibid

<sup>12</sup> Ibid

## RESULTS OF THE ANALYSIS

As the analysis resulted in multiple iterations of very similar scenarios, this section provides an overview of the high-level results for each dimension of the analysis. In the following section, we provide the specific results of key scenarios that we believe warrant further consideration by the Ministry.

Benefit-cost ratios are provided for each result. As explained above, **if a ratio is positive, the benefits outweigh the costs of that scenario, so it is cost-effective. If it is negative, the costs exceed the benefits and the scenario is not cost-effective.** To make the consideration of such a wide range of scenarios simpler, we have colour-coded the tables: green means the combination of options (the scenario) is cost-effective; red means it is not.

### GREEN BUTTON OPTIONS

The first dimension we analyzed was the consideration of Green Button implementation options: DMD only, or DMD and CMD together. The results show that, in general, a DMD/CMD implementation is more cost-effective across a range of scenarios.<sup>13</sup>

**Table 10. Green Button DMD Scenario Cost-Benefit Results**

Utility Type	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House	
	5-year	10-year	5-year	10-year	5-year	10-year	5-year	10-year
Electricity	2.2	3.5	2.1	3.4	1.8	3.03	1.4	2.5
Electricity and Natural Gas	2.3	2.9	2.1	2.8	1.7	2.5	1.3	2.1
Electricity, Natural Gas, and Water	0.3	0.8	0.6	1.4	0.2	0.5	0.2	0.6
Natural Gas Component	2.4	1.8	2.1	1.7	1.9	1.4	0.5	0.8
Water Component	0.04	0.1	0.1	0.3	0.02	0.1	0.03	0.1

<sup>13</sup> The analysis was built up from a base case of electricity utilities implementing Green Button, to which natural gas utilities were added, and then water utilities. For this reason, in all results tables, the natural-gas-only and water-only components are based on incremental results (the differences in benefits and cost when the other utility types are removed), rather than on independent scenario assumptions.

**Table 11. Green Button DMD/CMD Scenario Cost-Benefit Results**

Utility Type	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House	
	5-year	10-year	5-year	10-year	5-year	10-year	5-year	10-year
Electricity	4.1	3.6	4.04	3.6	3.5	3.5	3.2	3.4
Electricity and Natural Gas	4.4	3.8	4.4	3.8	3.9	3.7	3.5	3.6
Electricity, Natural Gas, and Water	1.9	2.8	1.8	2.8	1.4	2.5	1.1	2.3
Natural Gas Component	6.2	4.9	6.0	5.0	5.6	4.8	5.4	4.7
Water Component	0.5	1.1	0.5	1.04	0.3	0.8	0.3	0.7

As the tables above show, deploying Green Button Connect My Data (CMD) in conjunction with Download My Data (DMD) provides greater benefits than deploying DMD alone. While consistently formatted electronic data downloads (DMD-only) are beneficial for sophisticated customers, **the ability to develop tailor-made solutions and applications and create efficiencies with data transfer and authorization multiply the benefits** when CMD is added.

For this reason, for the remaining scenarios, we present the DMD/CMD option only.

UTILITY TYPE

As part of our analysis, we also examined whether the results changed, and to what extent, based on the type of utility to implement Green Button:

As shown in table 11 above, deploying Green Button for electricity and natural gas only is the most cost-effective option, with ratios ranging between 3.5 and 4.4 (meaning that benefits outweigh the costs by 3.5 to 4 times).

This scenario has the highest results because:

- **The benefits are greatest for electricity:** During stakeholder consultations and interviews, customers indicated they are most interested in energy efficiency and conservation for electricity and most often require data for internal reporting and benchmarking requirements. This perspective is supported by market pricing, with electricity having the highest average rate, followed by natural gas and then water.
- **The setup and integration costs for natural gas are comparatively low:** The setup and integration costs in relation to Green Button benefits are lower for natural gas utilities in comparison to electricity-only or with water utilities included because of the lower number of natural gas utilities.

While the most cost-effective option is electricity and natural gas only, **including water utilities is also cost-effective from a societal level when combined with electricity and natural gas.** However, this is primarily based on the benefits from electricity and natural gas outweighing the costs of implementing Green Button for water. In other words, implementing Green Button for water utilities in and of themselves is generally not cost-effective, because the costs outweigh the benefits when considering water on its own.<sup>14</sup>

**Table 12. Green Button Implementation for Water Utilities Only**

Option	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House	
	5-year	10-year	5-year	10-year	5-year	10-year	5-year	10-year
DMD	0.04	0.1	0.1	0.3	0.02	0.1	0.03	0.1
DMD/CMD	0.5	1.1	0.5	1.04	0.3	0.8	0.3	0.7

This option is not cost-effective under most scenarios for the following reasons:

- **Higher integration costs:**
  - There are a large number of metered water utilities (515), and each one would incur integration and platform development costs.
- **Lower unit benefits per customer:**
  - Customers (excluding large customers) are generally not engaged or interested in water conservation.
  - Water utilities generally distribute bills on a less frequent basis, so there is less opportunity for customers to use the data or receive benefits.

Water may be cost-effective on its own over a 10-year horizon with a Single Integrated Hosted or Multi-Integrated Hosted implementations; however, the result is well within the potential for error. Nevertheless, in developing our analysis, we have erred on the side of being conservative rather than permissive in terms of benefits, so this scenario should not be dismissed solely on a quantitative basis. Additional considerations may demonstrate added benefits.

## IMPLEMENTATION TYPE

Implementation type refers to the type of Green Button platform scenario assessed. As highlighted above, the differences between the implementation types are the following:

<sup>14</sup> Only water utilities with metering infrastructure were included in the analysis. Water utilities not included in the analysis are not generally planning to upgrade their infrastructure in the next five years.

- **Single Integrated (Hosted):** One Green Button hosted Software as a Service (SaaS) platform is used by each utility type (one each for electricity, natural gas, and water utilities).
- **Multi-Integrated (Hosted):** A limited number of Green Button hosted SaaS platforms are used by all utilities.<sup>15</sup>
- **Non-Integrated (Hosted):** Each utility has the option to develop/procure its own Green Button SaaS hosted platform.
- **In-House:** Each utility develops its own platform on its own IT systems.

In terms of Single Integrated (Hosted) and Multi-Integrated (Hosted), the same assumptions were used to develop costs and benefits for both scenarios. However, they were applied differently: we applied the costs to three platforms for the Single Integrated Scenario (one for each utility type) and twelve platforms for the Multi-Integrated Scenario (five for electricity and water, and two for natural gas), which increased the costs for the Multi-Integrated option. The results show that the Single Integrated Hosted implementation option is the most cost-effective option when implementing for all utility types over a five-year timeframe. However, the difference is only 0.1, which is well within a margin of error due to the high-level nature of the analysis. In addition, when implementing for all utility types over a ten-year timeframe or for electricity and natural gas only, both Single Integrated and Multi-Integrated implementations are equally cost-effective.

The assumptions for both the Single Integrated and Multi-Integrated hosted implementation scenarios were identical and further refinement and granularity of results is possible. For example, these scenarios do not fully explore all the potential synergies that may exist through a single or multi-hosted solution for electricity and natural gas utilities. More in-depth research and proposals or more refined quotes from Green Button hosted solutions providers could identify additional cost savings and would also provide an opportunity to increase the accuracy of the cost component of these scenarios. Similarly, the utilities' integration costs could be further researched to increase confidence in these assumptions. For example, they could demonstrate reduced costs in a Multi-Integrated Scenario due to increased competition.

A Non-Integrated Hosted option is assumed to increase costs because of the need to develop a greater number of platforms, and In-House implementation is the least cost-effective because IT hosting is not part of utilities' core business and is therefore the least efficient in terms of costs.

---

<sup>15</sup> This was a hypothetical scenario to demonstration potential synergies in limiting the number of providers; the same assumptions were used for this scenario as for the non-integrated, with the difference being the number of platforms developed and integrated.

Table 13. Green Button Implementation Type Cost-Benefit Results

Utility Type	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House	
	5-year	10-year	5-year	10-year	5-year	10-year	5-year	10-year
Electricity	4.1	3.6	4.04	3.6	3.5	3.5	3.2	3.4
Electricity and Natural Gas	4.4	3.8	4.4	3.8	3.9	3.7	3.5	3.6
Electricity, Natural Gas, and Water	1.9	2.8	1.8	2.8	1.4	2.5	1.1	2.3

## KEY SCENARIOS

This section provides an overview of the key scenarios resulting from the analysis. In general, all scenarios included the costs and benefits assumptions included above. Specific assumptions are provided in the explanations where warranted.

As indicated earlier in this report, our analysis is designed to be conservative, so some benefits that could not be quantified with a relative degree of certainty or documentation were excluded. In addition, because of the limited data for this relatively new initiative, some proxies have been used and high-level assumptions incorporated. Therefore, we recommend interpreting the results with caution, particularly with results for which the benefit-to-cost ratio is close to 1 or in which ratios are similar but not identical. In these cases, small deviations from the assumptions used can lead to different conclusions (e.g., the benefit/cost ratio can fall or rise above 1 or be ranked differently if assumptions change).

For this reason, results from this analysis should be used to guide, not dictate, decisions. Components and considerations not included in the CBA analysis (including qualitative benefits) should also be accounted for in the decision-making process.

### SCENARIO 1: SINGLE INTEGRATED/MULTI-INTEGRATED HOSTED DMD/CMD (ELECTRICITY AND NATURAL GAS ONLY)

This scenario assumes that all Ontario's electricity and natural gas utilities would implement Green Button Download My Data (DMD) and Connect My Data (CMD) for all their customers. In doing so, we assume that there is either a single hosted Software as a Service provider providing this service for all utilities (Single Integrated) or a limited number would serve the market, each with its own platform that would be shared by multiple utilities (Multi-Integrated).

**The key distinction between these scenarios lies in the number of independent Green Button Platforms included in the analysis, e.g., Single Integrated (3 platforms) and Multi-Integrated (12 platforms).** The difference in the number of platforms included in the analysis translates to a cost reduction for the Single Integrated scenario compared to the Multi-Integrated scenario because there are fewer platforms included in this scenario. **There are no differences in the total value of benefits estimated under these two scenarios,** since there is no evidence that the number of independent Green Button platforms would modify the nature and/or value of the benefits generated by Green Button DMD or CMD.

These scenarios are arguably the most cost-effective implementation scenarios analyzed. They capture the vast majority of potential benefits while reducing the costs required for developing and delivering Green Button solutions.

The benefit-cost ratios estimated for these scenarios are of a sufficient magnitude for us to consider them to be highly cost-effective for the province.

SCENARIO 1A: SINGLE INTEGRATED HOSTED DMD/CMD (ELECTRICITY AND NATURAL GAS UTILITIES ONLY)

This section provides an overview of the costs and benefits, in dollars, incorporated within the analysis of a **Single Integrated Green Button implementation for electricity and natural gas utilities only.**

**COSTS**

The following table outlines the cost categories included in the analysis.

**Table 14. Scenario 1A Cost Details**

Cost Category	Cost Type	5-Year Analysis (\$)	10-Year Analysis (\$)	Scenario-Specific Assumptions
Implementation (Utility one-time setup and integration costs)	Direct	3,920,248	3,924,558 <sup>16</sup>	The setup cost for the Single Integrated scenario assumes one setup cost per utility type. This is a conservative estimate based on input from a SaaS provider that indicated a cost per addition of utility type.
Operational Costs <sup>17</sup>	Direct	771,753	2,406,040	
Retrofit Costs	Indirect	11,172,735	67,265,834	
<b>Total</b>		<b>15,864,736</b>	<b>73,596,433</b>	

Operational costs are significantly higher over a 10-year timeframe than over a 5-year timeframe due to increased customer participation with Green Button. Operational costs are directly related to the number of participants. Retrofit costs are significantly higher over 10 years because individuals are less likely to undertake retrofits during the initial few years of Green Button. After implementation, customers will require time to receive their data, analyze it, determine next steps, and implement changes, which delays impacts from retrofits (on both the costs and benefits side) until later in the implementation period.

**BENEFITS**

<sup>16</sup> While in reality the 5-year and 10-year one-time implementation costs would likely be identical, the analysis required a mathematical function to forecast implementation costs. The mathematical function forecasts the following rollout of Green Button through the first 5 years following enactment of the policy: 35%, 70%, 92%, 99%, 99.9%, which means that 0.1% of costs remained to be implemented after the 5-year rollout period and are reflected in the slight increase in one-time costs for the 10-year period.

<sup>17</sup> Sum of net-present value of annual costs over the timeframe.



The following table outlines the benefits categories included in the analysis. We note that **multiple benefits are included in each category, but to avoid double-counting overlapping benefits, they have been aggregated into these higher-level considerations.** The specific benefits included in each category are outlined in Appendix C.

**Table 15. Scenario 1A Benefits Details<sup>18</sup>**

Benefit Category	Benefit Component	Benefit Type	5-Year Analysis (\$)	10-Year Analysis (\$)
Operational Efficiencies	Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	18,072,196	60,083,680
	Process Efficiencies (Large Building Energy and Water Reporting and Benchmarking requirements)	Direct	12,716,122	25,688,618
	Reduced Customer Care Efforts	Indirect	1,082,114	2,455,960
	CDM/DSM Program Efficiencies and Innovation	Indirect	893,384	2,027,619
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	11,413,765	57,765,514
	Increased Conservation - Retrofits	Indirect	26,093,050	134,153,770
	<b>Total</b>		<b>70,270,632</b>	<b>282,175,160</b>

Benefits from improvement in customers’ processes for accessing, cleaning, consolidating, analyzing, and reporting on their utility consumption, billing and generation data are also significantly higher over 10 years than over 5 years. During the initial period following enactment of the policy, customers with a direct interest in simplified access to building consumption data (because they already go through the process of accessing of requesting access to their consumption data in electronic format) are assumed to take advantage of Green Button features. During the next 5-year period, increased usage of Green Button is forecasted, leading to an increase in annual benefits.

Benefits resulting from retrofits are also significantly higher over 10 years than 5 for the same reasons that retrofit costs are higher: the impacts from retrofits will occur later in the period because it will take time for customers to make decisions and implement them.

**RESULTS**

Detailed results for the Single Integrated version of this scenario (Scenario 1A) are presented in the following tables.

<sup>18</sup> No scenario-specific assumptions required

**Table 16. Scenario 1A Benefit-Cost Ratios**

Ratio Type	5-Year Analysis	10-Year Analysis
Direct and Indirect Costs and Benefits	4.4	3.8
Direct Benefits and Costs only <sup>19</sup>	6.8	13.9

In this scenario, total benefits outweigh total costs by over 4 to 1 (over 5 years) or almost 4 to 1 (over 10 years). When analyzing direct benefits and costs only (excluding indirect considerations such as retrofits and program efficiencies, benefits outweigh the costs by almost 7 to 1 (over 5 years) or almost 14 to 1 (over 10 years).

**Additional Results:**

**Table 17. Scenario 1A Energy and GHG Cumulative Impacts**

Result	5-Year Analysis	10-Year Analysis
Electricity Savings	311 GWh	1741 GWh
Natural Gas Savings	1.65 PJ	8.67 PJ
GHG Reductions	168 kt CO <sub>2</sub> e	947 kt CO <sub>2</sub> e

To illustrate how the costs and benefits are distributed across stakeholder groups, we present the following tables.

**Table 18. Scenario 1A Costs by Stakeholder Groups (5-year horizon)**

Cost Component	Cost Type	Stakeholder Group			Total (\$)
		Electricity Utility (\$)	Natural Gas Utility (\$)	Customers <sup>20</sup> (\$)	
Implementation (One-time setup and integration costs)	Direct	3,380,494	539,754	-	<b>3,920,248</b>
Operational Costs <sup>21</sup>	Direct	456,696	315,057	-	<b>771,753</b>
Retrofit Costs	Indirect	-	-	11,172,735	<b>11,172,735</b>
<b>Total</b>		<b>3,837,190</b>	<b>854,811</b>	<b>11,172,735</b>	<b>15,864,736</b>

<sup>19</sup> Direct benefits and costs are a subset of total benefits and costs. However, the direct benefits and costs *ratios* are higher than the total ratios because the magnitude of benefits to costs is different for direct results than for total results.

<sup>20</sup> Includes all customer classes (Residential, Commercial, Industrial, and Institutional)

<sup>21</sup> Sum of net-present value of annual costs over the timeframe.

**Table 19. Scenario 1A Benefits by Stakeholder Group (5-year horizon)**

Benefit Category	Benefit Component	Benefit Type	Stakeholder Group					Total (\$)
			C&I (\$)	Industrial (\$)	Other <sup>22</sup> (\$)	Residential (\$)	Utility (\$)	
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	10,144,702	7,900	5,308,456	2,611,138	-	<b>18,072,196</b>
	Process Efficiencies (requirements)	Direct	12,631,762	84,360	-	-	-	<b>12,716,122</b>
	Reduced Customer Care Efforts	Indirect	-	-	-	-	1,082,114	
	CDM/DSM Program Efficiencies and Innovation	Indirect	-	-	-	-	893,384	
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	9,753,339	14,529	-	1,645,898	-	<b>11,413,765</b>
	Increased Conservation - Retrofits	Indirect	20,106,940	77,336	-	5,908,773	-	<b>26,093,050</b>
	<b>Total</b>		<b>52,636,743</b>	<b>184,125</b>	<b>5,308,456</b>	<b>10,165,809</b>	<b>1,975,478</b>	<b>70,270,631</b>

<sup>22</sup> Other Stakeholders include third-party Energy Efficiency Consultants/Service Providers providing utility consumption monitoring services, energy assessments, and/or engineering services.

**SCENARIO 1B: MULTI-INTEGRATED HOSTED DMD/CMD (ELECTRICITY AND NATURAL GAS UTILITIES ONLY)**

The table below provides an overview of the costs and benefits, in dollars, incorporated within the analysis of a Multi-Integrated Green Button implementation for electricity and natural gas utilities only.

We note that all costs and benefits are the same as for the Single Integrated scenario except for the Implementation (one-time setup and integration) costs. This is why the scenarios are labelled 1A and 1B rather than as two different scenarios.

**Table 20. Scenario 1B Cost Details**

Cost Category	Cost Type	5-Year Analysis (\$)	10-Year Analysis (\$)	Scenario-Specific Assumptions
Implementation (One-time setup and integration costs)	Direct	4,101,232	4,105,742 <sup>23</sup>	The setup cost for the Multi-Integrated scenario assumes: <ul style="list-style-type: none"> <li>• 5 independent platforms for the electricity sector</li> <li>• 1 platform for the natural gas sector (because there are so few utilities)</li> <li>• 5 platforms for the water utilities</li> </ul>
Operational Costs <sup>24</sup>	Direct	771,753	2,406,040	
Retrofit Costs	Indirect	11,172,735	67,265,834	
<b>Total</b>		<b>16,045,720</b>	<b>73,777,616</b>	

While most costs are approximately double when comparing the 10-year period to the 5-year period, the retrofit costs are significantly higher over 10 years because individuals are less likely to undertake retrofits during the initial few years of Green Button. After implementation, customers will require time to receive their data, analyze it, determine next steps, and implement changes, which delays impacts from retrofits (on both the costs and benefits side) until later in the implementation period.

<sup>23</sup> Differences between the 5-year and 10-year Implementation Costs are an artefact of the mathematical function used to forecast implementation costs. The mathematical function forecasts the following rollout of Green Button through the first 5 years following enactment of the policy: 35%, 70%, 92%, 99%, 99.9%.

<sup>24</sup> Sum of net-present value of annual costs over the timeframe.

**Table 21. Scenario 1B Benefits Details<sup>25</sup>**

Benefit Category	Benefit Component	Benefit Type	5-Year Analysis (\$)	10-Year Analysis (\$)
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	18,072,196	60,083,680
	Process Efficiencies (Large Building Energy and Water Reporting and Benchmarking)	Direct	12,716,122	25,688,618
	Reduced Customer Care Efforts	Indirect	1,082,114	2,455,960
	CDM/DSM Program Efficiencies and Innovation	Indirect	893,384	2,027,619
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	11,413,765	57,765,514
	Increased Conservation - Retrofits	Indirect	26,093,050	134,153,770
	<b>Total</b>		<b>70,270,632</b>	<b>282,175,160</b>

Benefits from improvement in customers' processes for accessing, cleaning, consolidating, analyzing, and reporting on their utility consumption, billing and generation data are significantly higher over 10 years than over 5 years. During the initial period following enactment of the policy, customers with a direct interest towards simplified access to building consumption data (because they already go through the process of accessing of requesting access to their consumption data in electronic format) are assumed to take advantage of Green Button features. During the next 5-year period, increased usage of Green Button is forecasted, leading to an increase in annual benefit.

Benefits resulting from retrofits are also significantly higher over 10 years than 5 for the same reasons that retrofit costs are higher: the impacts from retrofits will occur later in the period because it will take time for customers to make decisions and implement them.

The remaining benefits are approximately double when comparing a 10-year horizon to a 5-year horizon, meaning that a relatively steady and regular pace of benefits are incurred each year.

**RESULTS**

Detailed results for the Multi-Integrated version of this scenario (Scenario 1B) are presented in the following tables.

<sup>25</sup> No scenario-specific assumptions required

**Benefit-Cost Ratios:**

**Table 22. Scenario 1B Benefit-Cost Ratios**

Ratio Type	5-Year Analysis	10-Year Analysis
Direct and Indirect Costs and Benefits	4.4	3.8
Direct Benefits and Costs only <sup>26</sup>	6.8	13.6

**ADDITIONAL RESULTS:**

**Table 23. Scenario 1B Energy and GHG Cumulative Impacts**

Result	5-Year Analysis	10-Year Analysis
Electricity Savings	311 GWh	1741 GWh
Natural Gas Savings	1.65 PJ	8.67 PJ
GHG Reductions	168 kt CO <sub>2</sub> e	947 kt CO <sub>2</sub> e

Note that the energy and GHG impacts are identical to Scenario 1A, as the only differences between the two scenarios are in the costs; there are no differences in the benefits.

To illustrate how the costs and benefits are distributed across stakeholder groups, we present the following tables.

**Table 24. Scenario 1B Costs by Stakeholder Group (5-year horizon)**

Cost Category	Cost Type	Stakeholder Group			Total (\$)
		Electricity Utility (\$)	Natural Gas Utility (\$)	Customers <sup>27</sup> (\$)	
Implementation (One-time setup and integration costs)	Direct	3,561,478	539,754	-	<b>4,101,232</b>
Operational Costs <sup>28</sup>	Direct	456,696	315,056	-	<b>771,752</b>
Retrofit Costs	Indirect	-	-	11,172,735	<b>11,172,735</b>
<b>Total</b>		<b>4,018,174</b>	<b>854,810.5</b>	<b>11,172,735</b>	<b>16,045,720</b>

<sup>26</sup> Direct benefits and costs are a subset of total benefits and costs. However, the direct benefits and costs *ratios* are higher than the total ratios because the magnitude of benefits to costs is different for direct results than for total results.

