EEI AGA

April 10, 2017

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

To Whom It May Concern:

On behalf of our members, the American Gas Association ("AGA") and the Edison Electric Institute ("EEI") are pleased to submit this response as part of the public comment period for the Cybersecurity Framework Draft Version 1.1 ("Draft Framework"), which the National Institute of Standards and Technology ("NIST") published on its website on Tuesday, January 10, 2017.

AGA, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 71 million residential, commercial, and industrial natural gas customers in the U.S., of which 94 percent — over 68 million customers — receive their gas from AGA members. AGA is an advocate for natural gas utility companies and their customers and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international natural gas companies and industry associates. Today, natural gas meets more than one-fourth of the United States' energy needs.

EEI is the association that represents all U.S. investor-owned electric utilities and its affiliates worldwide. Our members provide electricity for 220 million Americans and operate in all 50 states and the District of Columbia, accounting for approximately 70% of the U.S. electric power industry. Protecting the nation's electric grid and ensuring a safe and reliable supply of power is the electric power industry's top priority. Thus, managing cybersecurity risk is a top priority.

We appreciate the ongoing effort by NIST to support a broad, cross-sector Cybersecurity Framework to reduce cybersecurity risk to critical infrastructure. The ability to maintain flexibility, while sufficiently detailing program components to provide substantive guidance is essential to risk management. The voluntary, high-level nature of the Framework has been critical to its successful deployment throughout industry, and has continued to strengthen the trusted partnership between NIST and private industry.

We believe NIST did an excellent job soliciting input and feedback during the initial drafting of the Framework, during which the Energy Sector was an active participant. As supporters of the NIST process, we appreciate the opportunity to provide the following comments and recommendations on the Draft Framework. We ask that NIST continue to maintain the Framework as a voluntary baseline tool. The Framework should be informative and high level, not prescriptive, and should not take positions in conflict with existing enforceable industry standards. More specific comments to the questions posted by NIST in the Draft Framework, and redline comments on the Draft Framework itself, are included in the attached documents. We look forward to participating in the May workshop.

The Framework should remain a voluntary baseline tool that identifies existing, cross-sector critical infrastructure cybersecurity standards and guidance

Cybersecurity capabilities vary by sector and entity. As noted during the initial drafting of the Framework, reducing the nation's cyber risk requires bringing the cybersecurity of critical infrastructure from all 16 sectors up to a minimum baseline level. This level will not be achieved in the same way for each sector, nor will it be achieved homogenously by organizations within each sector as they all have different critical infrastructure risk profiles. Anything further should continue to be addressed at the sector level through additional guidance in coordination with Sector-Specific Agencies ("SSA").

Strong member use and promotion of the Framework

After the NIST Cybersecurity Framework was released, AGA and EEI members worked with their SSA, the Department of Energy, to align existing cybersecurity risk management programs and tools with the Framework, ultimately producing the *Energy Sector Cybersecurity Framework Implementation Guidance* ("Implementation Guidance"). AGA and EEI members adapted various control-based approaches such as NIST's *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53), others used DOE's Cybersecurity Capability Maturity Model ("C2M2"), and some have integrated these and other approaches. The Framework and its alignment with C2M2 is helpful in encouraging further and more in-depth use of the C2M2 and other cybersecurity approaches. The Implementation Guidance will be updated to incorporate the new additions to the Framework, once finalized.

AGA, EEI, and our members continue to support NIST's efforts by raising awareness of the Framework through a variety of means, including outreach to our member committees and conferences focused on cybersecurity, through the Electricity Subsector Coordinating Council ("ESCC") and the Oil and Natural Gas Subsector Coordinating Council ("ONG SCC"), and in cross-sector venues. Though our members have already employed various cybersecurity risk management activities, the Framework has helped to encourage more comprehensive and mature, enterprise-wide approaches to cybersecurity.