<sup>27</sup> Includes all customer classes (Residential, Commercial, Industrial, and Institutional)

<sup>28</sup> Sum of net-present value of annual costs over the timeframe.

**Table 25. Scenario 1B Benefits by Stakeholder Group (5-year horizon)**

Benefit Category	Benefit Component	Benefit Type	Stakeholder Group					Total (\$)
			C&I (\$)	Industrial (\$)	Other <sup>29</sup> (\$)	Residential (\$)	Utility (\$)	
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	10,144,702	7,900	5,308,456	2,611,138	-	<b>18,072,196</b>
	Process Efficiencies (requirements)	Direct	12,631,762	84,360	-	-	-	<b>12,716,122</b>
	Reduced Customer Care Efforts	Indirect	-	-	-	-	1,082,114	<b>1,082,114</b>
	CDM/DSM Program Efficiencies and Innovation	Indirect	-	-	-	-	893,384	<b>893,384</b>
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	9,753,339	14,529	-	1,645,898	-	<b>11,413,765</b>
	Increased Conservation - Retrofits	Indirect	20,106,940	77,336	-	5,908,773	-	<b>26,093,050</b>
	<b>Total</b>		<b>52,636,743</b>	<b>184,125</b>	<b>5,308,456</b>	<b>10,165,809</b>	<b>1,975,498</b>	<b>70,270,632</b>

<sup>29</sup> Other Stakeholders include third-party Energy Efficiency Consultants/Service Providers providing utility consumption monitoring services, energy assessments, and/or engineering services.

## SCENARIO 2: SINGLE INTEGRATED/MULTI-INTEGRATED HOSTED DMD/CMD: ELECTRICITY, NATURAL GAS AND WATER

The second key scenario assumes that all of Ontario's metered electricity, natural gas and water utilities would implement Green Button Download My Data (DMD) and Connect My Data (CMD) for all their customers. The implementation could occur with either a single hosted Software as a Service provider providing the service for all utilities (Single Integrated) or a small group of Software as a Service providers serving the market through a limited number of platforms shared by multiple utilities (Multi-Integrated).

As with Scenario 1A and 1B (for Electricity and Natural Gas utilities only), the key distinction between these scenarios lies in the number of independent Green Button Platforms included in the analysis (i.e., Single Integrated (3) and Multi-Integrated (12)). The difference in the number of platforms included in the analysis translates to a cost reduction for the Single Integrated Scenario compared to the Multi-Integrated scenario. On the benefits side, there are no differences between the two, as there is no evidence that the number of independent Green Button platforms would modify the nature and/or value of the benefits generated by Green Button CMD.

The benefit-cost ratios for these scenarios indicate they are cost-effective, albeit to a lesser extent than the electricity and natural gas-only scenarios. The lower benefit-to-cost ratio is primarily driven by:

- Higher setup and integration costs required by the large number of water utilities in the province (because each utility requires its own setup costs).
- A lower benefit for water utility customers than for electricity and natural gas customers relating to conservation and access to billing and generation data. Specifically, customers consider access to their water consumption and billing data to be of less value than access to their electricity and natural gas data, and they are less concerned about conservation opportunities. This lower level of concern results in fewer benefits when Green Button is implemented for water utilities.

These two factors considerably reduce the value proposition of this scenario from a purely numbers-based perspective. As noted above, however, additional considerations not included in the quantitative analysis may be equally important and should inform part of the Ministry's policy.

Additional synergies that reduce set-up and integration costs could have a profound impact on the result of this analysis, considering they would apply to a much higher number of utilities. For example, if only the largest water utilities were included in the implementation (the 37 largest utilities serve approximately 78% of Ontario's population), it would reduce the number of implementations drastically. Another example would be to set up a water-focused task force to explore options that reduce integration costs for small utilities.



SCENARIO 2A: SINGLE INTEGRATED HOSTED DMD/CMD (ALL UTILITY TYPES)

The table below provides an overview of the costs and benefits, in dollars, incorporated within the analysis of a Single Integrated Green Button implementation for all utility types.

**Table 26. Scenario 2A Cost Details**

Cost Category	5-Year Analysis (\$)	10-Year Analysis (\$)	Scenario-Specific Assumptions
Implementation (One-time setup and integration costs)	30,408,975	30,442,411	The setup cost for the Single Integrated scenario assumes one setup cost per utility type. This is based on input from a SaaS provider that indicated a cost per addition of utility type and was selected to provide a conservative estimate.
Operational Costs <sup>30</sup>	1,225,917	3,822,160	
Retrofit Costs	13,290,836	79,923,128	
<b>Total</b>	<b>44,925,728</b>	<b>114,187,699</b>	

As indicated above, implementation and operational costs are significantly higher because of the number of water utilities: 590 utilities are included in this scenario (of which 515 are water utilities), compared with 75 in Scenarios 1A and 1B. The number of utilities translates into a multiplication of these costs.

10-year costs are significantly higher than 5-year costs for the same reasons as Scenarios 1A and 1B: individuals are less likely to undertake retrofits during the initial few years of Green Button. After implementation, customers will require time to receive their data, analyze it, determine next steps, and implement changes, which delays impacts from retrofits (on both the costs and benefits side) until later in the implementation period.

<sup>30</sup> Sum of net-present value of annual costs over the timeframe.

**Table 27. Scenario 2A Benefits Details<sup>31</sup>**

Benefit Category	Benefit Component	Benefit Type	5-Year Analysis (\$)	10-Year Analysis (\$)
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	25,228,276	78,289,889
	Process Efficiencies (Large Building Energy and Water Reporting and Benchmarking)	Direct	14,835,476	29,970,054
	Reduced Customer Care Efforts	Indirect	1,639,242	3,720,413
	CDM/DSM Program Efficiencies and Innovation	Indirect	1,712,222	4,609,824
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	14,071,675	71,530,678
	Increased Conservation - Retrofits	Indirect	26,802,103	137,226,936
	<b>Total</b>		<b>84,288,994</b>	<b>325,347,793</b>

Benefits from improvement in customers' processes for accessing, cleaning, consolidating, analyzing, and reporting on their utility consumption, billing and generation data are significantly higher over 10 years than over 5 years. During the initial period following enactment of the policy, customers with a direct interest towards simplified access to building consumption data (because they already go through the process of accessing of requesting access to their consumption data in electronic format) are assumed to take advantage of Green Button features. During the next 5-year period, increased usage of Green Button is forecasted, leading to an increase in annual benefit.

Benefits from increased conservation (retrofits and behavioural) are only marginally larger in this scenario than in Scenarios 1A and 1B because our research indicated that water conservation is not a primary concern for customers, who are more likely to invest in electricity and natural gas conservation.

**RESULTS**

Detailed results for the Single Integrated version of this scenario (Scenario 1B) are presented in the following tables.

<sup>31</sup> No scenario-specific assumptions required

**Table 28. Scenario 2A Benefit-Cost Ratios**

Ratio Type	5-Year Analysis	10-Year Analysis
Direct and Indirect Costs and Benefits	1.9	2.8
Direct Benefits and Costs only <sup>32</sup>	1.3	3.3

Scenario 2A, in which water utilities have been added to the analysis for a Single Integrated Hosted solution of both DMD and CMD, is cost effective when considering total costs and benefits.

While the analysis shows that considering direct costs and benefits only (i.e., excluding actions that are only indirectly resulting from a Green Button implementation, such as energy efficiency and conservation retrofits) is also cost-effective, the 5-year analysis is close enough to 1 (i.e., the benefits do not substantially outweigh the costs) that we cannot be confident in that particular result, since the data inputs and considerations are not granular enough to assume results close to 1 are definitely cost-effective.

However, we note that the analysis was designed to be conservative, in that we intentionally used mid-to-low range estimates of benefits, and mid-to-high ranges of costs, in order to provide as rigorous an analysis as possible within the scope of the work.

**ADDITIONAL RESULTS:**

**Table 29. Scenario 2A Energy and GHG Cumulative Impacts**

Result	5-Year Analysis	10-Year Analysis
Electricity Savings	311 GWh	1741 GWh
Natural Gas Savings	1.65 PJ	8.67 PJ
Water	1,567,203 m <sup>3</sup>	8,466,860 m <sup>3</sup>
GHG Reductions	168 kt CO <sub>2</sub> e	947 kt CO <sub>2</sub> e

To illustrate how the costs and benefits are distributed across stakeholder groups, we present the following tables.

---

<sup>32</sup> Direct benefits and costs are a subset of total benefits and costs. However, the direct benefits and costs *ratios* are higher than the total ratios because the magnitude of benefits to costs is different for direct results than for total results.

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

**Table 30. Scenario 2A Costs by Stakeholder Group (5-year horizon)**

Cost Category	Cost Type	Stakeholder Group				
		Electricity Utility (\$)	Natural Gas Utility (\$)	Water Utility (\$)	Customers (\$)	Total (\$)
Implementation (One-time setup and integration costs)	Direct	3,380,494	539,754	26,488,727	-	<b>30,408,975</b>
Operational Costs <sup>33</sup>	Direct	456,696	315,057	454,164	-	<b>1,225,917</b>
Retrofit Costs	Indirect	-	-	-	13,290,836	<b>13,290,836</b>
<b>Total</b>		<b>3,837,190</b>	<b>854,811</b>	<b>26,942,892</b>	<b>13,290,836</b>	<b>44,925,729</b>

**Table 31. Scenario 2A Benefits by Stakeholder Group (5-year horizon)**

Benefit Category	Benefit Component	Benefit Type	Stakeholder Group					
			C&I (\$)	Industrial (\$)	Other <sup>34</sup> (\$)	Residential (\$)	Utility (\$)	Total (\$)
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	12,285,408	9,875	10,038,462	2,894,531	-	<b>25,228,276</b>
	Process Efficiencies	Direct	14,737,056	98,420	-	-	-	<b>14,835,476</b>
	Reduced Customer Care Efforts	Indirect	-	-	-	-	1,639,242	<b>1,639,242</b>
	CDM/DSM Program Efficiencies and Innovation	Indirect	-	-	-	-	1,712,222	<b>1,712,222</b>
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	12,407,375	18,403	-	1,645,898	-	<b>14,071,675</b>
	Increased Conservation - Retrofits	Indirect	20,106,940	77,336	-	6,617,826	-	<b>26,802,103</b>
	<b>Total</b>		<b>59,536,779</b>	<b>204,035</b>	<b>10,038,462</b>	<b>11,158,255</b>	<b>3,351,464</b>	<b>84,288,994</b>

<sup>33</sup> Sum of net-present value of annual costs over the timeframe.

<sup>34</sup> Other Stakeholders include third-party Energy Efficiency Consultants/Service Providers providing utility consumption monitoring services, energy assessments, and/or engineering services.

SCENARIO 2B: MULTI-INTEGRATED HOSTED DMD/CMD (ALL UTILITY TYPES)

The table below provides an overview of the costs and benefits, in dollars, incorporated within the analysis of a Multi-Integrated Green Button implementation for electricity and natural gas utilities only.

**Table 32. Scenario 2B Cost Details**

Cost Category	Cost Type	5-Year Analysis (\$)	10-Year Analysis (\$)	Scenario-Specific Assumptions
Implementation (One-time setup and integration costs)	Direct	31,338,419	31,372,876	The setup cost for the Multi-Integrated scenario assumes: <ul style="list-style-type: none"> <li>• 5 independent platforms for the electricity sector</li> <li>• 1 platform for the natural gas sector (because there are so few utilities)</li> <li>• 5 platforms for the water utilities</li> </ul>
Operational Costs <sup>35</sup>	Direct	1,225,917	3,822,160	
Retrofit Costs	Indirect	13,290,836	79,923,128	
<b>Total</b>		<b>45,855,172</b>	<b>115,118,164</b>	

The costs are the same in this scenario as for the Single Integrated (All Utilities) scenario except for the Implementation (one-time setup and integration) costs. This is because the only assumptions that changed for the Multi-Integrated Scenario were the number of platforms (12 compared to 3), which then increased the platform setup and integration costs. All other assumptions remain the same. This is why the scenarios are labelled 2A and 2B rather than as two different scenarios.

<sup>35</sup> Sum of net-present value of annual costs over the timeframe.

**Table 33. Scenario 2B Benefits Details<sup>36</sup>**

Benefit Category	Benefit Component	Benefit Type	5-Year Analysis (\$)	10-Year Analysis (\$)
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	25,228,276	78,289,889
	Process Efficiencies	Direct	14,835,476	29,970,054
	Reduced Customer Care Efforts	Indirect	1,639,242	3,720,413
	CDM/DSM Program Efficiencies and Innovation	Indirect	1,712,222	4,609,824
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	14,071,675	71,530,678
	Increased Conservation - Retrofits	Indirect	26,802,103	137,226,936
	<b>Total</b>		<b>84,288,994</b>	<b>325,347,793</b>

The benefits for this Scenario are identical to those in the Single Integrated (All Utilities) Scenario, as our research indicated the benefits would not differ based on the number of platforms implemented.

**RESULTS**

Detailed results for the Multi-Integrated version of this scenario (Scenario 2B) are presented in the following tables.

**Table 34. Scenario 2B Benefit-Cost Ratios**

Ratio Type	5-Year Analysis	10-Year Analysis
Total	1.8	2.8
Direct Benefits and Costs only <sup>37</sup>	1.3	3.3

The results for this scenario are identical to the results for the Single Integrated scenario (2A) because the difference between the two are only related to the costs for developing 12 platforms (for Multi-Integrated) rather than 5 platforms (for Single Integrated). These costs are minimal compared to the overall costs, so the difference is eliminated through rounding the numbers to one decimal place. In other words, it is insignificant.

<sup>36</sup> No scenario-specific assumptions required

<sup>37</sup> Direct benefits and costs are a subset of total benefits and costs. However, the direct benefits and costs ratios are higher than the total ratios because the magnitude of benefits to costs is different for direct results than for total results.

**ADDITIONAL RESULTS:**

**Table 35. Scenario 2B Energy and GHG Cumulative Impacts**

Result	5-Year Analysis	10-Year Analysis
Electricity Savings	311 GWh	1741 GWh
Natural Gas Savings	1.65 PJ	8.67 PJ
Water	1,567,203 m <sup>3</sup>	8,466,860 m <sup>3</sup>
GHG Reductions	168 kt CO <sub>2</sub> e	947 kt CO <sub>2</sub> e

To illustrate how the costs and benefits are distributed across stakeholder groups, we present the following tables.

**Table 36. Scenario 2B Costs by Stakeholder Group (5-year horizon)**

Cost Category	Cost Type	Stakeholder Group				
		Electricity Utility (\$)	Natural Gas Utility (\$)	Water Utility (\$)	Customers (\$)	Total (\$)
Implementation (One-time setup and integration costs)	Direct	3,561,478	539,754	27,237,186	-	<b>31,338,419</b>
Operational Costs <sup>38</sup>	Direct	456,696	315,057	454,164	-	<b>1,225,917</b>
Retrofit Costs	Indirect	-	-	-	13,290,836	<b>13,290,836</b>
<b>Total</b>		<b>4,018,174</b>	<b>854,811</b>	<b>27,691,351</b>	<b>13,290,836</b>	<b>45,855,172</b>

<sup>38</sup> Sum of net-present value of annual costs over the timeframe.

**Table 37. Scenario 2B Benefits by Stakeholder Group (5-year horizon)**

Benefit Category	Benefit Component	Benefit Type	Stakeholder Group					Total (\$)
			C&I (\$)	Industrial (\$)	Other (\$)	Residential (\$)	Utility (\$)	
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	12,285,408	9,875	10,038,462	2,894,531	-	<b>25,228,276</b>
	Process Efficiencies	Direct	14,737,056	98,420	-	-	-	<b>14,835,476</b>
	Reduced Customer Care Efforts	Indirect	-	-	-	-	1,639,242	<b>1,639,242</b>
	CDM/DSM Program Efficiencies and Innovation	Indirect	-	-	-	-	1,712,222	<b>1,712,222</b>
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	12,407,375	18,403	-	1,645,898	-	<b>14,071,675</b>
	Increased Conservation - Retrofits	Indirect	20,106,940	77,336	-	6,617,826	-	<b>26,802,103</b>
	<b>Total</b>		<b>59,536,779</b>	<b>204,035</b>	<b>10,038,462</b>	<b>11,158,255</b>	<b>3,351,464</b>	<b>84,288,994</b>



## DIRECT AND INDIRECT COSTS

The tables on the following pages provide an overview of the total costs (in dollars) by key scenario, over five- and ten-year timeframes as well as subsequent breakouts of direct and indirect costs.

We note that these costs are high level and used to generate comparisons between potential scenarios; they are not implementation-level cost estimates.

**FIVE-YEAR HORIZON**

**Table 38. Total Benefits and Costs, Combining Direct and Indirect (5-year horizon)**

5 Years	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House	
	Benefits	Costs	Benefits	Costs	Benefits	Costs	Benefits	Costs
Electricity	\$54,348,157	\$13,239,659	\$54,348,157	\$13,420,643	\$54,348,157	\$15,353,563	\$54,348,157	\$17,153,013
Electricity and Natural Gas	\$70,270,632	\$15,864,736	\$70,270,632	\$16,045,720	\$70,270,632	\$18,255,315	\$70,270,632	\$20,133,528
Electricity, Natural Gas, and Water	\$84,288,994	\$44,925,729	\$84,288,994	\$45,855,172	\$84,288,994	\$59,527,055	\$84,288,994	\$73,435,858

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

**Table 39. Breakout of Direct and Indirect Benefits and Costs, Single- and Multi-Integrated (5-year horizon)**

5 Years	Single Integrated Hosted				Multi-Integrated Hosted			
	Benefits		Costs		Benefits		Costs	
	Direct	Indirect	Direct	Indirect	Direct	Indirect	Direct	Indirect
Electricity	\$24,638,139	\$29,710,018	\$3,837,190	\$9,402,468	\$24,638,139	\$29,710,018	\$4,018,174	\$9,402,468
Electricity and Natural Gas	\$31,903,633	\$38,366,999	\$4,692,001	\$11,172,735	\$31,903,633	\$38,366,999	\$4,872,985	\$11,172,735
Electricity, Natural Gas, and Water	\$42,555,032	\$41,733,962	\$31,634,892	\$13,290,836	\$42,555,032	\$41,733,962	\$32,564,336	\$13,290,836

**Table 40. Breakout of Direct and Indirect Benefits and Costs, Non-Integrated and In-House (5-year horizon)**

5 Years	Non-Integrated Hosted				In-House			
	Benefits		Costs		Benefits		Costs	
	Direct	Indirect	Direct	Indirect	Direct	Indirect	Direct	Indirect
Electricity	\$24,638,139	\$29,710,018	\$5,951,095	\$9,402,468	\$24,638,139	\$29,710,018	\$7,750,544	\$9,402,468
Electricity and Natural Gas	\$31,903,633	\$38,366,999	\$7,082,579	\$11,172,735	\$31,903,633	\$38,366,999	\$8,960,793	\$11,172,735
Electricity, Natural Gas, and Water	\$42,555,032	\$41,733,962	\$46,236,219	\$13,290,836	\$42,555,032	\$41,733,962	\$60,145,022	\$13,290,836

**TEN-YEAR HORIZON**

**Table 41. Total Benefits and Costs, Combining Direct and Indirect (10-year horizon)**

10 Years	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House	
	Benefits	Costs	Benefits	Costs	Benefits	Costs	Benefits	Costs
Electricity	\$220,141,043	\$60,938,670	\$220,141,043	\$61,119,853	\$220,141,043	\$63,155,925	\$220,141,043	\$65,199,079
Electricity and Natural Gas	\$282,267,635	\$73,635,939	\$282,267,635	\$73,777,616	\$282,267,635	\$76,187,875	\$282,267,635	\$78,477,384
Electricity, Natural Gas, and Water	\$325,440,269	\$114,227,205	\$325,440,269	\$115,118,165	\$325,440,269	\$129,204,994	\$325,440,269	\$143,778,684

COST-BENEFIT ANALYSIS REPORT

Green Button Consultation and Cost Benefit Analysis

**Table 42. Breakout of Direct and Indirect Benefits and Costs, Single and Multi-Integrated (10-year horizon)**

10 Years	Single Integrated Hosted				Multi-Integrated Hosted			
	Benefits		Costs		Benefits		Costs	
	Direct	Indirect	Direct	Indirect	Direct	Indirect	Direct	Indirect
Electricity	\$68,380,297	\$151,760,747	\$4,808,314	\$56,130,356	\$68,380,297	\$151,760,747	\$4,989,497	\$56,130,356
Electricity and Natural Gas	\$88,303,608	\$193,871,551	\$6,330,599	\$67,265,834	\$88,303,608	\$193,871,551	\$6,511,782	\$67,265,834
Electricity, Natural Gas, and Water	\$114,637,912	\$210,709,882	\$34,264,571	\$79,923,128	\$114,637,912	\$210,709,882	\$35,195,036	\$79,923,128

**Table 43. Breakout of Direct and Indirect Benefits and Costs, Non-Integrated and In-House (10-year horizon)**

10 Years	Non-Integrated Hosted				In-House			
	Benefits		Costs		Benefits		Costs	
	Direct	Indirect	Direct	Indirect	Direct	Indirect	Direct	Indirect
Electricity	\$68,380,297	\$151,760,747	\$7,166,269	\$56,130,356	\$68,380,297	\$151,760,747	\$9,209,423	\$56,130,356
Electricity and Natural Gas	\$88,303,608	\$193,871,551	\$9,132,166	\$67,265,834	\$88,303,608	\$193,871,551	\$11,420,804	\$67,265,834
Electricity, Natural Gas, and Water	\$114,637,912	\$210,709,882	\$49,530,676	\$79,923,128	\$114,637,912	\$210,709,882	\$64,103,496	\$79,923,128

## QUALITATIVE BENEFITS

In addition to the purely numerical analysis presented above, Green Button provides additional benefits to customers, utilities and the Government. Benefits that were minimal, could not be quantified or estimated due to a lack of data, or could not be robustly or clearly attributed to Green Button were excluded from the analysis presented above. However, this does not mean they are not important considerations.

We recommend the Ministry's use the quantitative analysis provided above to inform its proposal. However, the proposal should not be limited to this assessment; qualitative benefits should also be considered. The following are benefits related to Green Button that were confirmed by our research but were not included in the quantitative analysis for the reasons explained above:

- **Increased energy efficiency awareness/education:** Customers benefit from increased awareness about energy efficiency and utilities benefit from opportunities to educate their customers through Green Button applications. While some of these benefits are quantified through increased conservation efforts resulting from access to data, our research indicates additional opportunities exist that would result in higher benefits were they able to be quantified or confirmed.
- **Increased real estate value:** Access to data about utility costs for buildings (homes and commercial buildings) can increase real estate value when these buildings are for sale. However, this value tends to increase over time, as the market becomes attuned to looking for, and basing decisions on, this type of information. For this reason, the benefits would not be material in the early years. In addition, they would not be material because they would be a subset (of buildings sold on the market) of a subset (of buildings that had retrofits resulting from Green Button). In addition, while initiatives such as Home Energy Rating and Disclosure are being examined and planned in Ontario, without an immediate launch, owners will not be required to provide this information, leading to even lower potential benefits due to lack of consistency until programs launch. For this reason, we were not able to estimate the impacts, and we expect them to be minimal in the early years. However, over time, we suggest these benefits will play a larger role in overall Green Button benefits.
- **Increased customer satisfaction:** While increased customer satisfaction as a result of customers understanding their utility consumption and changes to bills can be quantified in terms of survey scale results, it is difficult to convert this satisfaction to dollars saved on the part of utilities. There is not an automatic, direct link between customer satisfaction and reduced customer care centre calls, for example. Therefore, we were not able to include this benefit in the quantified analysis. Nevertheless, it can be an important benefit to utilities at a qualitative level.
- **Innovation in CDM/DSM programs:** Future CDM/DSM programs being developed as a result of Green Button Connect My Data, including to assist with Pay-for-Performance program design, are a very real

possibility of a province-wide implementation of Green Button. We therefore included a token amount as an indirect benefit; however, it is not significant and not to the extent that could be expected for the following reasons:

- We did not have enough data to suggest the magnitude of such programs (either in terms of costs or savings).
- Concerned about the risk of relying on behavioural change to achieve their 2020 targets, electricity utilities were clear they were not specifically planning to design these programs in the near future.
- There is the potential for evaluation efficiencies related to easier, real-time access to consistent, machine-readable data; however, while utilities admitted this potential existed, they could not see how it could be executed.

We therefore believe there are benefits of CDM/DSM program innovation resulting from Green Button, but we were not able to quantify them to a great extent in the analysis.

- **Supporting government policy objectives:** An important benefit of Green Button is its ability to support government policy objectives, including helping to reduce fossil fuel emissions from enhanced customer access to utility data (as stated in Ontario’s Climate Change Action Plan). Another example is the Minister’s directive to the Ontario Energy Board to provide guidance and expectations to utilities within three parameters, one of which is customer control (defined as “providing the customer with increased information and tools to promote conservation of electricity”).<sup>39</sup> The Board highlights Green Button as an example for utilities to provide consumption data to their customers in a user-friendly format in order to achieve customer control objectives. Green Button is able to support these, and other similar objectives. However, the quantified dollar value cannot be estimated and is therefore addressed qualitatively only.
  
- **Economic development and innovation (i.e., improved access to North American market, supporting development of innovative services):** Third-party solution providers/application developers indicated that a province-wide implementation of Green Button would provide them with an important opportunity to develop applications that could be used in a broader North American market and support the development of innovative services. In addition, customer access to data could result in job creation and positive economic impact in Ontario (through increased demand for consultant/service provider services, greater efficiencies in existing organizations, etc.). While some of these benefits can be quantified, to do so requires a great number of assumptions that we believed would reduce the robustness and validity of the outputs. We therefore elected to exclude them from the model and address them qualitatively.

---

<sup>39</sup> Ontario Energy Board. 2013. *Supplemental Report on Smart Grid*. EB-2011-0004. February 11, 2013.

## CONCLUSION

Dunsky's cost-benefit analysis of mandating Green Button in Ontario, conducted for Ontario's Ministry of Energy, was designed to assess the cost-effectiveness of implementing Green Button across a range of scenarios, with variables focused on:

- **Green Button Options:** DMD only or DMD/CMD;
- **Utility Type:** Electricity, Natural Gas, Water; and
- **Implementation Type:** Single Integrated (Hosted), Multi-Integrated (Hosted), Non-Integrated (Hosted), In-House.

To develop inputs and obtain feedback on the results of the analysis, we consulted a broad range of stakeholders, including utilities, customers, government and intra-sector organizations, third-party service providers, and non-profit groups and associations.

The results of our analysis indicate that implementing Green Button in Ontario will be cost-effective from a societal standpoint. When focusing purely on the numbers, **implementing Green Button DMD/CMD across electricity and natural gas utilities is the most cost-effective path forward.**

Adding water utilities to the implementation is also a cost-effective scenario from a societal standpoint under a single-integrated or multi-integrated model. However, this is primarily based on the benefits from electricity and natural gas outweighing the costs of implementing Green Button for water. In other words, implementing Green Button for water utilities in and of themselves is generally not cost-effective, because the costs outweigh the benefits when considering water on its own.

In addition, implementing Green Button Connect My Data (CMD) in conjunction with Download My Data (DMD) provides the greatest benefits, and a single-integrated or multi-integrated implementation (with one, or a limited number of Green Button platforms for each utility type) is the most cost-effective implementation type, with negligible differences in results between the two.

We note that our analysis was high-level and designed to assess whether or not benefits outweighed the costs of a Green Button implementation. It does not contain enough granularity to assess actual implementation costs. Qualitative considerations such as increases in awareness of energy efficiency, real estate value, customer satisfaction, and CDM/DSM program innovation, and economic development and innovation, as well as support for government policy objectives would also increase the value of a Green Button implementation. They have not, however, been included within the quantitative analysis. For these reasons, any of the scenarios included in this report should be considered valid outputs to assist the Ministry in moving forward with a proposal for a Green Button implementation in Ontario.



**APPENDIX A: COST-BENEFIT ANALYSIS RESULTS STAKEHOLDER PRESENTATION**

# ONTARIO GREEN BUTTON COST-BENEFIT ANALYSIS Results

JULY 2016



**dunsky**  
ENERGY CONSULTING

[www.dunsky.com](http://www.dunsky.com)  
(514) 504-9030 | [info@dunsky.com](mailto:info@dunsky.com)



# TABLE OF CONTENTS

Overview and Methodology

Assumptions and Considerations

Cost-Benefit Analysis Results

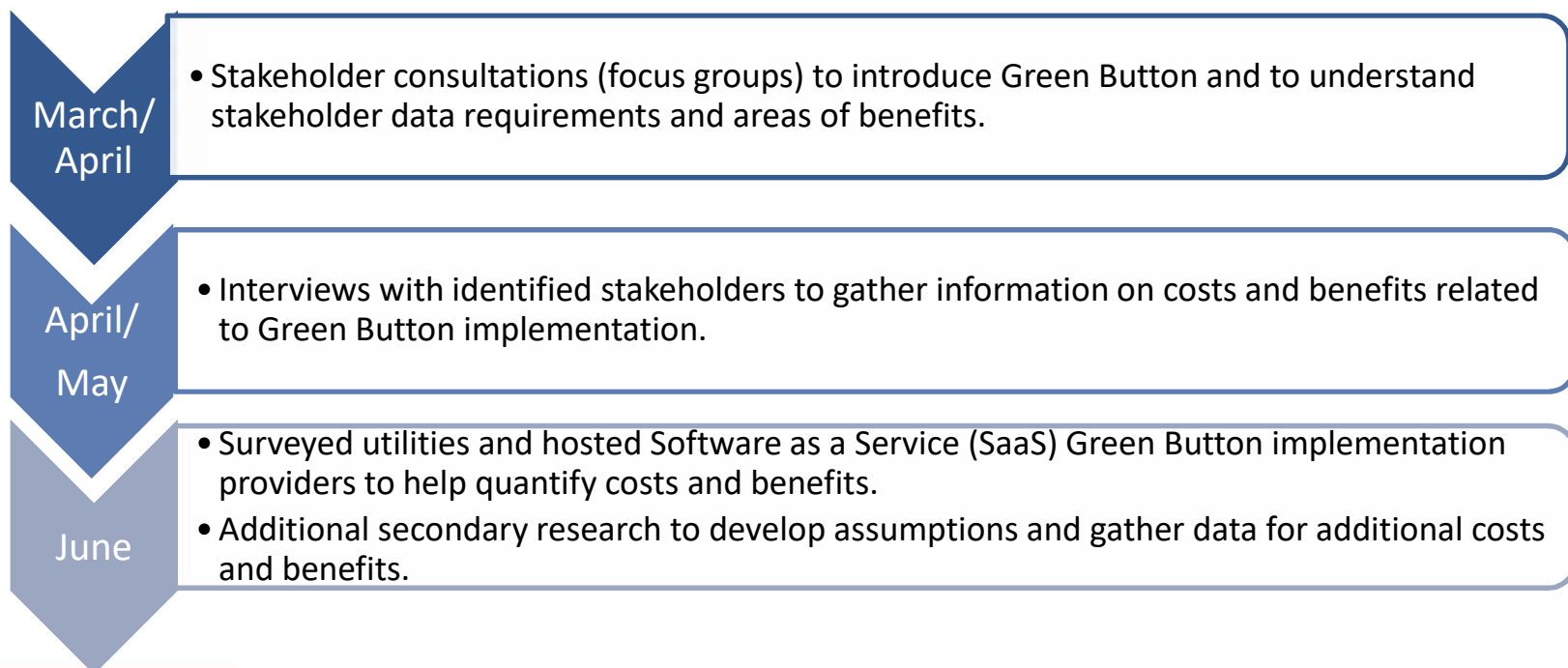
Appendices



# OVERVIEW

## ■ Objective:

- ▶ Assess the impacts of implementing Green Button in Ontario across a range of potential scenarios to help inform the Ministry of Energy's Green Button proposal.



# COST-BENEFIT ANALYSIS METHODOLOGY



1. Stakeholder Consultations

2. Primary and Secondary Research

3. Inputs and Assumptions

4. Implementation Scenarios

4. Scenario Analysis



# COSTS & BENEFITS – CATEGORIZATION



## QUANTITATIVE

### Direct (Layer 1A)

- Benefits and costs are a direct result of Green Button implementation
- Monetary value can be estimated based on available information

### Indirect (Layer 2A)

- Indirect consequence of Green Button implementation
- Require an additional external influence or decision point in order to materialize
- Monetary value can be estimated based on available information

## QUALITATIVE

### (Layer 2B)

- Not included in Cost-Benefit Model
- Reported as “additional costs/benefits”
- Used in overall analysis and policy recommendations



# COSTS AND BENEFITS

- Quantitative categories included in the cost-benefit analysis are presented below.
- The analysis is conservative.
  - ▶ Benefits that were minimal, could not be quantified or estimated, or could not be attributed clearly to Green Button were excluded or included in the qualitative benefits.

	Item	Impacted Groups*	Category
Costs	<ul style="list-style-type: none"> <li>• Implementation – one-time set-up costs (platform development and utility integration)</li> </ul>	Hosted SaaS GB Implementation Providers, Utilities	Direct, Quantified
	<ul style="list-style-type: none"> <li>• Operational - annual</li> </ul>	Utilities	Direct, Quantified
	<ul style="list-style-type: none"> <li>• Energy efficiency retrofits</li> </ul>	Customers	Indirect, Quantified
Benefits (Quantified)	<ul style="list-style-type: none"> <li>• Resource and time efficiencies due to simplified process and standard format related to accessing data (i.e., for internal or external monitoring, or benchmarking requirements)</li> <li>• Included for customers/service providers currently monitoring and benchmarking, and for new customer requirements resulting from Bill 135</li> </ul>	Customers, Service Providers	Direct, Quantified
	<ul style="list-style-type: none"> <li>• Increased energy efficiency and conservation (behavioural, operational, retrofit), both within and outside of existing CDM/DSM programs</li> </ul>	Customers**	Indirect, Quantified
	<ul style="list-style-type: none"> <li>• Reduced customer care effort</li> </ul>	Utilities	Indirect, Quantified
	<ul style="list-style-type: none"> <li>• CDM/DSM program efficiencies and innovations</li> </ul>	Utilities	Indirect, Quantified

\*Groups to which costs and benefits are assigned.

\*\*Benefits are assigned to end-users only (not utilities) to avoid double-counting.





# COSTS AND BENEFITS

- Qualitative categories are presented below but were not included in the cost-benefit analysis calculations.

	Item	Impacted Groups*	Category
Benefits (Not Quantified)	Increased energy efficiency awareness/education	Customers, Utilities	Direct, Qualitative
	Increased real estate value	Customers	Direct, Qualitative
	Increased customer satisfaction	Utilities	Direct, Qualitative
	Innovation in CDM/DSM programs	Utilities	Direct, Qualitative
	Supporting government policy objectives	Utilities, Government	Direct, Qualitative
	Economic development and innovation (i.e., improved access to North American market, supporting development of innovative services)	Service Providers, Government	Direct, Qualitative

\*Groups to which costs and benefits are assigned.



# KEY DRIVERS - COSTS

## ■ Setup Costs

- ▶ Setup costs are mostly influenced by the utility's integration services.\*
- ▶ For utility types with a significant number of individual utilities (e.g., water and electricity), the number of independent platforms represent a significant portion of the costs.

## ■ Annual Costs

- ▶ Ongoing annual costs are influenced mostly by the penetration of Green Button in Ontario.
- ▶ Directly related to activity level on the platform.

\*i.e., integration with customer portals, Extract, Transform, Load (ETL) systems, meter data, MDM/R; testing; marketing; security and privacy validation.



# KEY DRIVERS - BENEFITS

## ■ Benefits – ~85% in Commercial and Institutional (C&I) Sector

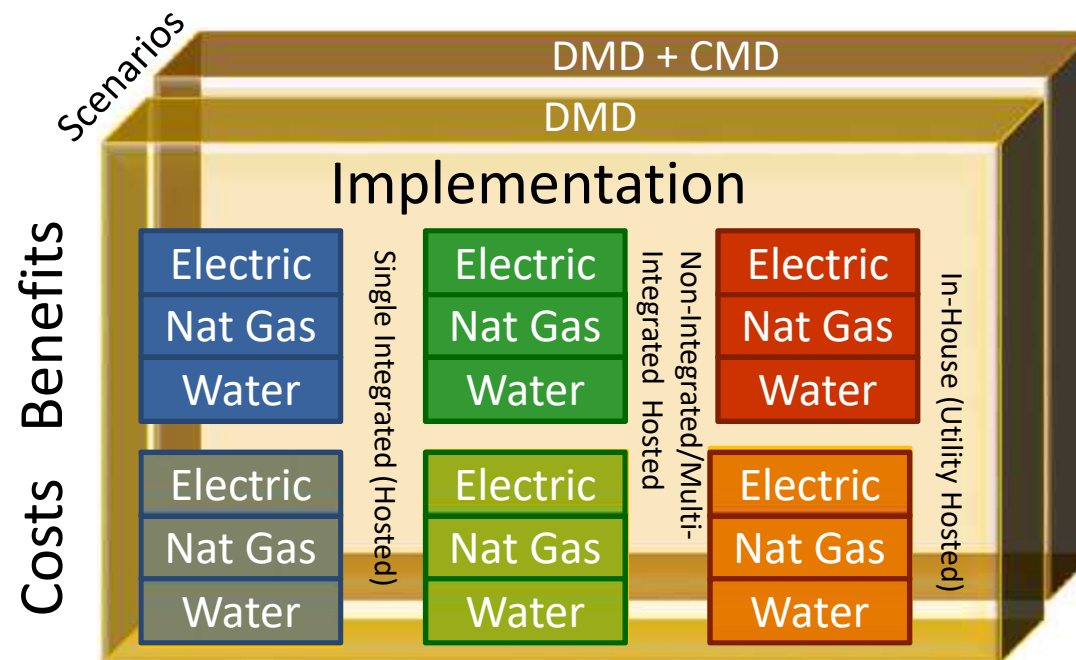
1. Increased Conservation – Energy Efficiency (EE) Retrofit and Behavioural (indirect benefit from Green Button)
  - *Green Button provides customers with more timely and easier access to data so they are more likely to undertake EE actions*
  - *Greatest benefits are in C&I EE Retrofit*
  - *2<sup>nd</sup> greatest benefits are in C&I Behavioural and Operational*
2. Future Large Building Energy and Water Reporting and Benchmarking requirements (Bill 135) (indirect benefit from Green Button)
  - *~18,000 buildings are expected to be required to annually report monthly energy and water consumption*
  - *Green Button provides a simplified process to collect this information*
3. Increased Efficiencies in Consumption, Billing and Generation Data Processes – replace existing processes (direct benefit from Green Button)
  - *Reduced efforts to collect and process utility consumption data*
  - *Reduced efforts to collect and process utility bills*
  - *Reduced efforts for data validation and quality control*

# SCENARIOS



## ■ 3 Dimensions

- ▶ **Utility Type:** Electric, Natural Gas, Water
- ▶ **Implementation Type:** Single Integrated (Hosted), Multi-Integrated/Non-Integrated (Hosted), In-House
- ▶ **Green Button Option:** DMD, DMD+CMD





# GREEN BUTTON OPTION

Option	Details
<b>Green Button Download My Data (DMD)</b>	<ul style="list-style-type: none"><li>• Provides customers with the ability to download their utility data directly, through their utilities' websites</li><li>• Data is downloaded in XML and is provided in a consistent format</li></ul>
<b>Green Button Connect My Data (CMD)</b>	<ul style="list-style-type: none"><li>• Provides customers with the ability to share their data with solution providers and compatible databases in an automated way, based on consumer authorization</li><li>• Process follows Privacy By Design principles</li></ul>



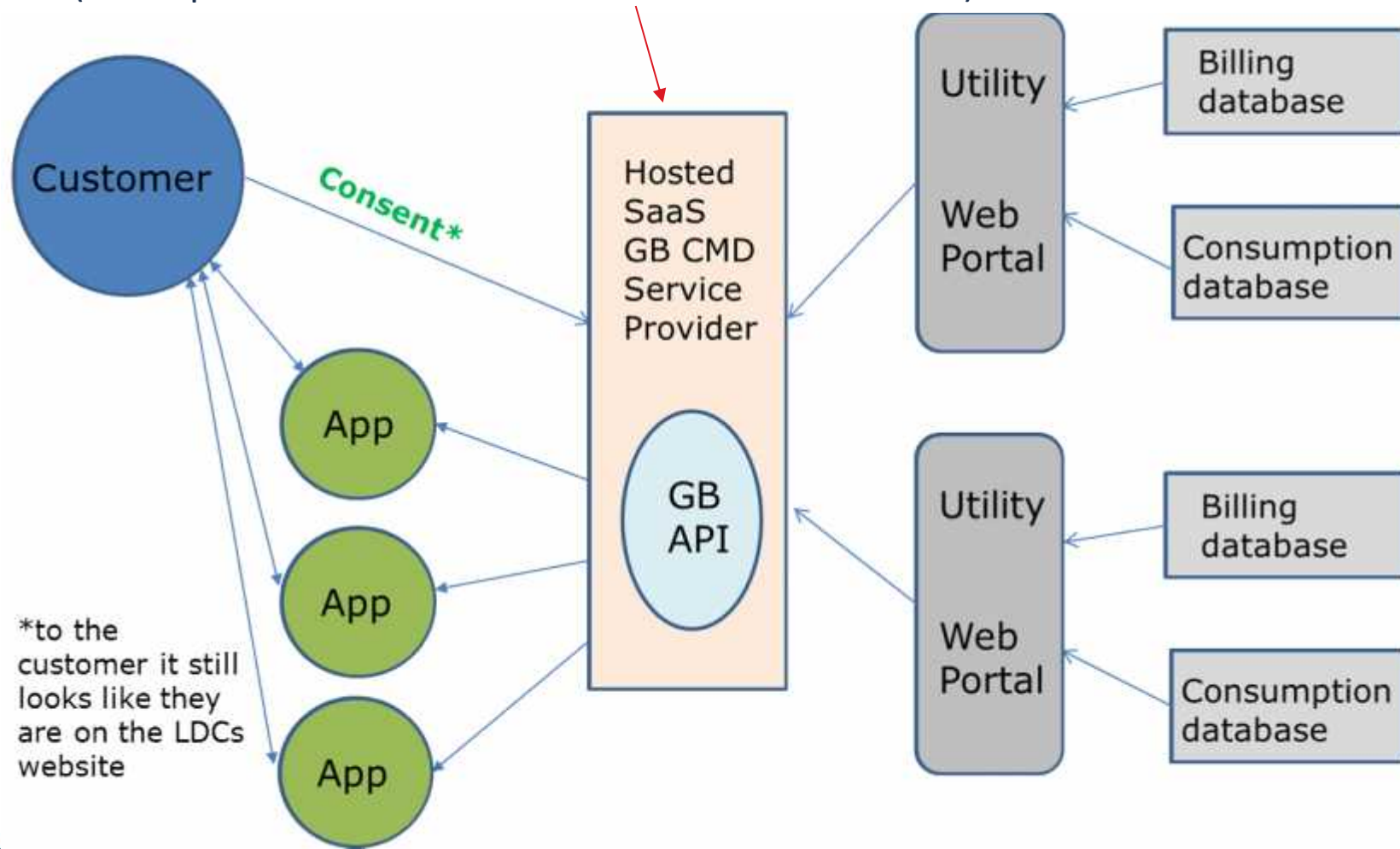
# UTILITY TYPE

Utility Type	Key Factors in Analysis	Details
<b>Electricity</b>	Utility Population and Sizes	• 7 Large, 21 Medium, 44 Small
	Metering Infrastructure	<ul style="list-style-type: none"> <li>• All are metered</li> <li>• Most have completed smart meter implementation for Residential and Small Commercial</li> <li>• Submeters exist for many buildings (but unknown to what extent by utilities)</li> </ul>
	Total Number of Accounts	• 5,162,768 accounts
<b>Natural Gas</b>	Utility Population and Sizes	• 2 Large, 1 Small
	Metering Infrastructure	<ul style="list-style-type: none"> <li>• All are metered</li> <li>• Combination of Automatic Meter Reading (AMR) and analog meters</li> </ul>
	Total Number of Accounts	• 3,423,622 accounts
<b>Water</b>	Utility Population and Sizes	• 39 Large, 91 Medium, 550 Small
	70% of Small Water Utilities are Metered	• Only metered utilities included in analysis
	Of the Metered Utilities: Utility Population and Sizes	• 39 Large, 91 Medium, 385 Small
	Total Number of Accounts	• 4,955,366 accounts