Cybersecurity risk management is a top priority of our members

In addition to the Framework, our members continue to use a number of sector specific standards, guidelines, and practices. Examples include the mandatory and enforceable North American Electric Reliability Corporation Critical Infrastructure Protection ("NERC CIP") Cybersecurity Standards, DOE's voluntary Electricity and Oil and Natural Gas Subsector Cybersecurity Capabilities and Maturity Models, the voluntary *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry*, the Transportation Security Administration ("TSA") *Pipeline Security Guidelines*, and the voluntary NIST *Guidelines for Smart Grid Cyber Security* (NISTIR 7628). These existing requirements and guidelines provide comprehensive guidance that help electricity asset owners and operators to assess, develop, and improve their cybersecurity capabilities. Electric power industry representatives also helped DOE, NIST, and NERC to develop the *Electricity Subsector Cybersecurity Risk Management Process* to help tailor cybersecurity risk management processes to meet organizational requirements. This guideline helps utilities incorporate cybersecurity risk considerations into their existing corporate risk management processes.

Minimize duplication of efforts, and avoid conflicting with existing rules and standards

In July 2016, the Federal Energy Regulatory Commission ("FERC") issued an order directing the NERC to "develop a forward-looking, objective-driven Reliability Standard that provides security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations." [1] The NERC CIP standard, *CIP-013-1 – Cyber Security – Supply Chain Risk Management* ("NERC CIP-013-1"), is currently in draft form. Publishing an updated Framework prior to the release of this mandatory, enforceable standard will be inherently problematic for combination gas-electric companies. NIST should avoid taking a position in opposition to this standard, as it will discourage entities required to implement NERC CIP-013-1 from also implementing version 1.1 of the NIST Cybersecurity Framework. NIST should work to harmonize the Framework updates with the approved version of NERC CIP-013-1 to avoid a counterproductive duplication of efforts.

Supply Chain Risk Management is an ongoing challenge

We view the addition of supply-chain risk management as a substantial improvement to the original Cybersecurity Framework, provided that it aligns with the aforementioned NERC CIP-013-1. We ask, however, that NIST review the updated text and appendices for relevance to operational technology (OT) in addition to information technology (IT), which appears to be the current focus of the draft language. Industry already has taken a number of steps to work with suppliers on viewing cybersecurity as a feature of their products. EEI established a cross-function team of information technology, cybersecurity, sourcing, risk management, and legal professionals to focus on this challenge as well as cyber supply chain integrity risk. Similarly, AGA has set up a task group to address this risk. Both AGA and EEI members are involved in DOE's supply Energy Sector Critical Manufacturers Working Group (ESCMWG), which works to bring together utilities and the vendor community to address supply chain risks.

The updated Framework should continue to be informative and voluntary guidelines, but not prescriptive

Determining what is prescriptive may be difficult due to the volume of input received by NIST from various stakeholders who have different experience, expertise, and perspective. A foundational characteristic of the Framework is that it remains a voluntary guide and is not an auditable standard. Drafters should be careful not to introduce prescriptive and directive language into the Framework, which creates risk for companies and may lead to reduced implementation of the updated Framework. Some of the newly proposed language, particularly in Section 4.2, "Types of Cybersecurity Measurement" is too prescriptive and points to specific technologies, creating applicability problems across the 16 sectors. Given the rapid evolution of tools and capabilities, the Framework and subcategories should continue to be outcome/objective focused to remain technology neutral. Avoiding specific technical solutions enables asset owner and operators to select the practices to reduce risk as well as the appropriate security controls and technologies to be used.

[1] Revised Critical Infrastructure Protection Reliability Standards, Order No. 829 156 FERC ¶ 61,050 at P 4 (July 21, 2016).

Framework methodology should be tailored to improving critical infrastructure cybersecurity while protecting individual privacy and civil liberties

Section 7(c) of Presidential Executive Order 13636 specifies that "[t]he Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and individual liberties."[2] Protecting customer privacy and civil liberties is important, and issues regarding those matters raised during the initial drafting of the Framework remain. However, we are concerned that instead of focusing on means to limit the privacy impacts of the Framework, the methodology appears to recommend independent privacy protections unrelated to the protection of critical infrastructure. Similar to risk management, the scope of privacy and civil liberty protections are beyond that of cybersecurity. The purpose of the framework is to "help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[3] The methodology provided should be tailored to the purpose of the Framework: to improve critical infrastructure cybersecurity. Additionally, it is critical that the privacy methodology is clear and actionable. The existing language does not readily allow companies to discern how to use the methodology or determine whether current practices already incorporate its elements.

Consider who is providing input to the Draft Framework process

Finally, we recommend that NIST consider who is providing the input when updating the Framework and determining how to use the input. We recognize and support NIST's efforts to encourage feedback from critical infrastructure owners and operators and cybersecurity staff, specifically those who have operational, managerial and policy experience and responsibilities for cybersecurity, technology and/or standards development for critical infrastructure companies.