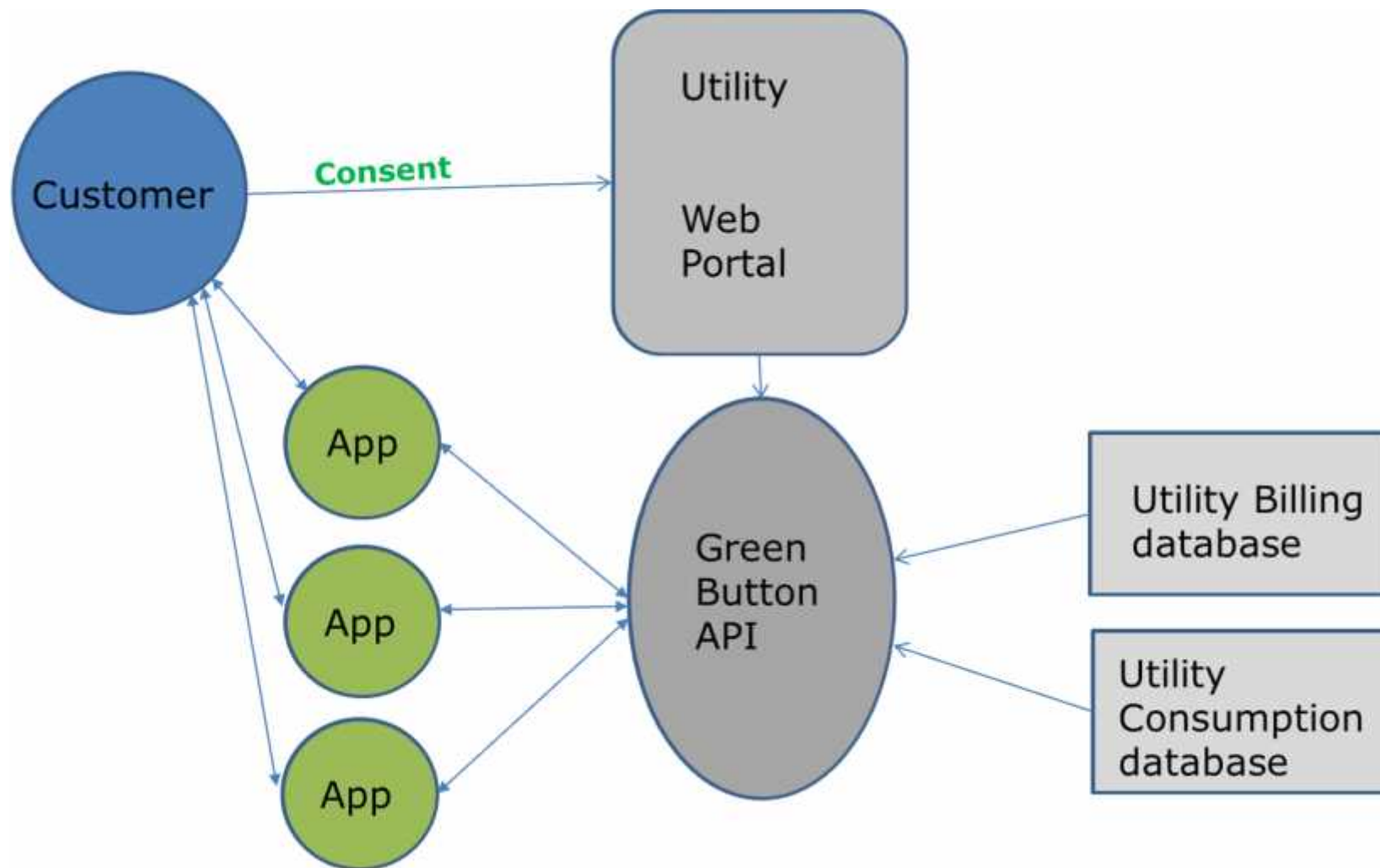
# IMPLEMENTATION TYPE: HOSTED

- Difference between hosted implementation types is in the number of providers (fewer providers creates efficiencies in cost and effort)





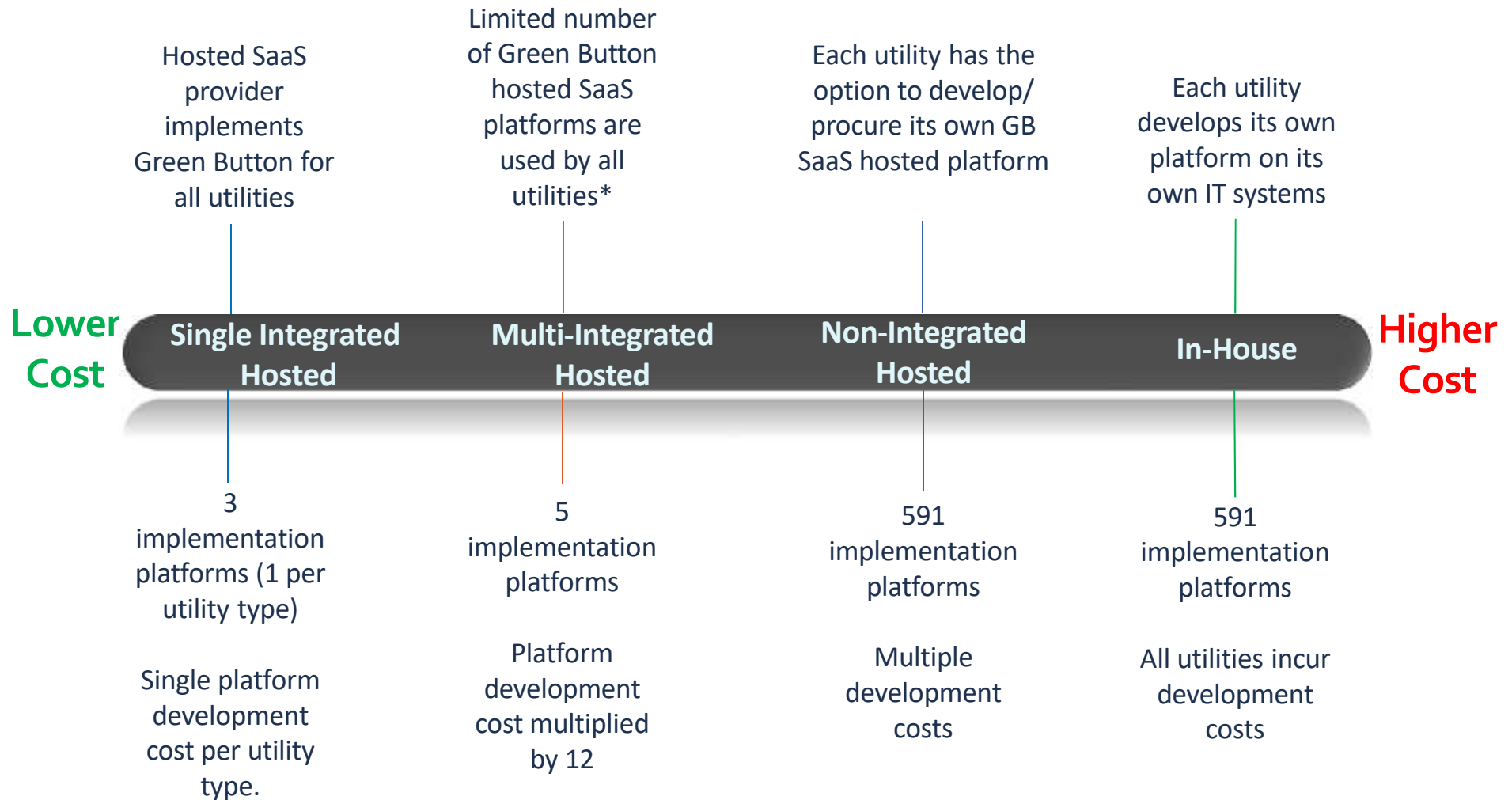
# IMPLEMENTATION TYPE: IN-HOUSE







# IMPLEMENTATION TYPE



\*Hypothetical scenario demonstrating potential synergies



# RESULTS



# CONTEXT AND CONSIDERATIONS

- Green Button is a relatively new standard, with little existing data on implementation.
  - ▶ Information gathered was largely new and primary-source based.
  - ▶ Data for some sectors and/or costs and benefits is more widely available than others.
  - ▶ Where detailed, granular data does not exist or the project scope did not allow for in-depth research, our team developed assumptions and proxies.
    - *The analysis shows scenarios that are cost-effective and ones that are not.*
    - *There is a margin of error associated with the results. Ratios should not be interpreted as exact; they should be interpreted as indicative.*
  
- Results are presented at the societal level, not for individual sectors or customer groups.
  - ▶ However, the results have been built up from inputs at the sector and customer-group level rather than developed from a top-down approach.
  
- Results include both direct and indirect benefits.



# SUMMARY OF SCENARIO RESULTS

## ■ Benefit/Cost Ratios of Green Button DMD only

Utility Type	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House	
	5-year	10-year	5-year	10-year	5-year	10-year	5-year	10-year
Electricity	2.2	3.5	2.1	3.4	1.8	3.03	1.4	2.5
Electricity and Natural Gas	2.3	2.9	2.1	2.8	1.7	2.5	1.3	2.1
Electricity, Natural Gas, and Water	0.3	0.8	0.6	1.4	0.2	0.5	0.2	0.6
Natural Gas Component**	2.4	1.8	2.1	1.7	1.9	1.4	0.5	0.8
Water Component**	0.04	0.1	0.1	0.3	0.02	0.1	0.03	0.1

\*Utility-hosted

\*\*Incremental results



# SUMMARY OF SCENARIO RESULTS

## ■ Benefit/Cost Ratios of Green Button DMD/CMD

Utility Type	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House*	
	5-year	10-year	5-year	10-year	5-year	10-year	5-year	10-year
Electricity	4.1	3.6	4.04	3.6	3.5	3.5	3.2	3.4
Electricity and Natural Gas	4.4	3.8	4.4	3.8	3.9	3.7	3.5	3.6
Electricity, Natural Gas, and Water	1.9	2.8	1.8	2.8	1.4	2.5	1.1	2.3
Natural Gas Component**	6.2	4.9	6.0	5.0	5.6	4.8	5.4	4.7
Water Component**	0.5	1.1	0.5	1.04	0.3	0.8	0.3	0.7

\*Utility-hosted

\*\*Incremental results

# RESULTS: GREEN BUTTON OPTION



- Deploying Green Button Connect My Data (CMD) in conjunction with Download My Data (DMD) provides greater benefits than DMD alone.
  - ▶ While consistently formatted electronic data downloads (DMD-only) are beneficial for sophisticated customers, the ability to develop tailor-made solutions and applications and create efficiencies with data transfer and authorization multiply the benefits when CMD is added.



# RESULTS: UTILITY TYPES

- Deploying Green Button for electricity and natural gas only is the most cost-effective option.
  - ▶ The benefits are highest for electricity, and the costs are lower for natural gas because there are so few utilities.
- Including water is cost-effective from a societal level when combined with electricity and natural gas.
- However, this is primarily based on the benefits from electricity and natural gas outweighing the costs of implementing Green Button for water.
  - ▶ The majority of water utilities are small, with limited resources and minimal IT and metering infrastructure.
  - ▶ The costs to become “Green Button ready” would be significant for them, and the benefits are limited.
  - ▶ Only water utilities with metering infrastructure were included in the analysis. Water utilities not included in the analysis are not generally planning to upgrade their infrastructure in the next five years.



# WATER UTILITIES

- Implementing Green Button for all water utilities on their own (i.e. not combined with electricity and natural gas) is not cost-effective under most options due to:
  - ▶ Higher integration costs:
    - *Large number of metered water utilities*
    - *Each one results in multiplied integration and platform costs*
  - ▶ Lower unit benefits per customer. For example:
    - *Lack of engagement in water conservation (not including large customers)*
    - *Lower bill frequency (so less chance to use data/receive benefits)*
- Water **may** be cost-effective on its own with Single Integrated Hosted and Multi-Integrated Hosted implementations over a 10-year horizon.
  - ▶ The result is well within the margin of error.
  - ▶ However, in developing our analysis, we have erred on the side of being conservative rather than permissive in terms of benefits.

Option	Single Integrated Hosted		Multi-Integrated Hosted		Non-Integrated Hosted		In-House*	
	5-year	10-year	5-year	10-year	5-year	10-year	5-year	10-year
DMD	0.04	0.1	0.1	0.3	0.02	0.1	0.03	0.1
DMD/CMD	0.5	1.1	0.5	1.04	0.3	0.8	0.3	0.7





# WATER UTILITIES

- There are some options that increase the cost-effectiveness of implementing Green Button for water utilities on their own, including implementing it only for the largest utilities:
  - ▶ 37 utilities, representing ~78% of the population
  - ▶ Lower integration costs:
    - *Fewer number of utilities, reducing integration and platform costs*
  - ▶ Larger number of customers per utility, reducing the per-customer cost

Deployment	Non-Integrated Hosted		Single Integrated Hosted		In-House*	
	5-year	10-year	5-year	10-year	5-year	10-year
DMD/CMD	1.7	1.7	1.2	1.8	0.8	1.4



# RESULTS: IMPLEMENTATION TYPE

- The Single Integrated Hosted implementation is the most cost-effective option when implementing for all utility types.\*
- Single Integrated and Multi-Integrated Hosted are equally cost-effective when implementing only for electricity and natural gas.
- A Non-Integrated Hosted option is assumed to increase costs because of the need to develop a greater number of platforms.
- In-House Hosting is the least efficient because it is not part of utilities' core business.

\*For Green Button DMD+CMD over 10 years, a Multi-Integrated implementation has the same cost-benefit ratio as the Single Integrated option.

# KEY SCENARIO 1: SINGLE INTEGRATED/MULTI-INTEGRATED HOSTED ELECTRICITY & NATURAL GAS



Dimension	Results	
Cost-Benefit Ratio	5-Year Horizon	4.4
	10-Year Horizon	3.8
Utility Type	Electricity and Natural Gas	
Implementation	Single Integrated Hosted; Multi-Integrated Hosted	
Green Button Option	Download My Data and Connect My Data	



## KEY SCENARIO 2: SINGLE INTEGRATED HOSTED ELECTRICITY, NATURAL GAS & WATER

Dimension	Results	
Cost-Benefit Ratio	5-Year Horizon	1.9
	10-Year Horizon	2.8
Utility Type	Electricity, Natural Gas and Water	
Implementation	Single Integrated Hosted	
Green Button Option	Download My Data and Connect My Data	

# KEY SCENARIO 3: MULTI-INTEGRATED HOSTED ELECTRICITY, NATURAL GAS & WATER



Dimension	Results	
Cost-Benefit Ratio	5-Year Horizon	1.8
	10-Year Horizon	2.8
Utility Type	Electricity, Natural Gas and Water	
Implementation	Multi-Integrated Hosted	
Green Button Option	Download My Data and Connect My Data	

## APPENDIX B: COST-BENEFIT ANALYSIS INPUT ASSUMPTIONS

**Green Button Cost-Benefit Analysis Input Assumptions**

**Appendix B**

**General Inputs:**

General Input	Source	Notes
Discount Rate (Societal): 2%	IESO real discount rate (CDM EE Cost-Effectiveness Test Guide): <a href="http://www.ieso.ca/-/media/files/ieso/document-library/conservation/ldc-toolkit/cdm-ee-cost-effectiveness-test-guide-v2-20150326.pdf?la=en">http://www.ieso.ca/-/media/files/ieso/document-library/conservation/ldc-toolkit/cdm-ee-cost-effectiveness-test-guide-v2-20150326.pdf?la=en</a> Ontario long-term bond rates: <a href="http://www.ofina.on.ca/pdf/bond_issue_details_DMTN228_to_R19.pdf">http://www.ofina.on.ca/pdf/bond_issue_details_DMTN228_to_R19.pdf</a>	Adjustment to IESO real discount rate of 4% (CDM EE Cost-Effectiveness Test Guide) to reflect conservative view of 30-year Ontario real bond rates of 1.2%). The social discount rate represents the public benefit perspective of the Green Button framework, and based on industry practices, normally reflects the long-term treasury bonds borrowing rates. For the Green Button Framework analysis, considering the IESO social discount rate, a 2% social discount rate was selected.
Inflation Rate: 1.7%	Ontario's annual inflation rate in June 2016: <a href="http://inflationcalculator.ca/2016-cpi-and-inflation-rates-for-ontario/">http://inflationcalculator.ca/2016-cpi-and-inflation-rates-for-ontario/</a>	As per leading industry practices, the cost-effectiveness analysis uses real values, and do not require adjustments for inflation.
Monetary values base year: 2016	Costs and benefits are expressed in 2016 values.	
Participation in Green Button	Rogers' Diffusion of Innovation	Varies by cost/benefit category

**Population Inputs:**

Group to which Costs/Benefits are Assigned	Sub Group	Population	Source	Submeter penetration	Source
Buildings/ Facilities	Large Commercial	32,011	Statistics Canada, Survey of Commercial and Institutional Energy use - Buildings 2009	0.03%	Estimates developed from IT Survey
	Small Commercial	112,672	Statistics Canada	0.40%	
	Large Industrial	120	Statistics Canada	0	
	Institutional	19,630	Statistics Canada	0.03%	
	Residential	3,342,822	Statistics Canada, Private Households, by structural type of dwellings	3.40%	
Total Utility Accounts per customer type	Large Commercial	54,706	OEB 2014 Yearbook of Electricity Distributors; Utility IT Survey; For water utilities: based on proportion of electric to water accounts	0.03%	Estimates for percentage of accounts by customer type developed from IT Survey
	Small Commercial	432,565		0.40%	
	Large Industrial	120		0.00%	
	Institutional	19,637	0.03%		
	Residential	4,655,740	OEB 2014 Yearbook of Electricity Distributors; Utility IT Survey; For water utilities: based on population in each municipality, average number of individuals per household in Ontario	3.40%	
Electricity Utility	Large	7	OEB 2014 Yearbook of Electricity Distributors		
Electricity Utility	Medium	21	OEB 2014 Yearbook of Electricity Distributors		
Electricity Utility	Small	44	OEB 2014 Yearbook of Electricity Distributors		
Natural Gas Utility	Large	2	OEB 2014 Yearbook of Natural Gas Distributors		
Natural Gas Utility	Small	1	OEB 2014 Yearbook of Natural Gas Distributors		
Water Utility	Large	39	<a href="http://www.watertapontario.com/asset-map/utilities/water-and-wastewater-utilities">http://www.watertapontario.com/asset-map/utilities/water-and-wastewater-utilities</a>		
Water Utility	Medium	91	<a href="http://www.watertapontario.com/asset-map/utilities/water-and-wastewater-utilities">http://www.watertapontario.com/asset-map/utilities/water-and-wastewater-utilities</a>		
Water Utility	Small	385	Assumes 70% are metered (IT Survey); <a href="http://www.watertapontario.com/asset-map/utilities/water-and-wastewater-utilities">http://www.watertapontario.com/asset-map/utilities/water-and-wastewater-utilities</a>		

**Green Button Cost-Benefit Analysis Input Assumptions**

**Appendix B**

**Costs:**

Category and Input	Source	Notes
<b>One-Time Green Button Implementation Costs</b>		
<i>Use Case: Set-Up and Integration Costs - One Time - DMD/CMD</i>		
<b>Key Inputs:</b>		
Platform Setup Costs	Stakeholder Interviews, Solution Providers survey	Includes front-end solutions, cloud services, Green Button platform, development and testing, and registration costs
Utility Integration Costs, variable by utility size	Stakeholder interviews with Ontario GB Pilot utilities	Includes ETL protocols and other integration costs such as integration with customer portals, meter data, external testing and validation, etc.
Variability by implementation scenario	Professional judgement and stakeholder interviews	Setup Costs account for the number of platforms in each implementation scenario (single integrated = 3 (1 per utility type), in-house/non-integrated = 591 (1 per utility)), multi-integrated = 12 (5 per utility type except 2 for natural gas) Efficiencies increase from in-house, to non-integrated, to single-integrated. Separate assumptions were not developed for multi-integrated hosted (centralized assumptions were used with a simple multiplication of development costs)
Forecasted Participation	Professional judgement	100% implementation within 4 years: 35%, 70%, 92%, 100% Accounts for current implementation of DMD and CMD in electricity utilities
<i>Use Case: Set-Up and Integration Costs - One Time - DMD</i>		
<b>Key Inputs:</b>		
Platform Setup Costs	Stakeholder Interviews, Solution Providers survey	Includes front-end solutions, cloud services, Green Button platform, development and testing (including of required security and privacy mechanisms and protocols), and registration costs
Utility Integration Costs, variable by utility size	Stakeholder interviews	Subset of DMD/CMD costs, based on cost breakdown and professional judgment. Includes ETL protocols and other integration costs such as integration with customer portals, meter data, external testing and validation, etc.
Variability by implementation scenario	Professional judgement and stakeholder interviews	Setup Costs account for the number of platforms in each implementation scenario (single integrated = 3 (1 per utility type), in-house/non-integrated = 591 (1 per utility)), multi-integrated = 12 (5 per utility type except 2 for natural gas) Efficiencies increase from in-house, to non-integrated, to single-integrated. Separate assumptions were not developed for multi-integrated hosted (centralized assumptions were used with a simple multiplication of development costs)
Forecasted Participation	Professional judgement	100% implementation within 4 years: 35%, 70%, 92%, 100% Accounts for current implementation of DMD in electricity utilities
<b>Annual Green Button Implementation Costs</b>		
<b>Key Inputs:</b>		
Annual Variable cost by participating customer	Stakeholder Interviews	Costs are for maintenance and ongoing operations
Impact of Implementation Scenarios	Professional judgement and stakeholder interviews	Efficiencies increase from utility-hosted, to non-integrated hosted, to single-integrated.
Forecasted Participation	Modeled through the Adoption/Penetration Rate analysis	
<b>Retrofit Costs</b>		
Costs are total measure costs.		
<b>General Notes:</b>	They do not include potential costs from new programs developed as a result of Green Button or additional program administrator costs that could be incurred due to higher participation in CDM/DSM programs (which are not a one-to-one relationship).	
<b>Key Inputs:</b>		
Unit Costs of Retrofit Activity (\$/conservation benefit)	Ontario utility and other Canadian CDM/DSM Plans	Water: assumes similar cost per benefit value as electricity
Forecasted Participation	Rogers' Diffusion of Innovation	Uses the same adoption rate as retrofit activity (see benefits).