We greatly appreciate the NIST efforts to update the Framework, as well as to listen to and incorporate our feedback. AGA, EEI, and our members look forward to continued collaboration with NIST and our other government partners to improve the cybersecurity of critical infrastructure.

Sincerely,

Scott I. Aaronson	Jim Linn
Executive Director, Security & Business Continuity	Managing Director, Information Technology
Edison Electric Institute	American Gas Association

[2] The President, Executive Order 13636—Improving Critical Infrastructure Cybersecurity, February 19, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[3] Executive Order 13636, Improving Critical Infrastructure Cybersecurity Sec. 7(b).

With the release of the Cybersecurity Framework Draft Version 1.1, NIST requested answers to the following questions:

Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

- No additional topics should be addressed in Version 1.1. However, the discussion of metrics in the new section "4.0 Measuring and Demonstrating Cybersecurity" could be expanded with the addition of additional practical guidance.

How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

- There is a greater emphasis on supply chain, though unfortunately the focus is largely on compliance-oriented controls. These types of controls may have some value but they often are not preventive. Reference to industry-standard certifications should be considered. For operational technology, there should be a greater recognition of the role of vendor involvement in system design and configuration.
-

For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

- We do not see substantial impact. The added language would provide additional support for third-party security review programs, however, NIST should recognize that under the current way SCRM has been incorporated in the Draft Framework, companies may not be able to identify as "Adaptive" if its suppliers are not SCRM compliant.

For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?

- Many of our members currently use the Framework. We anticipate that following the publication of version 1.1, the changes to the Framework will be reviewed for use by our members.

Does this proposed update adequately reflect advances made in the Roadmap areas?

- No opinion.

Is there a better label than "version 1.1" for this update?

- No opinion.

Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap? Comments:

- The next revision of the Framework should focus on challenges associated with operational technology (as compared to IT) and the emerging Internet of Things (IoT).

Framework for Improving Critical Infrastructure Cybersecurity

Draft Version 1.1

National Institute of Standards and Technology

January 10, 2017

Note to Reviewers on the Update and Next Steps

The draft Version 1.1 of Cybersecurity Framework refines, clarifies, and enhances the predecessor version 1.0.

Version 1.1 can be implemented by first time and current Framework users. Current users can implement Version 1.1 with minimal or no disruption, as refinements were made with the objective of being compatible with Version 1.0.

As with Version 1.0, use of the Version 1.1 is voluntary. Users of Version 1.1 are invited to customize the Framework to maximize organizational value.

The impetus to change and the proposed changes were collected from:

- □ Feedback and frequently asked questions to NIST since release of Framework Version 1.0 in February 2014,
- □ 105 responses to the December 2015 request for information (RFI), *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, and
- □ Comments provided by approximately 800 attendees at a workshop held in Gaithersburg, Maryland on April 6-7, 2016.

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 both private and public sector efforts, some areas of improvement have advanced enough to be included in the Framework Version 1.1.

Key refinements, clarifications, and enhancements in Framework Version 1.1 include:

Update	Description of Update
A new section on cybersecurity –measurement	Added Section 4.0 Measuring and Demonstrating Cybersecurity to discuss correlation of business results to cybersecurity risk management metrics and measures.
Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes	Considerations of Cyber Supply Chain Risk Management (SCRM) have been added throughout the document. An expanded Section 3.3 Communicating Cybersecurity Requirements with Stakeholders has been added to help users better understand –Cyber SCRM. Cyber SCRM has also been added as a property of Implementation Tiers. Finally, a Supply Chain Risk Management Category 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 account for authentication, authorization, and identity proofing. A Subcategory has been added to that Category. Finally, 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 Establishing or Improving a Cybersecurity Program on using Framework Tiers in Framework implementation. Added language to Framework Tiers to reflect integration of Framework considerations within organizational risk management programs. Updated Figure 2.0 to include actions from the Framework Tiers.

Comment [KB2]: Should this say "to help" or "helps" (or even "has been added to help")? It seems grammatically incorrect as currently written.

Comment [KB1]: As added these are less recommendation. The wording may prohibit some companies from attaining their desired tier, due to suppliers inability to comply.

A more detailed review of Version 1.1 refinements, clarifications, and enhancements can be found in Appendix D.