Green Button Cost-Benefit Analysis Input Assumptions

Appendix B

Benefits:

Category and Input	Source	Notes
<b>Utility Consumption, Billing and Generation Data Process Efficiencies</b>		
<b>Customers</b>		
<b>General Notes:</b>	<b>GB Phase:</b> DMD and CMD do not bring the same value to participants	
	<b>Customer Type:</b> Residential and Small Commercial customers have less sophisticated processes to collect and analyze consumption data - GB translates into higher unit benefits	
	<b>Current Practices:</b> Customers already accessing consumption data in e-format will have lower benefits than new participants	
	<b>Utility Type:</b> The benefits are higher when more utility types are involved. Customers need to access or request data to each utility type individually.	
<b>Ownership Status:</b> C&I Building Owners and Property Managers are experiencing higher benefits: benchmarking efficiencies, more use cases for energy tracking.		
<b>Key Inputs:</b>		
Value by customer participating through a CMD solution (quantified through avoided costs)	Stakeholder consultations and interviews	
<b>Assigning benefit unit value</b>	Source Data: interviews with stakeholders	Stakeholders clearly identified electricity as the key utility consumption data that would provide the majority of benefits for a GB implementation. The distribution reflects the feedback provided by stakeholders.
Benefits for a new user of utility data through CMD, for electricity	Stakeholder consultations and interviews	Distribution by utility type based on the value of each utility type's data to customers (+/-64% of total benefits attributed to electricity)
Benefits for a new user of utility data through CMD, for natural gas	Stakeholder consultations and interviews	Distribution by utility type based on value of each utility type's data to customers (+/-22% of total benefits attributed to natural gas)
Benefits for a new user of utility data, through CMD, for water	Stakeholder consultations and interviews	Distribution by utility type based on value of each utility type's data to customers (+/-14% of total benefits attributed to water)
Benefits for existing users of utility data in e-format	Interviews with Stakeholders & Professional Judgement	Incremental benefits to current process. Benefits stem from simplified process and standardized format. A minimal dollar value was assigned because several of the key benefits were already being experienced by those customers.
Benefits for tenants	Professional judgement used to link to study addressing behavioural spillover effects	
<b>Assigning customers to appropriate category</b>		
Existing users of utility data in e-format	Utility IT surveys	
O.Reg. 20/17	Communication with the Ministry of Energy; Ministry of Energy "Energy use and greenhouse gas emissions from the Broader Public Sector: 2014" (reporting and non-reporting organizations).	Institutional buildings accessing data through the EBT Hub are excluded from this class. Includes the 10% of federal and provincial institutional buildings not included in O.Reg. 397/11
New C&I users of utility data	Communication with the Ministry of Energy; Ministry of Energy "Energy use and greenhouse gas emissions from the Broader Public Sector: 2014" (reporting and non-reporting organizations).	Remaining proportion of population of C&I buildings not currently accessing consumption data or subject to O.Reg. 20/17
New residential users of utility data	See number of customer accounts and number of buildings in General Inputs	
<b>Forecasting Penetration</b>		
Based on diffusion of innovation algorithm	Rogers' Diffusion of Innovation	This theory has been applied successfully to DSM/CDM programs to forecast participation.
Parameters of Algorithm	Professional judgement based on barriers for each customer type, considering sophistication in consumption data management, resource availabilities (lower penetration for small commercial and residential)	
	Other requirements (compliance to O.Reg. 20/17)	

**Green Button Cost-Benefit Analysis Input Assumptions**

**Appendix B**

**Benefits (continued):**

Category and Input	Source	Notes
<b>Utility Consumption, Billing and Generation Data Process Efficiencies</b>		
<b>Customers</b>		
<b>Use Case: Increased Conservation: Behavioural &amp; Operational</b>		
<b>General Sources:</b>	Literature review including: - Murray, M. and J. Hawley. 2016. Got Data? The Value of Energy Data Access to Consumers. Mission:Data. - Navigant Consulting Inc., 2016. Home Energy Report Opwer Program PY7 Evaluation Report: Commonwealth Edison. - Opinion Dynamics. 2013. Massachusetts Cross-Cutting Behavioral Program Evaluation Integrated Report: Massachusetts Energy Efficiency Advisory Council and Behavioral Research Team.	
<b>General Notes:</b>	Conservation savings achieved as a result of increased access to data. Does not differentiate between savings within and outside of CDM/DSM programs. Does not include potential savings resulting from new programs developed as a result of Green Button. Behavioural savings from access to consumption data have been evaluated to vary between 4 and 12%, depending on the technology involved and engagement methodologies. The model assumes a conservative 1% for behavioural savings to recognize that the utilities do not have control over the engagement. The penetration curve selected were modest, and reflects early evidence of use of GB-enabled apps in other jurisdictions. A DSM-driven GB-related program would elicit a much higher level of participation than what is included in the model. Current behavioural programs available (Home Energy Report) claim 1 to 2% savings across the entire population receiving the reports. Savings by individual customers attributable to reports can be much higher than this.	
<b>Key Inputs:</b>		
Average Building Electricity Consumption	Average Electricity Intensity in Ontario, based on NRCAN's Comprehensive Energy Use Database	Conservative estimates were used due to unknowns regarding actual impacts
Average Building Natural Gas Consumption	Average Electricity Intensity in Ontario, based on NRCAN's Comprehensive Energy Use Database	Conservative estimates were used due to unknowns regarding actual impacts
Average Building Water Consumption	Calculated from Total Water Consumption per Capita (Sustainable Water Management Division, Environment Canada. 2011 Municipal Water Use Report – Municipal Water Use 2009 Statistics), Residential Water Consumption per Capita, number of accounts.	Assuming water consumption across customer class is proportional to electricity consumption. Conservative estimates were used due to unknowns regarding actual impacts
Value of Conservation	Avoided Costs - based on Union Gas DSM Plan 2015-2018 , app. B (the Plan includes avoided costs for natural gas, electricity, and water	Conservative estimates were used due to unknowns regarding actual impacts
Conservation Level	Literature Review of conservation programs based on access to utility consumption data (Murray, M. and J. Hawley. 2016. Got Data? The Value of Energy Data Access to Consumers. Mission:Data)	Conservative estimates were used due to unknowns regarding actual impacts
<b>Calculation:</b>		
Behavioural & Operational Savings Unit Value per building type	Average Building Utility Consumption by building type * Avoided Costs * Conservation Level	
Electricity Retrofit Savings	Ontario utility and other Canadian CDM/DSM Plans and average energy rates	
Natural Gas Retrofit Savings	Ontario utility and other Canadian CDM/DSM Plans and average energy rates	
Water Retrofit Savings	Conservatively estimated based on electricity/natural gas potential savings (Ontario utility and other Canadian CDM/DSM Plans and average energy rates)	Conservatively estimated based on electricity/natural gas potential savings
<b>Forecasting Penetration</b>		
Based on diffusion of innovation algorithm	Rogers' Diffusion of Innovation	
Parameters of Algorithm	Professional judgement based on barriers for each customer type, considering sophistication in consumption data management, resource availabilities (lower penetration for small commercial and residential)	
<b>Results:</b>	Residential: Participation after 5 yrs is 1% of total customers Commercial participation after 5 yrs: large: 6%, small: 2%, institutional: 6%	

Green Button Cost-Benefit Analysis Input Assumptions

Appendix B

Benefits (continued):

Category and Input	Source	Notes
<b>Utility Consumption, Billing and Generation Data Process Efficiencies</b>		
<b>Customers (continued)</b>		
<b>Use Case: Increased Conservation: Retrofit</b>		
<b>Key Inputs:</b>		
Average Building Electricity Consumption	Average Electricity Intensity in Ontario, based on NRCAN's Comprehensive Energy Use Database	
Average Building Natural Gas Consumption	Average Electricity Intensity in Ontario, based on NRCAN's Comprehensive Energy Use Database	
Average Building Water Consumption	Calculated from Total Water Consumption per Capita, Residential Water Consumption per Capita, number of accounts per capita	Assuming water consumption across customer class is proportional to electricity consumption
Value of Conservation	Avoided Costs - based on Union Gas DSM Plan 2015-2018, app. B (the Plan includes avoided costs for natural gas, electricity, and water)	
Conservation Level	Savings estimation based on evaluation experience and Ontario utility and other Canadian CDM/DSM Plans.	Conservative Estimate - 10% savings - average of retrofit activities considering several achieve 20% more savings with utility conservation programs.
<b>Calculation:</b>		
Behavioural & Operational Savings Unit Value per building type	Average Building Utility Consumption by building type* Avoided Costs * Conservation Level	
<b>Forecasting Penetration:</b>		
Based on diffusion of innovation algorithm	Rogers' Diffusion of Innovation	This theory has been applied successfully to DSM/CDM programs to forecast participation.
Parameters of Algorithm	Professional judgement based on barriers for each customer type, considering sophistication in consumption data management, resource availabilities (lower penetration for small commercial and residential)	
<b>Results:</b>		Residential: Participation after 5 yrs is 0.4% of total customers - this captures conservation activities requiring expenditure
		Commercial participation after 5 yrs: large: 0.7%, small: 0.12%, institutional:0.7%

<b>Solution Providers</b>		
<b>Use Case: Ongoing Utility Consumption Monitoring and Benchmarking</b>		
<b>Key Inputs:</b>		
Average benefit per building, per building type, utility type	Interviews with Stakeholders	This benefit is included as a dollar value reflecting reduced effort to access utility consumption data for monitoring and benchmarking activities
<b>Forecasting Penetration</b>		
Based on diffusion of innovation algorithm	Rogers' Diffusion of Innovation	This theory has been applied successfully to DSM/CDM programs to forecast participation
Parameters of Algorithm	Professional judgement based on barriers, interviews with stakeholders	
<b>Use Case: Engineering Services - One-Time Services Requiring Utility Consumption Data</b>		
<b>Key Inputs:</b>		
Average benefit per building, per building type, utility type	Interviews with Stakeholders	This benefit stems from reduced effort to access utility consumption data to conduct engineering analysis
<b>Forecasting Penetration</b>		
Based on diffusion of innovation algorithm	Rogers' Diffusion of Innovation	This theory has been applied successfully to DSM/CDM programs to forecast participation
Parameters of Algorithm	Professional judgement based on barriers, interviews with stakeholders	

<b>Utility Reduced Customer Care Effort</b>		
<b>Key Inputs:</b>		
Annual Cost Reduction- reduced customer care efforts - by utility type and size	Stakeholder Interviews, Utility IT Surveys	
<b>Forecasting Penetration</b>		100% implementation within 4 years: 35%, 70%, 92%, 100%

<b>Utility CDM/DSM Program Efficiencies and Innovations</b>		
<b>Key Inputs:</b>		
Annual Cost Reduction- CDM/DSM Program Efficiencies and Innovations - by utility type and size	Values estimated based on Stakeholder Interviews	This is a token benefit expressed in \$ per utility

## APPENDIX C: COSTS AND BENEFITS OVERVIEW TABLE

Proposed Use Cases: Costs and Benefits Overview Table

Benefits	Customer Groups																												
	Property Owners/Managers															Tenants/Residents													
	Large Commercial			Small Commercial			Large Industrial			Institutional			Residential			Large Commercial			Small Commercial			Large Industrial			Institutional			Residential	
	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual		
<b>Utility Consumption, Billing and Generation Data Process Efficiencies</b>																													
<b>Energy tracking (voluntary and internal) - customers who currently gather and track data</b>	Y			Y			Y			Y			Y			Y			Y			Y			Y				
Energy audit efficiencies																													
Energy tracking																													
Energy and water reporting and benchmarking																													
Consistent machine readable data among multiple utilities																													
Increased data (consumption, billing and generation) accuracy/quality																													
Simplified data sharing authorization process																													
Increased frequency and granularity of utility data																													
<b>Energy and water reporting and benchmarking - customers' future data collection related to Bill 135</b>	Y			Y			Y			Y			Y			Y			Y			Y			Y				
Energy audit efficiencies (new customer requirements)																													
Energy tracking (new customer requirements)																													
Energy and water reporting and benchmarking																													
Consistent machine readable data among multiple utilities																													
Increased data (consumption, billing and generation) accuracy/quality																													
Simplified data sharing authorization process																													
Increased frequency and granularity of utility data																													
Increased operational efficiencies within utilities from improvements to IT systems																													
<b>Increased Conservation</b>																													
<b>Non-retrofit savings</b>		Y			Y			Y			Y			Y			Y			Y			Y			Y			
Greater behavioural-based conservation																													
Greater operational savings in buildings																													
Increased CDM/DSM program participation																													
<b>Increased energy efficiency retrofit savings</b>		Y			Y			Y			Y			Y															
Increased energy efficiency / conservation education																													
Increased CDM/DSM program participation																													
<b>Other Conservation</b>																													
CMD/DSM program efficiencies and innovations																													
New CDM/DSM program design based on Green Button																													
CDM/DSM program implementation efficiencies																													
CDM/DSM program evaluation efficiencies																													

Quantitative input into model	Benefit that is not broken out quantitatively in the model	Category Heading
-------------------------------	--	------------------

Proposed Use Cases: Costs and Benefits Overview Table

	Customer Groups																												
	Property Owners/Managers															Tenants/Residents													
	Large Commercial			Small Commercial			Large Industrial			Institutional			Residential			Large Commercial			Small Commercial			Large Industrial			Institutional			Residential	
Benefits	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual		
Increased Real Estate Value			Y			Y			Y			Y			Y														
<b>Customer Service Benefits</b>																													
Reduced customer care effort																													
Increased customer satisfaction / engagement																													
Improved customer access to data																													
<b>Support government policy objectives</b>																													
Reduce/remove barriers to reporting & benchmarking requirements																													
Support OEB's customer education/customer control goals																													
Support Ontario's Conservation objectives and Climate Change Action Plan																													
<b>Economic Development and Innovation</b>																													
Job Creation																													
Improved Access to North American Market																													
Support new use cases and development of innovative services																													
<b>Costs</b>																													
<b>GB Implementation Costs</b>																													
GB infrastructure - cloud services, platform																													
GB infrastructure - front end																													
Security and privacy																													
Third-party applications - registration and testing																													
<b>GB Utility Integration</b>																													
Integration with customer portal																													
Computer information systems Extract, Transform, and Load (ETL) protocols																													
Meter Data																													
Integration with third-party meter data management																													
Testing																													
Marketing																													
Security and privacy																													
Increased energy efficiency retrofit costs		Y			Y			Y			Y			Y															

Quantitative input into model	Benefit that is not broken out quantitatively in the model	Category Heading
-------------------------------	--	------------------

Proposed Use Cases: Costs and Benefits Overview Table

Benefits	Utilities																										
	Electric Utilities									Natural Gas Utilities						Water Utilities											
	Electricity (Large)			Electricity (Medium)			Electricity (Small)			Natural Gas Utilities (Large)			Natural Gas Utilities (Small)			Water Utilities (Large)			Water Utilities (Medium)			Water Utilities (Small)			Water Utilities (linked to LDC)		
	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual
<b>Utility Consumption, Billing and Generation Data Process Efficiencies</b>																											
<b>Energy tracking (voluntary and internal) - customers who currently gather and track data</b>	Y			Y			Y			Y			Y			Y			Y			Y			Y		
Energy audit efficiencies																											
Energy tracking																											
Energy and water reporting and benchmarking																											
Consistent machine readable data among multiple utilities																											
Increased data (consumption, billing and generation) accuracy/ quality																											
Simplified data sharing authorization process																											
Increased frequency and granularity of utility data																											
<b>Energy and water reporting and benchmarking - customers' future data collection related to Bill 135</b>	Y			Y			Y			Y			Y			Y			Y			Y			Y		
Energy audit efficiencies (new customer requirements)																											
Energy tracking (new customer requirements)																											
Energy and water reporting and benchmarking																											
Consistent machine readable data among multiple utilities																											
Increased data (consumption, billing and generation) accuracy/quality																											
Simplified data sharing authorization process																											
Increased frequency and granularity of utility data																											
Increased operational efficiencies within utilities from improvements to IT systems																											
<b>Increased Conservation</b>																											
<b>Non-retrofit savings</b>																											
Greater behavioural-based conservation*																											
Greater operational savings in buildings*																											
Increased CDM/DSM program participation*																											
<b>Increased energy efficiency retrofit savings</b>																											
Increased energy efficiency / conservation education			Y			Y			Y			Y			Y			Y			Y			Y			Y
Increased CDM/DSM program participation*																											
<b>Other Conservation</b>																											
CMD/DSM program efficiencies and innovations		Y	Y		Y	Y		Y	Y		Y	Y		Y	Y		Y		Y		Y		Y		Y	Y	
New CDM/DSM program design based on Green Button			Y			Y			Y			Y			Y			Y			Y			Y			Y
CDM/DSM program implementation efficiencies			Y			Y			Y			Y			Y			Y			Y			Y			Y
CDM/DSM program evaluation efficiencies			Y			Y			Y			Y			Y			Y			Y			Y			Y

Quantitative input into model	Benefit that is not broken out quantitatively in the model	Category Heading
-------------------------------	--	------------------

Proposed Use Cases: Costs and Benefits Overview Table

Benefits	Utilities																										
	Electric Utilities									Natural Gas Utilities						Water Utilities											
	Electricity (Large)			Electricity (Medium)			Electricity (Small)			Natural Gas Utilities (Large)			Natural Gas Utilities (Small)			Water Utilities (Large)			Water Utilities (Medium)			Water Utilities (Small)			Water Utilities (linked to LDC)		
	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual
<b>Increased Real Estate Value</b>																											
<b>Customer Service Benefits</b>																											
Reduced customer care effort	Y			Y			Y			Y			Y			Y			Y			Y			Y		
Increased customer satisfaction / engagement			Y			Y			Y			Y			Y			Y			Y			Y			Y
Improved customer access to data			Y			Y			Y			Y			Y			Y			Y			Y			Y
<b>Support government policy objectives</b>																											
Reduce/remove barriers to reporting & benchmarking requirements																											
Support OEB's customer education/customer control goals																											
Support Ontario's Conservation objectives and Climate Change Action Plan																											
<b>Economic Development and Innovation</b>																											
Job Creation																											
Improved Access to North American Market																											
Support new use cases and development of innovative services			Y			Y			Y			Y			Y			Y			Y			Y			Y
<b>Costs</b>																											
<b>GB Implementation Costs</b>	Y			Y			Y			Y			Y			Y			Y			Y			Y		
GB infrastructure - cloud services, platform																											
GB infrastructure - front end																											
Security and privacy																											
Third-party applications - registration and testing																											
<b>GB Utility Integration</b>	Y			Y			Y			Y			Y			Y			Y			Y			Y		
Integration with customer portal																											
Computer information systems Extract, Transform, and Load (ETL) protocols																											
Meter Data																											
Integration with third-party meter data management																											
Testing																											
Marketing																											
Security and privacy																											
<b>Increased energy efficiency retrofit costs*</b>																											

\*Included as a cost/benefit to end users (customers) rather than utilities



Proposed Use Cases: Costs and Benefits Overview Table

	Additional Stakeholders														
	Government									Third Parties					
	Gov Depts			IESO			OEB			SaaS GB Implementation Providers			EE/Technical Service Solution Providers		
	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual
<b>Utility Consumption, Billing and Generation Data Process Efficiencies</b>															
<b>Energy tracking (voluntary and internal) - customers who currently gather and track data</b>										Y			Y		
Energy audit efficiencies															
Energy tracking															
Energy and water reporting and benchmarking															
Consistent machine readable data among multiple utilities															
Increased data (consumption, billing and generation) accuracy/ quality															
Simplified data sharing authorization process															
Increased frequency and granularity of utility data															
<b>Energy and water reporting and benchmarking - customers' future data collection related to Bill 135</b>										Y			Y		
Energy audit efficiencies (new customer requirements)															
Energy tracking (new customer requirements)															
Energy and water reporting and benchmarking															
Consistent machine readable data among multiple utilities															
Increased data (consumption, billing and generation) accuracy/quality															
Simplified data sharing authorization process															
Increased frequency and granularity of utility data															
Increased operational efficiencies within utilities from improvements to IT systems															
<b>Increased Conservation</b>															
<b>Non-retrofit savings</b>															
Greater behavioural-based conservation															
Greater operational savings in buildings															
Increased CDM/DSM program participation															
<b>Increased energy efficiency retrofit savings</b>															
Increased energy efficiency / conservation education						Y									
Increased CDM/DSM program participation															
<b>Other Conservation</b>															
CDM/DSM program efficiencies and innovations												Y			
New CDM/DSM program design based on Green Button															Y
CDM/DSM program implementation efficiencies															Y
CDM/DSM program evaluation efficiencies						Y									

Quantitative input into model	Benefit that is not broken out quantitatively in the model	Category Heading
-------------------------------	--	------------------

Proposed Use Cases: Costs and Benefits Overview Table

	Additional Stakeholders														
	Government									Third Parties					
	Gov Depts			IESO			OEB			SaaS GB Implementation Providers			EE/Technical Service Solution Providers		
	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual	Direct Quant	Indir. Quant	Qual
<b>Increased Real Estate Value</b>															
<b>Customer Service Benefits</b>															
Reduced customer care effort															
Increased customer satisfaction / engagement															
Improved customer access to data															
<b>Support government policy objectives</b>															
Reduce/remove barriers to reporting & benchmarking requirements			Y												
Support OEB's customer education/customer control goals								Y							
Support Ontario's Conservation objectives and Climate Change Action Plan			Y			Y		Y							
<b>Economic Development and Innovation</b>															
Job Creation			Y							Y			Y		
Improved Access to North American Market			Y									Y			Y
Support new use cases and development of innovative services												Y			Y
<b>Costs</b>															
<b>GB Implementation Costs</b>															
GB infrastructure - cloud services, platform															
GB infrastructure - front end															
Security and privacy															
Third-party applications - registration and testing**															
<b>GB Utility Integration</b>															
Integration with customer portal															
Computer information systems Extract, Transform, and Load (ETL) protocols															
Meter Data															
Integration with third-party meter data management															
Testing															
Marketing															
Security and privacy															
<b>Increased energy efficiency retrofit costs</b>															

\*\*Included within costs to utilities but not for SaaS implementation providers as it is a business-related cost built into existing costs

## APPENDIX D: CONSERVATION METHODOLOGY

The following section walks through the methodology, assumptions and inputs used to estimate impacts from increased conservation activity resulting from improved access to utility consumption and billing data. We use building retrofits as the basis of the example, and **the same methodology is used for behaviour-based conservation.**

### INCREASED CONSERVATION

#### ALGORITHM

Our general methodology links estimated energy and water savings to avoided costs to derive an annualized benefit from energy conservation. The general algorithm used is:

$$\text{Conservation Benefit} = \text{Unitary Benefit} * \text{Participation}$$

$$\text{Unitary Benefit} = \% \text{ Savings} * \text{Annual Consumption} * \text{AC}$$

Where:

- **Conservation Benefit:** Total annual conservation benefits from increased retrofit activity
- **Unitary Benefit:** Average annual benefit value per participant
- **% Savings:** Percentage of total building or house consumption saved through retrofit
- **Annual Consumption:** Total yearly building or house consumption (electricity, natural gas or water)
- **AC:** Utility avoided costs
- **Participation:** Annual number of participants

Where additional information was available to assess the unitary benefit value, an alternative approach based on the available information was used. This is notably the case for natural gas benefits in the residential sector. For natural gas savings, Union Gas presents unitary savings for its Home Renovation program. Considering that in the residential sector, the vast majority of benefits would be derived from measures and technologies covered under the Union Gas program, it was deemed a good representation of energy efficiency improvements.

The annual benefit value per participant is a model input, and the participation level is calculated through application of penetration curves. Inputs and assumptions used for each of these variables are presented below.

UTILITY SAVINGS

The impacts of increasing access to utility consumption and billing data has the potential to induce increased conservation activities, both through increased home and building retrofit activities (envelope improvements, high-efficiency HVAC equipment, etc.) and other actions requiring investments from the participants.

*Residential Sector*

For the residential sector, annual incremental savings are presented in the following table:

Utility Type	Annual Savings: Retrofit-Based Efficiency and Conservation	Annual Savings: Behaviour-Based Efficiency and Conservation
Electricity	10%	1%
Natural Gas	12%	1%
Water	3%	1%

**Electricity Savings:** Participants in Ontario’s ecoENERGY retrofit program have realised a 20% reduction in their annual energy consumption.<sup>1</sup> More specifically for electricity, a Canmet Energy Study<sup>2</sup> has identified average potential savings representing 11% of individual home baseload electricity consumption (defined as lighting, major appliances, common plug-load and other atypical loads). We used 10%, which is lower than both these values, to ensure our analysis was conservative.

**Natural Gas Savings:** The potential measures to reduce consumption are essentially covered by Union Gas Home Renovation programs. Union Gas 2015-2020 DSM Plan provides information that allows us to calculate the average natural gas savings of 1,039 m<sup>3</sup>/year for participants in the program. Considering that those natural gas savings were derived from utility programs, and that envelope improvements have higher barriers to participation (access to capital, discretionary measures, etc.) only 30% of those savings have been retained for the cost-benefit analysis.

**Water Savings:** In the absence of robust data on potential water savings improvements, a conservative 3% of annual load savings was used to estimate impacts.

<sup>1</sup> Natural Resources Canada, ecoENERGY Retrofit Statistics, August 1<sup>st</sup>, 2012.

<sup>2</sup> Canmet ENERGY: Base-Load Electricity Usage – Results from In-home Evaluations, 2012.

**Commercial Sector**

For the commercial sector, annual incremental savings are presented in the following table:

Utility Type	Annual Savings: Retrofit-Based Efficiency and Conservation	Annual Savings: Behaviour-Based Efficiency and Conservation
Electricity	10%	2%
Natural Gas	4%	2%
Water	3%	1%

**Electricity and Natural Gas Savings:** Annual savings factors were derived from Ontario’s potential studies<sup>3</sup>. The economic potential was used as a representation of potential energy savings for the average C&I building in Ontario. Recognising that the economic potential (24% of commercial sector consumption for electricity and 23% for natural gas) represents all the savings economically feasible in buildings, the results from the potential studies were reduced to account for several barriers not addressed by increased access to energy consumption and billing information. The conservative estimates used for the analysis are also meant to reflect *incremental* savings specifically due to increased access to information. Specifically, for natural gas savings, we took into consideration the magnitude of required investments to achieve savings (i.e., most measures will require significant upfront capital investments to be realized). This is less of an issue for electricity measures, since lighting and plug load improvements can be individually procured for a reasonable cost.

For water savings, in the absence of robust information assessing the economic potential, we have used a conservative estimate of 3% annual savings.

---

<sup>3</sup> (ICF International, Natural Gas Potential Study, June 2016. [http://www.ontarioenergyboard.ca/oeb/ Documents/EB-2015-0117/ICF\\_Report\\_Gas\\_Conservation\\_Potential\\_Study.pdf](http://www.ontarioenergyboard.ca/oeb/ Documents/EB-2015-0117/ICF_Report_Gas_Conservation_Potential_Study.pdf); Nexant Achievable Potential Study: Short Term Analysis, June 2016. <http://www.ieso.ca/-/media/files/ieso/document-library/working-group/aps/aps-short-term-analysis-2016.pdf>)

COST-BENEFIT ANALYSIS REPORT

APPENDIX D

BASELINE ANNUAL CONSUMPTION

Baseline average consumption was used to calculate unit annual savings per home or per building.

*Residential Sector*

Annual Utility Consumption – Residential Sector		
Utility Type	Annual Consumption	Source
Electricity	5,454 kWh	<ul style="list-style-type: none"> <li>Natural Resources Canada <i>Comprehensive Energy Use Database</i>, Residential Sector, Ontario, table 1 for 2014.                             <ul style="list-style-type: none"> <li>Total residential electricity consumption is reported as 118.7 PJ for 5,196,000 households.</li> <li>For the purpose of the analysis, we used 85% of the calculated average consumption, considering notably the evolution of codes and standards and their potential impacts on electrical savings.</li> </ul> </li> </ul>
Natural Gas	2,600 m <sup>3</sup>	<ul style="list-style-type: none"> <li>Navigant. <i>Analysis Investigating Revenue Decoupling for Electricity and Natural Gas Distributors in Ontario</i>, March 2014.</li> </ul>
Water	213.5 m <sup>3</sup>	<ul style="list-style-type: none"> <li>Environment Canada, <i>2011 Municipal Water Use Report</i>:                             <ul style="list-style-type: none"> <li>Assumes 225 liters per capita per day</li> </ul> </li> <li>Statistics Canada, <i>2011 Census</i>:                             <ul style="list-style-type: none"> <li>2.6 persons per household</li> </ul> </li> </ul>

*C&I Sector*

The following values were used for the annual utility consumption for non-residential buildings in Ontario.

Annual Utility Consumption – Commercial and Institutional Sector				
Utility Type	Small Buildings (less than 10,000 ft <sup>2</sup> )	Large Buildings (more than 10,000 ft <sup>2</sup> )	Institutional	Source
Electricity (kWh)	42,464	508,905	344,105	Natural Resources Canada's Comprehensive Energy Use Database for the Commercial and Institutional Sector
Natural Gas (m <sup>3</sup> )	7,442	89,912	60,309	
Water (m <sup>3</sup> )	3,441	41,240	27,885	

COST-BENEFIT ANALYSIS REPORT

APPENDIX D

The energy consumption values for non-residential buildings were derived from Natural Resources Canada’s Comprehensive Energy Use Database for the Commercial and Institutional Sector. The total energy consumption by energy source for and total Floor Space was used to estimate an average energy intensity (GJ/m<sup>2</sup>) for the C&I sector. This resulted in an average energy intensity of 116,25 kWh/m<sup>2</sup> for electricity and 20.374 m<sup>3</sup>/m<sup>2</sup> for natural gas. The energy intensity factor was then applied to average building size for small, large and institutional buildings based on information from the Survey of Commercial and Institutional Energy use – Buildings 2009 (Detailed Statistical Report December 2012).

Building Size (ft <sup>2</sup> )	Average Size	Count	Distribution	Estimated Electricity Consumption (kWh/yr)	Natural Gas Consumption (m <sup>3</sup> /yr)
Less than 5,000	2,500	80082	49%	26,999	4,732
5,000-10,000	7,500	32141	20%	80,997	14,196
10,000 to 50,000	30,000	39054	24%	323,988	47,319
50,000 to 200,000	125,000	10103	6%	1,349,950	189,277
Greater than 200,000	200,000	2157	1%	2,159,920	378,554

The average energy consumption for small, large and institutional buildings were estimated through a weighted average of buildings for small (less than 10,000 ft<sup>2</sup>), large (more than 10,000 ft<sup>2</sup>) and institutional (more than 5,000 ft<sup>2</sup>).

Information for water consumption for non-residential accounts is not readily available. Our analysis used a water use intensity of 380 L/ft<sup>24</sup> applied to the average size to estimate annual water consumption per building size.

---

**AVOIDED COSTS**

Annual resource benefits for all utility types were calculated using a fixed discount rate based on information provided in the Union Gas 2015-2020 DSM Plan, Appendix B. Electricity and water avoided costs remain constant in real value, whereas natural gas avoided costs vary annually. To simplify analysis, the cost-benefit models has assumed constant real avoided costs for each utility

---

<sup>4</sup> This water use intensity was derived from the City of Orillia Water Conservation and Efficiency Plan – 2014. The Plan indicates a 1,476 m<sup>3</sup> per non-residential connection. Considering Orillia is a small city, we have assumed that most of those connections would be in the small building category.

COST-BENEFIT ANALYSIS REPORT

APPENDIX D

type. For natural gas, baseload avoided costs have been selected to remain conservative. The following table presents the avoided costs used in the analysis.

Utility Type	Avoided Costs
Electricity	0.1128 \$/kWh
Natural Gas	0.21378 \$/m <sup>3</sup>
Water	2.2729 \$/m <sup>3</sup>

PARTICIPATION RATE

Participation rates for increased retrofit activities were based on the adoption curves developed for the cost-benefit model (see Penetration Level on page 26 of the report).

The table below presents the annual participation as a % of eligible population.

	Year									
	1	2	3	4	5	6	7	8	9	10
Small Commercial & Residential	0.66%	0.87%	1.13%	1.48%	1.93%	2.50%	3.24%	4.20%	5.41%	6.96%
Large Commercial, Industrial & Institutional	1.66%	3.20%	5.23%	7.86%	11.24%	15.52%	20.82%	27.22%	34.69%	43.04%

*Eligible Population*

The following table presents the eligible population for each customer class included in the analysis. We further include an applicability factor to further reduce the proportion of GB participants estimated to conduct retrofit activity due to increased accessibility to consumption and billing data. This was done to ensure our analysis was conservative and is highlighted as the Eligible Population in the table below.

SubGroup	Population (Number of Buildings)	Applicability Factor	Eligible Population	Source
Large Commercial	32,011	25%	8,003	Calculated from Survey of Commercial and Institutional Energy use – Buildings 2009 and Submeter Penetration Estimates developed from IT survey
Small Commercial	112,672	25%	28,168	
Large Industrial	120	25%	30	
Institutional	19,630	25%	4,908	
Residential	3,342,822	25%	835,706	



COST-BENEFIT ANALYSIS REPORT

APPENDIX D

CALCULATION EXAMPLE

Below, we present the calculations conducted to evaluate the benefits for the DMD/CMD Electric Utility Only Scenario.

$$\text{Unitary Benefit} = \% \text{ Savings} * \text{Annual Consumption} * \text{AC}$$

*Unit Benefit*

Customer Class	% Savings (1)	Annual Consumption (kWh) (2)	Avoided Costs (\$/kWh) (3)	Unit Benefits (\$) (1)*(2)*(3)
Residential	10%	5454	0.11	60
Small Commercial	10%	42,464	0.11	467
Large Commercial	10%	508,906	0.11	5,598
Institutional	10%	344,105	0.11	3,785
Large Industrial	10%	763,359	0.11	8,397

*Eligible Population*

Customer Class	Population (1)	Applicability (2)	Eligible Population (1) * (2)
Residential	3,342,822	25%	835705
Small Commercial	112,672	25%	28168
Large Commercial	32,011	25%	8003
Institutional	19,630	25%	4908
Large Industrial	120	25%	30

ESTIMATION OF COSTS

The calculation of costs was conducted at a high level, as the cost-benefit analysis was focused on the overall impacts of a Green Button implementation rather than a measure-level analysis.

CALCULATION OF COST ESTIMATES

COST-BENEFIT ANALYSIS REPORT

APPENDIX D

Because the benefits of increased conservation (energy savings) are calculated on an annualized basis, the costs are as well in order to ensure alignment. Our methodology for estimating costs is as follows:

- The energy savings as calculated in earlier sections of this appendix were used as a starting point.
- As a starting point, we used cost-benefit results from the Union Gas 2015-2020 DSM Plan to estimate the costs of the energy savings that were calculated. The Union Gas Plan was used as it provided the most detail for an entire portfolio.
- We made adjustments for applicable factors:
  - For the Residential Sector, because Total Resource Cost (TRC)-Plus values are available for the home renovation rebate, we incorporated those values and removed the generic 15% non-energy benefits adder from the DSM Plan.
    - We removed costs unrelated to energy retrofits (for example, audit costs), which resulted in costs being calculated as 89 percent of the TRC-plus costs.
    - This provided a cost-to-benefit ratio of 0.69 for natural gas.
    - For electricity and water, we applied a slightly lower ratio of 0.65. This decision was based on professional experience and a comparison of the results with measure-level annualized cost-to-benefit values from the IESO's Technical Reference Manual as well as internal sources from prior work.
  - For the Commercial, Industrial and Institutional Sector we followed the same methodology without the home renovation input adjustment. This resulted in 0.494 for natural gas and a 0.5 ratio for electricity and water.
- We applied these cost ratios to the annual benefit value to estimate the annualized costs.

COST-BENEFIT ANALYSIS REPORT

APPENDIX D

*Annual Benefits*

Conservation Benefit = Unitary Benefit \* Participation

Customer Class	Unit Ben (\$) (1)	Eligible Pop. (2)	Annual Benefits (\$)										
			(1) * (2) * Adoption Curve for each year; Net Present Values use a 2% discount rate										
			Yr1	Yr2	Yr3	Yr4	Yr5	Yr6	Yr7	Yr8	Yr9	YR10	NPV (10yr)
<b>Adoption Curve Res &amp; Small Commercial</b>			0.66%	0.87%	1.13%	1.48%	1.93%	2.50%	3.24%	4.20%	5.41%	6.96%	
<b>Adoption Curve Large Commercial, Institutional, Large Industrial</b>			1.66%	3.20%	5.23%	7.86%	11.24%	15.52%	20.82%	27.22%	34.69%	43.04%	
<b>Residential</b>	60	835,705	330,505	433,984	568,022	741,455	965,542	1,254,543	1,626,377	2,103,314	2,712,641	3,487,147	12,291,436
<b>Small Commercial</b>	467	28,168	86,733	113,889	149,064	194,578	253,384	329,226	426,805	551,967	711,870	915,122	3,225,605
<b>Large Commercial</b>	5,598	8,003	743,665	1,433,572	2,342,994	3,521,211	5,035,421	6,952,824	9,327,177	12,194,321	15,540,816	19,281,542	65,651,588
<b>Institutional</b>	3,785	4,908	308,356	594,421	971,506	1,460,046	2,087,903	2,882,941	3,867,450	5,056,291	6,443,892	7,994,959	27,221,980
<b>Large Industrial</b>	8,397	30	4,182	8,061	13,175	19,800	28,315	39,096	52,447	68,569	87,387	108,421	369,163

COST-BENEFIT ANALYSIS REPORT

APPENDIX D

#### CALCULATION OF GREENHOUSE GAS REDUCTIONS

Greenhouse gas (GHG) reductions are calculated by multiplying the energy impacts as described above by the emissions factors provided by the Ministry of Energy:

$$\text{GHG Reduction} = \text{Energy Savings} * \text{Emission Factor}$$

As with other inputs, GHG emissions factors may not be up to date with current Ontario government GHG calculation assumptions because of the timeframe in which the analysis was conducted.

## APPENDIX E: ADDITIONAL SCENARIO ANALYSIS

This appendix, developed in 2017 after the initial cost-benefit analysis was completed, provides additional results for Scenarios 1B (Multi-Integrated Hosted DMD/CMD for Electricity and Natural Gas utilities) and 2B (Multi-Integrated Hosted for All Utility Types), using a real discount rate of 3.5%, which has been used by the Ministry of Energy in other recent analyses.

### SCENARIO 1B: MULTI-INTEGRATED HOSTED DMD/CMD (ELECTRICITY AND NATURAL GAS UTILITIES ONLY)

**Table 1. Scenario 1B Cost Details**

Cost Category	Cost Type	5-Year Analysis (\$)	10-Year Analysis (\$)	Scenario-Specific Assumptions
Implementation (One-time setup and integration costs)	Direct	3,982,723	3,986,847 <sup>1</sup>	The setup cost for the Multi-Integrated scenario assumes: <ul style="list-style-type: none"> <li>• 5 independent platforms for the electricity sector</li> <li>• 1 platform for the natural gas sector (because there are so few utilities)</li> <li>• 5 platforms for the water utilities</li> </ul>
Operational Costs <sup>2</sup>	Direct	735,433	2,182,967	
Retrofit Costs	Indirect	10,573,953	60,072,210	
<b>Total</b>		<b>15,292,109</b>	<b>66,242,024</b>	

<sup>1</sup> Differences between the 5-year and 10-year Implementation Costs are an artefact of the mathematical function used to forecast implementation costs. The mathematical function forecasts the following rollout of Green Button through the first 5 years following enactment of the policy: 35%, 70%, 92%, 99%, 99.9%.

<sup>2</sup> Sum of net-present value of annual costs over the timeframe.

**Table 2. Scenario 1B Benefits Details<sup>3</sup>**

Benefit Category	Benefit Component	Benefit Type	5-Year Analysis (\$)	10-Year Analysis (\$)
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	17,221,476	54,410,886
	Process Efficiencies (Large Building Energy and Water Reporting and Benchmarking)	Direct	12,143,948	23,695,626
	Reduced Customer Care Efforts	Indirect	1,029,360	2,252,663
	CDM/DSM Program Efficiencies and Innovation	Indirect	849,831	1,859,779
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	10,821,748	51,787,669
	Increased Conservation - Retrofits	Indirect	24,721,779	120,255,887
	<b>Total</b>		<b>66,788,142</b>	<b>254,262,509</b>

**RESULTS**

**DETAILED RESULTS FOR THE MULTI-INTEGRATED VERSION OF THIS SCENARIO (SCENARIO 1B) ARE PRESENTED IN THE FOLLOWING TABLES.**

**BENEFIT-COST RATIOS:**

**Table 3. Scenario 1B Benefit-Cost Ratios**

Ratio Type	5-Year Analysis	10-Year Analysis
Direct and Indirect Costs and Benefits	4.4	3.8
Direct Benefits and Costs only <sup>4</sup>	6.5	13.0

To illustrate how the costs and benefits are distributed across stakeholder groups, we present the following tables.

**Table 4. Scenario 1B Costs by Stakeholder Group (5-year horizon)**

Cost Category	Stakeholder Group
---------------	-------------------

<sup>3</sup> No scenario-specific assumptions required

<sup>4</sup> Direct benefits and costs are a subset of total benefits and costs. However, the direct benefits and costs ratios are higher than the total ratios because the magnitude of benefits to costs is different for direct results than for total results.

COST-BENEFIT ANALYSIS REPORT

APPENDIX E

	Cost Type	Electricity Utility (\$)	Natural Gas Utility (\$)	Customers <sup>5</sup> (\$)	Total (\$)
Implementation (One-time setup and integration costs)	Direct	3,458,565	524,157	-	<b>3,982,723</b>
Operational Costs <sup>6</sup>	Direct	435,205	300,228	-	<b>735,433</b>
Retrofit Costs	Indirect	-	-	10,573,953	<b>10,573,953</b>
<b>Total</b>		<b>3,893,770</b>	<b>824,385</b>	<b>10,573,953</b>	<b>15,292,109</b>

<sup>5</sup> Includes all customer classes (Residential, Commercial, Industrial, and Institutional)

<sup>6</sup> Sum of net-present value of annual costs over the timeframe.

COST-BENEFIT ANALYSIS REPORT

APPENDIX E

**Table 5. Scenario 1B Benefits by Stakeholder Group (5-year horizon)**

Benefit Category	Benefit Component	Benefit Type	Stakeholder Group					Total (\$)
			C&I (\$)	Industrial (\$)	Other <sup>7</sup> (\$)	Residential (\$)	Utility (\$)	
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	9,667,413	7,554	5,056,785	2,489,724	-	<b>17,221,476</b>
	Process Efficiencies (requirements)	Direct	12,063,383	80,564	-	-	-	<b>12,143,948</b>
	Reduced Customer Care Efforts	Indirect	-	-	-	-	1,029,360	<b>1,029,360</b>
	CDM/DSM Program Efficiencies and Innovation	Indirect	-	-	-	-	849,831	<b>849,831</b>
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	9,243,371	13,761	-	1,564,616	-	<b>10,821,748</b>
	Increased Conservation - Retrofits	Indirect	19,031,618	73,190	-	5,616,971	-	<b>24,721,779</b>
	<b>Total</b>		<b>50,005,785</b>	<b>175,069</b>	<b>5,056,785</b>	<b>9,671,311</b>	<b>1,879,191</b>	<b>66,788,142</b>

<sup>7</sup> Other Stakeholders include third-party Energy Efficiency Consultants/Service Providers providing utility consumption monitoring services, energy assessments, and/or engineering services.



**SCENARIO 2B: MULTI-INTEGRATED HOSTED DMD/CMD (ALL UTILITY TYPES)**

**Table 6. Scenario 2B Cost Details**

Cost Category	Cost Type	5-Year Analysis (\$)	10-Year Analysis (\$)	Scenario-Specific Assumptions
Implementation (One-time setup and integration costs)	Direct	30,432,861	30,464,379	The setup cost for the Multi-Integrated scenario assumes: <ul style="list-style-type: none"> <li>• 5 independent platforms for the electricity sector</li> <li>• 1 platform for the natural gas sector (because there are so few utilities)</li> <li>• 5 platforms for the water utilities</li> </ul>
Operational Costs <sup>8</sup>	Direct	1,168,226	3,467,786	
Retrofit Costs	Indirect	12,578,686	71,377,618	
<b>Total</b>		<b>44,179,773</b>	<b>105,309,783</b>	

**Table 7. Scenario 2B Benefits Details<sup>9</sup>**

Benefit Category	Benefit Component	Benefit Type	5-Year Analysis (\$)	10-Year Analysis (\$)
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	24,054,230	71,046,545
	Process Efficiencies	Direct	14,167,939	27,644,897
	Reduced Customer Care Efforts	Indirect	1,559,328	3,412,449
	CDM/DSM Program Efficiencies and Innovation	Indirect	1,627,629	4,201,293
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	13,340,724	64,123,022
	Increased Conservation - Retrofits	Indirect	25,395,815	123,019,789
	<b>Total</b>		<b>80,145,666</b>	<b>293,447,994</b>

**RESULTS**

**DETAILED RESULTS FOR THE MULTI-INTEGRATED VERSION OF THIS SCENARIO (SCENARIO 2B) ARE PRESENTED IN THE FOLLOWING TABLES.**

<sup>8</sup> Sum of net-present value of annual costs over the timeframe.