NIST is seeking public comment on this draft Framework Version 1.1, specifically regarding the following questions:

- Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?
- How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?
- For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?
- For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?
- Does this proposed update adequately reflect advances made in the Roadmap areas?
- Is there a better label than "version 1.1" for this update?
- Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

Feedback and comments should be directed to cyberframework@nist.gov. After reviewing public comments regarding the draft Version 1.1 and convening a workshop on the Framework, NIST intends to publish a final Framework Version 1.1 around the fall of 2017.

Table of Contents

List of Figures

List of Tables

Executive Summary

The national and economic security of 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 risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

To better address these risks, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. There are many ways to achieve security and organizations should not be limited in their approach. This Framework recognizes that there are existing standards and regulations, as well as other voluntary frameworks for critical infrastructure sectors to use for cybersecurity risk management.

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 Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business 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.

The Executive Order also requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. While processes and existing needs will differ, the Framework can assist organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program.

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 the security and resilience of critical infrastructure. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. This Framework recognizes that innovation by cyber adversaries is dynamic, and defending against them requires organizations to react constantly. As a static document, the Framework cannot be expected to provide full protection from those adversaries. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. 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.

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 industry as directed in the Cybersecurity Enhancement Act of 2014[1]. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Use, evolution, and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing guidance for individual organizations, while increasing the cybersecurity posture of the Nation's critical infrastructure as a whole.

Formatted: Character scale: 105%

Comment [KB3]: Coordinating **with** industry

Deleted: is

Comment [KB4]: What defines the term "best practices"? Is this based from other industries, an aggregation of a given industry collectively, or based on federal recommendations of securing our infrastructures?

[1] *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.

1.0 Framework Introduction

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity," on February 12, 2013.[2] This Executive Order calls for the development of a voluntary Cybersecurity Framework ("Framework") that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk.

Critical infrastructure is defined in the EO 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 information technology (IT) and industrial control systems (ICS).[3] This reliance on technology, communication, and the interconnectivity of IT and ICS has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as ICS and the data produced in ICS operations are increasingly used to deliver critical services and support business decisions, the potential impacts of a cybersecurity incident on an organization's business, assets, health and safety of individuals, and the environment should be considered. To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of IT and ICS is required. Because each organization's risk is unique, along with its use of IT and ICS, 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 Executive Order requires that the Framework include 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.

[2] 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

[3] The 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

To ensure extensibility and enable technical innovation, the Framework is technology neutral. The Framework relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience. 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 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.

Just as the Framework is not industry-specific, 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 1Overview 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 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 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 drivers and a risk assessment, determine which are most important; they 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 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 resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services 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[4], ISO/IEC 27005:2011[5], National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39[6], and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline[7].

1.3 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 Framework for cybersecurity measurement.
- 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.
- Appendix D is a detailed listing of updates between the Framework Version 1.0 and 1.1.

[4] International Organization for Standardization, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[5] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. http://www.iso.org/iso/catalogue_detail?csnumber=56742

[6] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[7] 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

2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. 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 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 industry as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in **Figure 1**:

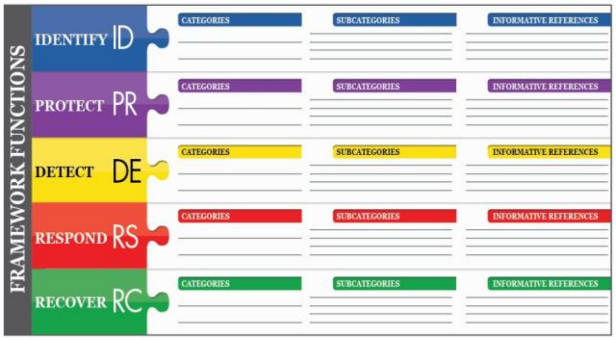

Figure 1: Framework Core Structure

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," "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.[8]

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 can 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 the organizational understanding to manage cybersecurity risk to systems, 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 the appropriate safeguards to ensure delivery of critical infrastructure 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: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement the 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.

[8] NIST developed a Compendium of informative references gathered from the Request for Information (RFI) input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process. The Compendium includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on initial stakeholder input. The Compendium and other supporting material can be found at http://www.nist.gov/cyberframework/.

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

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

- **Recover** – 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.

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

2.2 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. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and 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, cyber supply chain risk management needs, 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), 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. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective. Successful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier determination. However, Tier selection and designation naturally affect Framework Profiles. The risk disposition expressed in a desired Tier should influence prioritization within a Target Profile. Similarly, the organizational state represented in an assessed Tier will indicate the likely findings of an assessed Profile, as well as inform realistic progress in addressing Profile gaps.

Comment [KB5]: The use of independent audit/assessment of risk should be explicitly included in the appropriate tier(s).

Comment [KB6]: A company that has adopted the CSF may not be able to identify as Adaptive if its suppliers are not SCRM compliant as specified. The language should be eased to allow companies to consider the controls rather using a Thou Shalt approach.

Comment [KB7]: The addition could be interpreted in a contradictory manner: not considering program maturity in tier selection but then again, actually considering maturity when a tier is selected. The logic seems circular and, if it was intended to clarify the use of tiers, framework profiles, and target profiles, it did not succeed.

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* – An organization may not have the processes in place to participate in coordination or collaboration with other entities.
- *Cyber Supply Chain Risk Management* – An organization may not understand the full implications of cyber supply chain risks nor have the processes in place to identify, assess and mitigate its cyber supply chain risks.

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 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 mission/business objectives may occur at some levels of the organization, but not at all levels. Cyber risk assessment of organizational assets is not typically repeatable or reoccurring.
- *External Participation* – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.
- *Cyber Supply Chain Risk Management* – The organization understands the cyber supply chain risks associated with the products and services that either supports the business mission function of the organization or that are utilized in the organization's products or services. The organization has not formalized its capabilities to manage cyber supply chain risks internally or with its suppliers and partners and performs these activities inconsistently.

Comment [KB8]: wording of the bullet on *Cyber Supply Chain Risk Management* should be synchronized with the second bullet, specifically, "Consideration of cybersecurity in mission/business objectives may occur at some levels of the organization, but not at all levels. Cyber risk assessment of organizational assets is not typically repeatable or reoccurring."

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 dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.
- *Cyber Supply Chain Risk Management* – An organization-wide approach to managing cyber supply chain risks is enacted via enterprise risk management policies, processes and procedures. This ~~likely~~ should include~~s~~ a governance structure (e.g. Risk Council) that manages cyber supply chain risks in balance with other enterprise risks. Policies, processes, and procedures are implemented consistently, as intended, and continuously monitored and reviewed. Personnel possess the knowledge and skills to perform their appointed cyber supply chain risk management responsibilities. The organization has formal agreements in place to communicate baseline requirements to its suppliers and partners.

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- *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. This approach is consistent with an overall corporate management program that includes appropriate stakeholder engagement and avoids redundancy. The relationship between cybersecurity risk and mission/business 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 understanding of current and predicted risk environment and future risk appetites. Business units implement executive vision and analyze system level risks in the context of the organizational risk appetite and tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other

Comment [KB9]: *Integrated Risk Management Program*: "The organization consistently and accurately monitors cybersecurity risk of organizational assets." The term "organizational assets" should be defined. Also - "Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk." With whom are they communicating? (In other words, an object is called for but is not present.)

Comment [KB10]: Hard to understand what is being said given that it's not focused on other risk management

Comment [KB11]: Prioritization should be predicated on criticality – not every acquisition brings the same set of risk governance structures that set up the risk value equation. Not every acquisition needs the same level of risk management.

Comment [KB12]: *Integrated Risk Management Program:* "The organizational budget is based on understanding of current and predicted risk environment and future risk appetites. Business units implement executive vision and analyze system level risks in the context of the organizational risk appetite and tolerances." These statements imply that a risk appetite has been defined at this tier. The document should define the concept, expand on it, and more clearly call for it to be done. In particular, the document should address possibilities for **who defines the risk appetite.** Risk appetite should be defined at the level appropriate within the organization.

Comment [KB13]: Suggest to remove all document references to "risk appetite" and replace with "risk tolerance" as defined in NIST Special Publication 800-39.

sources, and continuous awareness of activities on their systems and networks. Cybersecurity risk is ~~clearly~~ articulated and understood across all strata of the enterprise. The organization can quickly and efficiently account for changes to business/mission objectives and threat and technology landscapes in how risk is communicated and approached.