<sup>9</sup> No scenario-specific assumptions required

COST-BENEFIT ANALYSIS REPORT

APPENDIX E

**Table 8. Scenario 2B Benefit-Cost Ratios**

Ratio Type	5-Year Analysis	10-Year Analysis
Total	1.8	2.8
Direct Benefits and Costs only <sup>10</sup>	1.3	3.1

To illustrate how the costs and benefits are distributed across stakeholder groups, we present the following tables.

**Table 9. Scenario 2B Costs by Stakeholder Group (5-year horizon)**

Cost Category	Cost Type	Stakeholder Group				
		Electricity Utility (\$)	Natural Gas Utility (\$)	Water Utility (\$)	Customers (\$)	Total (\$)
Implementation (One-time setup and integration costs)	Direct	3,458,565	524,157	26,450,138	-	<b>30,432,861</b>
Operational Costs <sup>11</sup>	Direct	435,205	300,228	432,792	-	<b>1,168,226</b>
Retrofit Costs	Indirect	-	-	-	12,578,686	<b>12,578,686</b>
<b>Total</b>		<b>3,893,771</b>	<b>824,385</b>	<b>26,882,930</b>	<b>12,578,686</b>	<b>44,179,773</b>

<sup>10</sup> Direct benefits and costs are a subset of total benefits and costs. However, the direct benefits and costs *ratios* are higher than the total ratios because the magnitude of benefits to costs is different for direct results than for total results.

<sup>11</sup> Sum of net-present value of annual costs over the timeframe.

COST-BENEFIT ANALYSIS REPORT

APPENDIX E

**Table 10. Scenario 2B Benefits by Stakeholder Group (5-year horizon)**

Benefit Category	Benefit Component	Benefit Type	Stakeholder Group					Total (\$)
			C&I (\$)	Industrial (\$)	Other (\$)	Residential (\$)	Utility (\$)	
Operational Efficiencies	Customers' Utility Consumption, Billing and Generation Data Process Efficiencies	Direct	11,708,323	9,443	9,576,590	2,759,875	-	<b>24,054,230</b>
	Process Efficiencies	Direct	14,073,947	93,992	-	-	-	<b>14,167,939</b>
	Reduced Customer Care Efforts	Indirect	-	-	-	-	1,559,328	<b>1,559,328</b>
	CDM/DSM Program Efficiencies and Innovation	Indirect	-	-	-	-	1,627,629	<b>1,627,629</b>
Energy Efficiency and Conservation	Increased Conservation - Behavioural & Operational	Indirect	11,758,678	17,431	-	1,564,616	-	<b>13,340,724</b>
	Increased Conservation - Retrofits	Indirect	19,031,618	73,190	-	6,291,008	-	<b>25,395,815</b>
	<b>Total</b>		<b>56,572,566</b>	<b>194,055</b>	<b>9,576,590</b>	<b>10,615,498</b>	<b>3,186,957</b>	<b>80,145,666</b>

**DIRECT AND INDIRECT COSTS**

The following table provides a breakout of direct and indirect benefits and costs for two key scenarios. We note that these costs are high level and used to generate comparisons between potential scenarios; they are not implementation-level cost estimates.

**Table 11. Breakout of Direct and Indirect Benefits and Costs, Single and Multi-Integrated (10-year horizon)**

10 Years	Single Integrated Hosted				Multi-Integrated Hosted			
	Benefits		Costs		Benefits		Costs	
	Direct	Indirect	Direct	Indirect	Direct	Indirect	Direct	Indirect
Electricity	\$62,275,755	\$136,049,865	\$4,578,270	\$50,137,048	\$62,275,755	\$136,049,865	\$4,754,206	\$50,137,048
Electricity and Natural Gas	\$80,428,288	\$173,834,221	\$5,993,878	\$60,072,210	\$80,428,288	\$173,834,221	\$6,169,814	\$60,072,210
Electricity, Natural Gas, and Water	\$104,514,518	\$188,933,476	\$33,028,644	\$71,377,618	\$104,514,518	\$188,933,476	\$33,932,165	\$71,377,618

**ADDITIONAL COST-BENEFIT RATIO RESULTS FOR THE MULTI-INTEGRATED HOSTED SCENARIOS**

The following table provides updated cost-benefit ratios for multi-integrated scenarios. Most of the results are the same as when a 2% discount rate is used, since the relative change in results is applied to both costs and benefits.

**Table 12. Green Button DMD/CMD Multi-Integrated Scenario Cost-Benefit Results**

Utility Type	5-Year	10-Year
Electricity	4.04	3.6
Electricity and Natural Gas	4.4	3.8
Electricity, Natural Gas, and Water	1.8	2.8
Natural Gas Component	6.1	4.9
Water Component	0.5	1.0



## Data Platform Governance Council - Qualifications

In response to the New Hampshire Public Utilities Commission's request for a list of NH Data Platform Governance Council members and their qualifications, we are providing the attached documents. Please note that the Council also relies on the expertise of numerous utility staff who regularly attend Council meetings, and who would also be responsible for contracting and implementing the platform. While this group brings a wide range of expertise, this document will focus on the qualifications that the Council believes are most pertinent to its success in overseeing the creation and management of the NH Energy Data Platform.

The following is a partial list of the qualifications that members of the Council need to embody, based on the responsibilities laid out in section II.B. of the Docket DE 19-197 Settlement Agreement:

**Stakeholder Representation:** To elicit and articulate the needs of a particular stakeholder group and advocate for their priorities or voice concerns about issues that could negatively impact them.

**Consensus Negotiation:** To engage in respectful dialog with representatives of other stakeholders and find mutually acceptable solutions or opportunities for compromise.

**Policy and Process Development:** To articulate the governing policies for the Platform and associated services and the means for those policies to evolve over time.

**Software Requirements Specification:** To establish the functional and technical requirements of the platform and articulate them in the RFP.

**Technical Project Planning and Management:** To plan and oversee the design, implementation, and operation of the Platform.

**Data Structures and Standards:** To develop the Logical Data Model and determine whether the APIs and utility back-end systems comply with those standards.

**Data Privacy and Security Policies and Practices:** To develop minimum requirements for all components of the platform and verification procedures to ensure that both utility back-end systems and vendor-provided Platform Hub systems meet those requirements.

**Software Quality Assurance and Testing:** To create unambiguous acceptance criteria and procedures for ensuring that all software systems deliver all the required functionality with no adverse behavior.

**User Outreach and Complaint Resolution:** To educate members of the different user communities (energy service providers, software developers, commercial and residential customers, etc.) about the platform, elicit feedback, and address their concerns.

**The Qualifications of Prof. Amro Farid were stated in his testimony at pp. 131-133 of Exhibit 9 of this docket DE 19-197,<sup>1</sup> which are recapitulated below for convenient review. Dr. Farid is also now a Visiting Associate Professor at MIT and a Fulbright Future Scholar contributing to the Australian government's 2022 National Hydrogen Infrastructure Assessment.<sup>2</sup> Some of his publications since his prefiled testimony from August 2020 can be found through the IEEE website.<sup>3</sup>**

**Q1.1. Please state your name, business address, and position relative to this docket.**

A1.1. My name is Dr. Amro M. Farid. I am an Associate Professor of Engineering at the Thayer School of Engineering at Dartmouth<sup>4</sup> and an Adjunct Associate Professor of Computer Science at the Department Science at Dartmouth College, which is located at 14 Engineering Drive, Hanover, NH. I am also the Chief Executive Officer of Engineering Systems Analytics (ESA) LLC which is located at 89 Washburn Hill Road, Lyme NH.

**Q1.2. Please describe your background and qualifications as they relate to energy data platforms and software development.**

A1.2. I received my B.Sc. in 2000 and M.Sc. in 2002 from the MIT Mechanical Engineering Department. I received my Ph.D. in Engineering in the area of Industrial Automation and Control Systems Engineering from the University of Cambridge (UK) in 2007. In addition to the formal positions stated above, I am the director of the Laboratory for Intelligent Integrated Networks of Engineering Systems (LIINES) at the Thayer School of Engineering at Dartmouth.<sup>5</sup> I am a research affiliate at the MIT Mechanical Engineering Department. I currently also serve as Chair of the Council of Engineering Systems Universities<sup>6</sup> (CESUN). I am the Chair of the IEEE Smart Cities Technical Activities Committee<sup>7</sup>, the Chair of the IEEE Smart Buildings Loads and Costumers Architecture Subcommittee<sup>8</sup>, and the Co-Chair of the IEEE Systems, Man &

---

<sup>1</sup> [https://www.puc.nh.gov/Regulatory/Docketbk/2019/19-197/TRANSCRIPTS-OFFICIAL%20EXHIBITS-CLERKS%20REPORT/19-197\\_2021-05-05\\_EXH\\_9.PDF](https://www.puc.nh.gov/Regulatory/Docketbk/2019/19-197/TRANSCRIPTS-OFFICIAL%20EXHIBITS-CLERKS%20REPORT/19-197_2021-05-05_EXH_9.PDF).

<sup>2</sup> <https://engineering.dartmouth.edu/news/professor-amro-m-farid-receives-2021-fulbright-scholar-award-to-australia>

<sup>3</sup> <https://ieeexplore.ieee.org/author/38665664100>

<sup>4</sup> <https://engineering.dartmouth.edu/people/faculty/amro-farid>

<sup>5</sup> <https://amfarid.scripts.mit.edu/>

<sup>6</sup> <https://cesun.org/>

<sup>7</sup> <https://smartcities.ieee.org/about/ieee-smart-cities-committees>

<sup>8</sup> <https://site.ieee.org/pes-sblc/subcommittees/>

Cybernetics Technical Committee on Intelligent Industrial Systems<sup>9</sup>. I am a senior member of the IEEE and a member of the ASME and INCOSE.

As an academic, I maintain an active and broad computational research expertise in intelligent energy systems across five research themes: smart power grids, energy-water nexus, electrified transportation, industrial energy management, and interdependent smart city infrastructures. Consequently, we have extensive experience in software engineering and “Big Data Analytics” as they pertain to energy applications. I have published over 140 peer-reviewed publications in these areas. Our research projects have been externally funded by ISO New England, the Electric Power Research Institute, the Department of Energy, the Department of Defense, the National Science Foundation, and Mitsubishi Heavy Industries. This academic research has led to several notable achievements of particular relevance to this docket. 1) The Dartmouth-LIINES has published some of the latest methodological research supporting the integration of variable renewable energy, energy storage, and demand-side resources. 2) We have conducted the 2017 ISO New England System Operational Awareness and Renewable Energy Study (SOARES) and presented it to ISO New England stakeholders in 2018. 3) We have published the first book on the “energy Internet of Things” (eloT). It discusses how network-enabled energy devices (or the energy Internet of Things) will play an indispensable role in bringing about a cost-effective transition to sustainable energy. 4) We have published extensively on distributed-ledger based “Transactive Energy” markets and control systems where deregulated retail electricity markets support near real-time transactions of electricity from distributed energy resources (DERs) in a manner that is similar to the energy markets found in wholesale independent system operators. The Dartmouth-LIINES has also completed several relevant publications on the Shared Integrated Grid, in general, and the more specific cases of New England region and the State of New Hampshire.

---

<sup>9</sup> <https://sites.google.com/view/ieece-smc-tc-iis/>



As a professor, I actively teach a course on model-based systems engineering which explains how to collaboratively architect, design, and ultimately implement complex engineering systems including, specifically, complex software systems. I also actively teach a course in power systems engineering from technical, economic, and policy perspectives.

As a small business owner of ESA LLC, we have developed the Electric Power Enterprise Control System (EPECS) Simulator and licensed it to ISO New England for their planned integration of variable renewable energy, energy storage, and demand-side resources. It was the central software used in the SOARES study. ISO New England is currently using the EPECS and plans on doing so until 2025 (at a minimum).

**The Qualifications of Assistant Mayor Clifton Below were stated in his testimony at pp. 3-5 of Exhibit 9 of this docket DE 19-197,<sup>10</sup>** which are recapitulated below for convenient review. Below is currently serving in his 8<sup>th</sup> year as a Lebanon City Councilor and is in his 4<sup>th</sup> year as Assistant Mayor. He Chair of the Board of the Community Power Coalition of New Hampshire (CPCNH) comprised of 18 municipal members that represent 20% of the state's residential population, plus one county. His role on the Governance Council is to represent the perspective of communities developing power aggregations. He previously collaborated with other stakeholders interested in the development of community power in petitioning the PUC for proposed rules for community power, including the cities of Keene and Claremont, the Office of the Consumer Advocate, Clean Energy New Hampshire, Conservation Law Foundation, Standard Power, Good Energy, Freedom Energy Logistics, and Colonial Power Group.<sup>11</sup>

**Q. Please describe your relevant experience and expertise regarding electric utilities.**

A. A detailed background statement can be found at p.66 of my testimony attachments in DE 19-067 found under tab 43<sup>12</sup>. I will only highlight a few keys elements of my background here. During my tenure as a State Representative from 1992-1998 I served on the House Science, Technology, and Energy Committee where I was heavily involved in energy and regulatory legislation. As Chair of the Policy Principles, Social and Environmental Issues Subcommittee of the Retail Wheeling and Restructuring Study Committee in 1995 I facilitated a consensus building legislative and stakeholder process that resulted in recommended "Restructuring Policy Principles" that became the core of NH's Electric Utility Restructuring statute, RSA 374-F, that was enacted to restructure and guide the future regulation of electric utilities in NH . In 1998 I was elected to the NH Senate, serving on the energy and utility policy committees throughout my six-year tenure. From 1997-2004 I served on the Advisory Council on Energy of the National Conference of State Legislatures (NCSL), including 3 years

---

<sup>10</sup> [https://www.puc.nh.gov/Regulatory/Docketbk/2019/19-197/TRANSCRIPTS-OFFICIAL%20EXHIBITS-CLERKS%20REPORT/19-197\\_2021-05-05\\_EXH\\_9.PDF](https://www.puc.nh.gov/Regulatory/Docketbk/2019/19-197/TRANSCRIPTS-OFFICIAL%20EXHIBITS-CLERKS%20REPORT/19-197_2021-05-05_EXH_9.PDF).

<sup>11</sup> [https://www.puc.nh.gov/Regulatory/Docketbk/2021/21-142/INITIAL%20FILING%20-%20PETITION/21-142\\_2021-12-01\\_CPCNH\\_PETITION-RULEMAKING.PDF](https://www.puc.nh.gov/Regulatory/Docketbk/2021/21-142/INITIAL%20FILING%20-%20PETITION/21-142_2021-12-01_CPCNH_PETITION-RULEMAKING.PDF)

<sup>12</sup> [https://www.puc.nh.gov/Regulatory/Docketbk/2019/19-064/TESTIMONY/19-064\\_2019-12-10\\_COL\\_ATT\\_TESTIMONY\\_FILED\\_12-09-19.PDF](https://www.puc.nh.gov/Regulatory/Docketbk/2019/19-064/TESTIMONY/19-064_2019-12-10_COL_ATT_TESTIMONY_FILED_12-09-19.PDF).

as Chair, which advised NCSL staff on emerging energy issues that may need the attention of state legislatures. I also served on the Energy & Electric Utilities Committee, Assembly on Federal Issues of NCSL where, as Chair in 2000-2001, I facilitated a consensus based comprehensive update of NCSL's National Energy Policy. I testified on behalf of NCSL before the United States Senate Committee on Energy and Natural Resources on "Electric Industry Restructuring," focusing on transmission and jurisdictional issues. I also served as a member of the National Council on Electricity Policy Steering Committee from 2001-2004, which was a policy collaborative with NARUC, NGA, and NASEO.

In late 2005 I was appointed to serve as a NHPUC Commissioner with my tenure ending in February 2012. During that time, I served on the FERC-NARUC Smart Grid and Demand Response Collaborative, 2008-2011, and on the Electric Power Research Institute (EPRI) Advisory Council, 2009-2011 and its Energy Efficiency/Smart Grid Public Advisory Group, 2008-2010. I also served in a variety of other capacities, including as a Vice Chair of NARUC's Energy Resources and Environment Committee, as a member and Co-Chair of the NEEP Steering Committee for the Regional Evaluation, Measurement & Verification (EM&V) Forum, and as President of NECPUC. Through my involvement in NCSL, NARUC, NECPUC, ISO New England stakeholder processes and particularly with EPRI I was fortunate to enjoy numerous deep dives into emerging issues in the electric utility industry at the intersection of technology, science, policy, markets, and regulation, including grid modernization, smart rates, market design, energy efficient technologies, and distributed energy resource issues.

**Melissa Samenfeld**  
**Rates Analyst II – Liberty Utilities**

I am currently employed as a Rates Analyst II for Liberty Utilities Rates and Regulatory Affairs department and am responsible for providing rate-related services for EnergyNorth Natural Gas and Granite State Electric. I graduated from Southern New Hampshire University in 2014 with a Bachelor of Science degree in Business Administration, with a concentration in Organizational Leadership.

Some of my current responsibilities include: supporting departments for studies, projects, and research and analysis for regulatory affairs; conducting analysis and gathering data to provide advice to company's management on emerging regulations and developments in the industry; identify areas of concern within projects/programs and collaborate with appropriate departments for solutions; docket management; and supporting all aspects of Liberty's Battery Storage Pilot program.

## Michael E. Murray

---

### EXPERIENCE

**Mission:data Coalition**      **President**      Dec 2013 – present

- Co-founded non-profit coalition of 30+ companies (representing \$1b/year in energy management) to support electricity consumers' access to data from smart meters, thereby enabling data-driven energy efficiency measures and dramatically reducing transaction costs ([www.missiondata.io](http://www.missiondata.io))
- Nationally-recognized expert on data privacy and data portability
- Testified before public utility commissions in California, Colorado, Georgia New York, North Carolina, Ohio and Texas

**Lucid**      **CEO and President**      May 2004 – Oct 2014

- Co-founded Lucid and led the company to profitability with market-leading energy efficiency software products. Building Dashboard® tracks energy and resource consumption information in commercial buildings to empower and motivate conservation behaviors. BuildingOS® is a cloud-based operating system for buildings that connects building automation systems, lighting controls, inverters and submeters into an online platform. The company was sold to Acuity Brands (NYSE: AYI).

#### Lucid Company Statistics

*Employees:* 45

*Customers:* Over 350 including Google, Yahoo!, Starbucks, Fidelity Investments, Washington D.C. district government, all eight Ivy League universities, K-12 school districts, local and state governments

*Partnerships:* Siemens, Johnson Controls, Constellation Energy, U.S. Green Building Council, U.S. EPA's ENERGY STAR®

#### Lucid Awards

**Cleantech Group's "Global 100" Top Cleantech Company 2014**

**California Cleantech "Game Changer" Award 2011** – *Formal resolution by the California Legislature and Assemblymember V. Manuel Pérez to 18 leading companies including Lucid, Tesla and Sungevity*

**Adobe MAX Award 2010** – *Best Application in Social Computing*

**Press:** [New York Times](http://www.nytimes.com), Forbes, CBS Smart Planet, WIRED, Treehugger.com, NPR, Gartner "Cool Vendor in Sustainability"

## PATENTS

#8,375,068: *Extensible Framework and Graphical User Interface for Sharing, Comparing, and Displaying Resource Usage Data* (issue date: February 12, 2013). Systems and methods for presenting data showing comparative electricity, water and natural gas consumption, and an extensible framework and user interface that facilitates the sharing, comparing, and displaying of such data in competition and goal-setting environments.

#8,176,095: *Collecting, Sharing, Comparing, and Displaying Resource Usage Data* (issue date: May 8, 2012). Interactive and comparative displays of electricity, natural gas and water consumption data in group environments such as social networks.

## SELECTED PRESENTATIONS

### White House Presentations

“The Promise of Green Button Energy Data” at the White House’s *Energy Datapalooza* with the **U.S. Secretary of Energy Steven Chu** and **U.S. Chief Technology Officer Todd Park**. Oct 2012. <http://player.vimeo.com/video/50575212>

“Green Button’s role in Commercial Building Energy Efficiency.” Presentation with first **U.S. Chief Technology Officer Aneesh Chopra** appointed by President Obama. Hosted by Silicon Valley Leadership Group. Jan 2012.

International keynote: Energy Consumers Australia’s *Foresighting Forum*. February, 2019 in Sydney, Australia. <https://youtu.be/x9B8CkGPZiY>

“Waiting for Data: Market Adaptations to Poor Smart Meter Policies in America.” Presentation at TEDDINET, Edinburgh Centre for Carbon Innovation, UK. July 2016. <https://youtu.be/VXaTpqmiE9A>

## PUBLICATIONS

“Digital Platform Regulation.” Mission:data Coalition. January, 2021. <http://www.missiondata.io/s/Digital-Platform-Regulation.pdf>

“Energy Data Portability: Assessing Utility Performance and Preventing ‘Evil Nudges.’” Mission:data Coalition. January, 2019. <http://www.missiondata.io/s/Energy-Data-Portability.pdf>

“Energy Data: Unlocking Innovation With Smart Policy.” Mission:data Coalition. Dec 2017, with Robert King and Laura Kier. <http://www.missiondata.io/s/Energy-data-unlocking-innovation-with-smart-policy.pdf>

“New Smart Meter Policies Yielding Data (and Savings) for End-Users” published in the journal *Natural Gas & Electricity*, Nov, 2016, p. 9-15, with James Hawley.

## C. Riley Hastings

318 Greendale Ave, Needham, MA 02494

Email: [rileyhastings13@gmail.com](mailto:rileyhastings13@gmail.com) Phone: 617-308-5794

---

<b>EXPERIENCE</b>	<b>EVERSOURCE ENERGY, Westwood, MA</b> <b>Lead Analyst, Energy Efficiency Regulatory, Planning, &amp; Evaluation</b> <b>May 2020 – Present</b> <ul style="list-style-type: none"><li>• Provide input into the modernization and standardization of energy efficiency data management practices across Eversource's three state service territory.</li><li>• Lead efforts related to the creation of data management platforms and/or statewide databases</li><li>• Perform internal analysis to provide additional insight and proactively identify potential areas of concern in order to allow implementation to make mid-course corrections.</li><li>• Respond to regulatory or stakeholder requests/inquiries related to data, data management, data platforms, and/or databases.</li><li>• Collaborate with other supervisors and managers, as well as other Program Administrators, regarding data management policies.</li></ul>
	<b>EVERSOURCE ENERGY, Westwood, MA</b> <b>Senior Analyst, Energy Efficiency Regulatory, Planning, &amp; Evaluation</b> <b>July 2010 – May 2020</b> <ul style="list-style-type: none"><li>• Responsible for preparing Energy Efficiency ("EE") plans and reports for regulatory entities including forecasting of expected future performance and analysis of differences between planned and actual performance.</li><li>• Prepare and give presentations for various stakeholder meetings and industry conferences.</li><li>• Provide expert testimony.</li><li>• Manage development and production of reports from various databases and systems.</li><li>• Oversee the collection and analysis of information to document the impacts of EE programs and improve the effectiveness of these programs.</li><li>• Responsible for overseeing consultants who manage utility data, conduct impact evaluations, market evaluations, process evaluations, market characterizations or assessments and evaluations of new initiatives.</li><li>• Manage maintenance and recommend improvements to a Statewide website which the MA utilities utilize to report performance in their EE programs.</li><li>• Conduct economic analysis to determine cost-effectiveness and net savings of individual technologies, programs, and services.</li></ul>
	<b>OPINION DYNAMICS CORPORATION, Waltham, MA</b> <b>Energy Research Manager, Energy Area</b> <b>October 2005 – July 2010</b> <ul style="list-style-type: none"><li>• Program CATI and Internet surveys, develop survey instruments, and review survey instrument skip patterns and design.</li></ul>



- Provide direction to operations staff in my role as a liaison between project managers and operations staff.
- Responsible for sample analysis, database development, and data management.
- Adept at managing databases and developing innovative ways to handle data.
- Analysis and reporting of client satisfaction, process evaluation and impact evaluation survey results for Independent System Operator and utility clients.
- Perform regression analyses using survey data to examine the relationship between client satisfaction and factors that drive satisfaction (i.e., responsiveness, cost, etc.).
- Prepare datasets for billing analyses, prospective benefits and net-to-gross calculations.

**ABT ASSOCIATES INC.**, Cambridge, MA **January 1998 - October 2005**

**Analyst**, Environmental Research Area (Economics Practice Group)

- Developed methodologies to analyze economic and financial impacts, cost-effectiveness, small business impacts, foreign trade effects, community impacts and impacts on governments.
- Designed complex spreadsheet models and databases to evaluate impacts on facilities and firms owning facilities subject to regulation for a variety of U.S. EPA regulations.
- Performed econometric analyses using SAS to estimate baseline capital expenditure spending and effects on prices due to regulation.
- Analyzed publicly available data to determine the size, structure, competitiveness and financial condition of facilities and firms within a variety of manufacturing industries.
- Oversaw and managed day-to-day activities of other staff.
- Responsible for quality assurance and control for various projects.

**THE WALL STREET JOURNAL**, New York, NY **Summers 1994 - 1996**

**Marketing Research Intern**, Sales and Marketing Department

- Developed an analytical model for targeted marketing activities in high tech, automotive and travel categories.
- Designed and executed extensive spreadsheet analysis on client and competitive trends.
- Initiated and presented briefing materials and background analysis with and for sales executives.
- Designed presentation materials for clients with sales executives.

EDUCATION COLGATE  
UNIVERSITY Hamilton, NY B.A. in  
Economics May 1997

**PRESENTATIONS** Riley Hastings, Jason Lai (Navigant), Bob Wirtshafter (Wirtshafter Associates), *Multifamily Program Design Opportunities and Where to Find Them: Discovering Customer Insights from Diverse Data Sources*, International Energy Program Evaluation Conference, Denver, CO, August 2019.

Riley Hastings, Justin Spencer (Navigant), *Measuring up -- how does my baseline compare?*, International Energy Program Evaluation Conference, Baltimore, MD, August 2017.

Riley Hastings, Michael Goldman, *Driving Miss Participation*, Association of Energy Service Professionals National Conference, Orlando, FL, February 2015.

Riley Hastings, Michael Goldman, *A Case Study in Targeted Residential Marketing: Customizing Marketing Campaigns Based on Customer Data*, Association of Energy Service Professionals National Conference, San Diego, CA, January 2014.

Riley (Newbert) Hastings, Jennifer Mitchell-Jackson, Sharyn Barata, *Channeling Customers: Effects of Information-Based Programs as Feeders into Resource Acquisition Programs*, Association of Energy Service Professionals National Conference, Las Vegas, NV, January 2007.

**SKILLS** Proficient in Excel, Access, Word, PowerPoint, SPSS, and SAS.

**REFERENCES** Available upon request.

### **Tim Sink Bio**

Tim Sink is President & CEO of the Greater Concord Chamber of Commerce, New Hampshire's State Capital Chamber of Commerce serving more than 900 businesses and organizations from throughout Central New Hampshire.

Tim is active on the board of the NH Association of Chamber of Commerce Executives and serves as Administrator for the New England Association of Chamber of Commerce Executives. He is a graduate of the Institutes for Organizational Management from the University of Colorado and the Center for Creative Leadership in Greensboro, NC. He earned a bachelor degree in music education from Notre Dame College and performs regularly at various Jazz venues.

Tim has an extensive network of Chambers of Commerce throughout New England representing thousands of businesses collectively. This is a potential asset to the project in terms of business outreach and data gathering

Locally, he currently serves on the board of directors for Care Women's Center NHTI Community College Advisory Board, NH State Council on the Arts and The concord Coalition to End Homelessness Advisory Board.

**Justin Eisfeller**

**Unitil CTO / Vice President, Information Technology**

I am the Vice President, Information Technology for Unitil Service Corp. ("USC"), which provides centralized utility management services to Unitil Corporation's subsidiary companies including Unitil Energy Systems, Inc. and Northern Utilities, Inc. As VP, Information Technology, I am responsible for Unitil's information technology infrastructure, software development, cyber security and software systems support. I have previously held the positions of Manager of Distribution Engineering, Director of Engineering and Director of Energy Measurement and Control at USC.

I received my Bachelor of Science Degree in Electrical Engineering (Power Option) from 25 Northeastern University in 1990 and my Master of Business Administration from the University of New Hampshire in 2005. I joined USC in 2002 as Manager of Distribution Engineering and was promoted in 2004 to the position of Director of Engineering with responsibilities for distribution engineering, planning, transmission and substation engineering, system protection and control, computer aided design, and geographic information systems. In 2008, I assumed responsibilities of Director, EM&C and in 2017 I was promoted to VP, Information Technology, which is my current position.

I have been a registered Professional Engineer in the State of New Hampshire since 1996; received my Project Management Professional certificate in 2005; and received my Information Technology Infrastructure Library Foundation Certificate in IT Service Management in 2018.

**Kimberly Hood**

**Unitil Manager of Cyber Security and Compliance**

I am the Manager of Cyber Security and Compliance for Unitil Service Corp. (“USC”), which provides centralized utility management services to Unitil Corporation’s subsidiary companies including Unitil Energy Systems, Inc. and Northern Utilities, Inc.

I have 30 years of experience in a variety of information systems roles, including both programming and infrastructure. I have a BS in Computer Science from Oklahoma Christian University and a Master’s Certificate in Cyber Security with a concentration in Power Systems from Worcester Polytechnic Institute. I joined Unitil in September of 2012 where I am the Manager of Cyber Security and Compliance. I am responsible for cyber security policies and procedures, security awareness training, threat and vulnerability management, vendor security posture assessment, Industrial Control System (ICS) and SCADA infrastructure protection at electric substations and natural gas plants and leading the Cyber Incident Response Team (CIRT). I manage both internal and external audits and assessments including SOX, NERC-CIP, PCI, C2M2/NIST Framework, and penetration testing. In addition, I am a member of the American Gas Association (AGA) Cyber Security Strategy Task Force, the Edison Electric Institute (EEI) Security Committee, and InfraGard NH and Boston.

**Jeremy Haynes**

**Unitil Director of Enterprise IT Systems**

I am the Director of Enterprise IT Systems for Unitil Service Corp. ("USC"), which provides centralized utility management services to Unitil Corporation's subsidiary companies including Unitil Energy Systems, Inc. and Northern Utilities, Inc. I have previously held the positions of Manager, Application Development and Director, Application Development for USC.

I have a Master's Degree in Business Administration from the University of New Hampshire, as well as a Bachelor of Science in Computer Information Systems from Post University and I received my Information Technology Infrastructure Library Foundation Certificate in IT Service Management in 2018.

I joined the Unitil Information Technology department in January 2013 where I have personnel and technological responsibility for all aspects of the design, creation, delivery and support for Unitil's internal line of business applications and database systems as well as broad responsibility for our networking, systems and telecomm infrastructure. In total, I have nearly 25 years of professional IT systems and software experience with increasing levels of hands on technical and managerial responsibility covering a wide range of varied vertical domains including the Electric and Gas industry.

**Mark Lambert**

**Unitil Vice President, Customer Operations**

I assumed the responsibilities of Vice President, Customer Operations for Unitil in January of 2017. In this role, I am responsible to develop, execute and lead the successful operations for the 5 customer functions – Customer Solutions, Quality Assurance, Accounts Receivables, Customer Billing, Regulatory Rate Compliance and Customer Revenue Reconciliation for the company's distinct utility divisions operating in three state jurisdictions. My most recent prior role was as Unitil's Director of Government Affairs which I held from 2011 to 2017 responsible for the execution of all federal, state and local advocacy and legislative objectives for the gas and electric issues in the company's three statewide jurisdictions. I have testified before the New Hampshire Public Utilities Commission, the Massachusetts Department of Public Utilities and the Maine Public Utilities Commission in previous rate case proceedings, numerous dockets and also in Unitil Corporation's proceeding regarding the acquisition of Northern Utilities, Inc. in 2008. I have most recently provided testimony before the New Hampshire Public Utility Commission in both the UES and NU rate case proceedings.

In addition to responsibilities at Unitil, I serve on the New Hampshire's Air Resource Council representing the natural gas industry, NH/VT American Red Cross chapter, and serves on the strategic steering committee for the New Hampshire Scholars.

### **Qualifications of Stephen R. Eckberg**

My name is Stephen R. Eckberg. I am employed as a Utility Analyst with the Regulatory Support Division of the New Hampshire Department of Energy. My business address is 21 S. Fruit Street, Suite 10, Concord, New Hampshire 03301.

I earned a B.S. in Meteorology from the State University of New York at Oswego and an M.S. in Statistics from the University of Southern Maine.

After receiving my M.S. degree, I was employed as an analyst in the Boston office of Hagler Bailly, Inc, a consulting firm working with regulated utilities to perform evaluations of energy efficiency and demand-side management programs. My responsibilities included complex data analysis including cleaning and combining information from multiple large datasets using SAS statistical analysis software. Subsequently, I was employed as a statistical applications programmer in the Work Environment Department at UMass Lowell. In that position, I was responsible for performing epidemiological data analysis in support of multiple academic research projects. I worked with SAS statistical analysis software on both PC and Unix platforms and taught SAS programming to graduate students. From 2000 through 2003, I was employed at the NH Governor's Office of Energy and Community Services as the Director of the Weatherization Assistance Program. Following that, I was employed at Belknap Merrimack Community Action Agency as the Statewide Program Administrator of the NH Electric Assistance Program (EAP). In that capacity, I presented testimony before the NH Public Utilities Commission (PUC) in dockets related to the design, implementation and management of the EAP. I have also testified before Committees of the New Hampshire General Court on issues related to energy efficiency and low income electric bill assistance. From 2007 – 2014 I was employed as a Utility Analyst with the New Hampshire Office of the Consumer Advocate (OCA). During my tenure with the OCA, I attended rate making and regulatory training at New Mexico State University's Center for Public Utilities.

In my position with the OCA, I entered pre-filed testimony jointly with Kenneth E. Traum, former Assistant Consumer Advocate, in the following dockets: • DG 08-048 Unitil Corporation and Northern Utilities, Inc. Joint Petition for Approval of Stock Acquisition • DW 08-070 Lakes Region Water Company Financing & Step Increase

- DW 08-098 Aquarion Water Company of New Hampshire
- DE 09-035 Public Service of New Hampshire Distribution Service Rate Case I entered (non-joint) pre-filed testimony in the following dockets:
  - DT 07-027 Kearsarge Telephone Company, Wilton Telephone Company, Hollis Telephone Company & Merrimack County Telephone Company Petition for Alternative Form of Regulation. Phase II & Phase III.
  - DW 08-073 Pennichuck Water Works, Inc. Petition for Rate Increase



- DW 08-070 Lakes Region Water Company Third Step Increase.
- DW 08-065 Hampstead Area Water Company Petition for Rate Increase.
- DE 09-170 2010 CORE Energy Efficiency Programs.
- DW 10-090 Pittsfield Aqueduct Company Petition for Rate Increase.
- DW 10-091 Pennichuck Water Works Petition for Rate Increase.
- DW 10-141 Lakes Region Water Petition for Rate Increase.
- DE 10-188 2011-2012 CORE and Natural Gas Energy Efficiency Programs.
- DE 11-250 PSNH Installation of a Wet Flue-Gas Desulphurization Scrubber.
- DE 12-262 2013-2014 CORE and Natural Gas Energy Efficiency Programs.
- DE 12-292 PSNH 2013 Default Energy Service Rate.
- DE 12-262 2014 CORE Energy Efficiency Programs Update Filing.
- DE 13-108 PSNH 2012 Energy Service Reconciliation.
- DG 14-091 Liberty Utilities Special Contract and Lease Agreement with Innovative Natural Gas, LLC dba iNATGAS.

In August 2014, I joined the PUC's Sustainable Energy Division (SED). My responsibilities included grant review and administration, and compliance oversight of New Hampshire's Renewable Portfolio Standard requirements. While employed with SED, I filed testimony in:

- DE 18-140 Liberty Utilities Petition for Approval of a Renewable Natural Gas Supply and Transportation Contract

In October 2019, I joined the PUC's Electric Division. During my tenure there, I filed testimony in:

- DE 17-136 2018-2020 New Hampshire Statewide Energy Efficiency Plan - 2020 Third Year Programs.
- DE 19-197 Development of a Statewide, Multi-Use Online Energy Data Platform (Joint Testimony with Jason Morse).
- DE 20-092 2021 – 2023 Triennial Energy Efficiency Plan.
- DE 21-030 Unitil Request for Change in Rates.

In July 2021, with the passage of HB2, the New Hampshire Legislature created the Department of Energy, I became an employee of the Regulatory Support Division of the Department of Energy.

- DE 21-020 Eversource Energy and Consolidated Communications Joint Petition to Approve Pole Asset Transfer.
- DG 21-104 Northern Utilities, Inc. Request to Change Rates.

In addition to dockets in which I have filed testimony, I have been the primary regulatory analyst on many other dockets, working closely with Staff attorneys to prepare for participation in technical sessions and regulatory hearings before the NH Public Utilities Commission. These dockets have covered such matters as default energy service, stranded costs, transmission costs, master metering waiver requests, franchise boundary adjustments, and annual major storm report reviews.

# Ethan Goldman

[ethan@resilientedge.io](mailto:ethan@resilientedge.io) · 5 Pavilion Ave., South Burlington, VT 05403 · (412) 759-1036

---

## Experience

**Resilient Edge, LLC: Founder** (2020-Present). Supporting the transition to a carbon-neutral energy system by designing data-driven software, analysis approaches, and policy solutions that deliver demand flexibility from resilient buildings and communities. Harnessing smart meter and connected device data to fully value demand-side services. Providing energy research, data analysis, and consulting services.

- Created the load research component for a Distributed Energy Resources (DER) Potential Study.
- Provided technical support for the ENERGY STAR™ Smart Thermostat certification savings metric.
- Measured energy and hourly peak demand savings of weatherization and HVAC upgrades.
- Co-authored "[Maximizing Mini-Split Performance Report](#)" on improving heat pump programs.
- Provided guidance on energy data analytics strategy and methods for a distribution utility.
- Provided measurement and verification support for a new energy-saving product.

**Recurve: Director of Customer Solutions** (2019). Promoted the use of metered savings and performance-based incentive programs to regulators, program administrators, and implementers. Worked with clients to specify and configure Recurve's automated efficiency M&V platform; trained clients to use the platform and incorporate the results into their operations. Demonstrated the platform and the underlying open-source CalTRACK methods to prospective clients and at conferences.

**VEIC: Energy Informatics Architect** (2012-2018). Designed and managed systems for gathering, storing, analyzing, and presenting interval data from utility meters, sub-meters, smart thermostats, and other sources. Supported R&D projects with technical specifications, recommendations, and implementation assistance. Promoted VEIC's data analytics capabilities at conferences, developed relationships with customers, and gathered market intelligence.

- **Technical Lead** for the creation of Smart Thermostat Analytics Toolkit (2016-2018).
- **Subject Matter Expert** on 2013-2015 Efficiency Vermont Smart Thermostat pilot.
- **Product Manager** for Efficiency Vermont's sub-meter analytics platform (2015-2017).
- **Subject Matter Expert** for Efficiency Vermont's state-wide AMI data platform (2011-2014).

**VEIC: Evaluation, Measurement, and Verification Specialist** (2009-2012). Oversaw and maintained metering equipment and procedures for measuring energy efficiency and coincident demand savings.

**BuildingGreen, Lead Web Application Developer** (2001-2007) Gathered requirements, designed, specified, and coded internet and intranet applications for ecommerce and content management.

## Education

Research MS, **Carnegie Mellon University**, Green Design / Energy Informatics, 2009.

Co-developed a patented non-intrusive load monitoring system for disaggregating electrical loads and estimating individual appliance energy consumption from whole-house meter data.

BA, **Hampshire College**, Concentration in Computer Science (focused on Machine Learning) and Sustainability, 2001. Thesis: *Cultivating Energy Consciousness Through Feedback: Designing Home Energy Use Monitors for Conservation*

## Specialized computer skills

Data cleaning, analytics, and visualization in Excel and Python; data acquisition with loggers and internet-connected systems. Tinkering with Arduino, Raspberry Pi, WiFi / cellular / LoRa radio, and similar embedded systems for acquiring and visualizing data with ambient displays.

## Leadership and Affiliations

- DOE / Lawrence Berkeley National Labs Demand Flexibility M&V Working Group, Member.
- CalTRACK Working Group, Member, 2018-2019; Chair, 2020.
- Lawrence Berkeley National Labs M&V 2.0 National Stakeholder Group, Member.
- New England Energy Efficiency Partnership (NEEP) Loadshape Sub-Committee, Member.
- Consortium for Energy Efficiency Commercial Whole Building Performance Committee, Member.
- ENERGY STAR Smart Thermostat Metric Working Group, Member.
- American Council for an Energy Efficient Economy (ACEEE) Intelligent Efficiency Conference, Coordinating Committee, 2015.

## Patents

*System and Methods for Assessing Whole-Building Thermal Performance* ([US9709449B2](#)) Thermostat data analysis technique for estimating the building envelope's thermal efficiency by automatically identifying quiescent periods from indoor temperature data and comparing the rate of change to the outdoor temperature. Filed 2014, granted 2017.

*Methods and Apparatuses for Monitoring Energy Consumption and Related Operations* ([US9104189B2](#)) Non-intrusive load monitoring system that detects transients in the signal, extracts a "signature" of indicative features, and automatically classifies it against a catalog of previously labeled signatures. Filed 2010, granted 2015.

## Selected Publications

“Maximizing Mini-split Potentials” (2022; in review). ACEEE Summer Study on Energy Efficiency in Buildings

“Toward Residential Upgrade Savings Guarantees: An AMI-based Diagnostic Interface” (2022). ECEEE Summer Study on Energy Efficiency in Buildings

“[Your Guidebook to Adoption of M&V 2.0](#)” (2018). Prepared by VEIC for the Missouri Department of Economics, Division of Energy under a U.S. Department of Energy, State Energy Program grant-funded project.

“[Measuring Demand Savings with Smart Thermostat Data](#)” (2017). International Energy Program Evaluation Conference

“[Overview of Existing and Future Residential Use Cases for Connected Thermostats](#)” (2016). Prepared for: U.S. Department of Energy Office of Energy Efficiency and Renewable Energy, Building Technologies Office

“[Enhancing Electricity Audits in Residential Buildings with Nonintrusive Load Monitoring](#)” (2010) Journal of Industrial Ecology 14 (5), 844-858

## Selected Presentations

“Data Informed Energy Policy” (2021). New Hampshire Local Energy Solutions Conference

“Calculating Metered Savings Using CalTRACK and the OpenEEMeter” (2019). International Energy Program Evaluator Conference (half-day training)

“The Challenge and Opportunity of Thermostat Data” (2018). EPRI Connected Devices Workshop

“Measuring Energy Savings When it Counts: How Smart Grid Data and Open-Source Analytics Can Lead to Savings Load-Shapes” (2015). ADS Smart Grid and Climate Change Conference

“Custom Energy Analytics, Or How I Stopped Worrying and Learned to Love Big Data” (2015). ACEEE Intelligent Efficiency Conference

## Guest Lectures

Carnegie Mellon, 2022: Presented in *Autonomous Sustainable Buildings* on measuring energy impacts

Vermont Law School, 2019 and 2020: Presented in *End-Use Energy Efficiency* course on Advanced M&V

**Donald M. Kreis**, an attorney, has served as New Hampshire's Consumer Advocate since 2016. A former general counsel of the Public Utilities Commission, he has also previously served as a hearing officer with the Vermont Public Utility Commission and as an energy law professor at Vermont Law School, where he co-authored a white paper about customer data privacy. In 2019 he was the principal author of the legislation that became the enabling statute of the statewide utility customer data platform. In 2021 he received an Energy Data Policy Leader award from the Green Button Alliance.

**Christopher James Leigh**

Christopher Leigh is currently the Director and Chief of Information Security Officer at Eversource Energy. Christopher has over 20 years of domestic and global experience in leading cyber-security teams. In the current role, he is responsible for all aspects of information security including Threat and Risk Management, Policy and Compliance, architecture, and Incident Response. Christopher has held similar roles at Consolidated Edison, United Technologies Corporation.

Christopher's education includes a Bachelor of Science in Business Administration, specializing in Accounting and Management, minoring in Psychology from Saint Joseph's College. He also has a Master's degree in Business Economics from Southern Connecticut State University and a Master's degree in Information Assurance from Norwich University. Christopher is a Certified Privacy Professional and a Certified Risk and Information Systems Control professional.

Christopher is an adjunct professor at Boston College and Central Connecticut State University and on the Board of Directors for Community Solutions, Incorporated. He was also a member of the United States Navy Reserves for 14 years and named 2020 Top 100 CISO's by Cyber Defense Awards.

**Donald Perrin** has been the State Energy Manager (SEM) for the State of New Hampshire since August 2017. As the State Energy Manager, I am responsible for administering statewide energy management programs for all state facilities. I manage, track and report energy usage/cost data related to the operations of state-owned and leased buildings through the State's Enterprise Energy Management System (EEMS). Currently, the State has over 1,000 electric and gas accounts within all four Local Distribution Companies.

I came to the State of New Hampshire from Plymouth State University, where I worked previously for 22 years and the last 4 years I served as the Assistant Director of Physical Plant. My training and work experience have included project management (capital and sustainable projects), energy procurements, utility budgeting and tracking and data analysis. I received my bachelor degree in Computer Information Systems from Plymouth State University in Plymouth, NH.