- *External Participation* – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.
- *Cyber Supply Chain Risk Management* – The organization can quickly and efficiently account for emerging cyber supply chain risks using real-time or near real-time information and leveraging an institutionalized knowledge of cyber supply chain risk management with its external suppliers and partners as well as internally, in related functional areas ~~and at all levels of the organization.~~ The organization communicates proactively and uses formal (e.g. agreements) and informal mechanisms to develop and maintain strong relationships with its suppliers, partners, and individual and organizational buyers.

2.3 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 the communication of risk within and between organizations. This Framework document 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 can contribute to the roadmap described above. Prioritization of gap mitigation is driven by the organization’s business needs and risk management processes. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner.

Comment [KB14]: Remove the word “clearly” as it is too vague and undefined.

Comment [KB15]: *Cyber Supply Chain Risk Management:* "The organization can quickly and efficiently account for emerging cyber supply chain risks using real-time or near real-time information and leveraging an institutionalized knowledge of cyber supply chain risk management with its external suppliers and partners as well as internally, in related functional areas and at all levels of the organization." This criterion feels aspirational, given the present state of technology and relationships between suppliers and buyers, wherein buyers should, in theory, have the upper hand but, in reality, suppliers often are dictating agreement terms (for a variety of reasons). The need for supplier cooperation needs to be explicitly stated as an expectation.

Comment [KB16]: The new controls do not support this. The new controls clearly prescribe behaviors (contracts, audits, reviewing R&R plans...) and do not speak to informal mechanisms.

2.4 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.

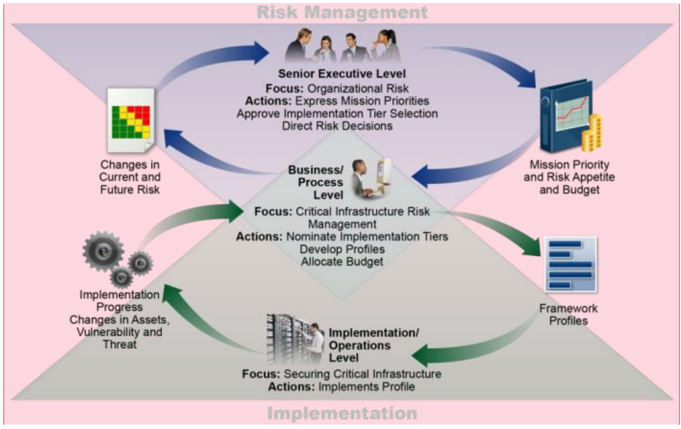
Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Figure 2: Notional Information and Decision Flows within an Organization

Comment [A1]: Note addition of Implementation Tiers to the Actions in the figure.

3.0 How to Use the Framework

Comment [KB17]: Recommend including a version of this paragraph earlier, such as in the executive summary or introduction.

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. Utilizing 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 in design, build/buy, deploy, operate, and decommission system lifecycle phases. The design phase should account for cybersecurity requirements as a part of a larger multi-disciplinary systems engineering process[9]. A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as summarized in a Framework Profile. The cybersecurity outcomes prioritized in a Profile should be enacted during either a) development of the system during the build phase or b) purchase or outsourcing of the system during the buy phase. In the system deploy phase, the cybersecurity features of the system should be assessed to verify the design was enacted. The cybersecurity outcomes of the Framework then serve as a basis for on-going operation of the system, including occasional reassessment to verify that cybersecurity requirements are still fulfilled. Typically, a complex web of dependencies amongst systems means Framework outcomes should be carefully considered as one or more systems are decommissioned.

Comment [KB18]: This should be separate. Building means defining and initiating from scratch. Buying means purchasing something that has already been built, generally from an outside vendor or party.

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

3.1 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 outcomes, thus managing cybersecurity commensurate with the known risk. Conversely, 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

[9] NIST Special Publication 800-160: *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, November 2016, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

certain outcomes. The organization can use this information to reprioritize resources to strengthen other cybersecurity practices.

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 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. Implementation Tiers may be used to express varying risk tolerances.

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.

Deleted: identifies threats to, and vulnerabilities of, those systems and assets.

Comment [KB19]: *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." Seems innocuous but indirect - could be described more plainly. (Same comment at step 4, conducting a risk assessment.)

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.

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. When used in conjunction with an

Implementation Tier, characteristics of the Tier level should be reflected in the desired cybersecurity outcomes.

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 those gaps, - drawing upon mission drivers, a cost/benefit analysis, and risk understanding - to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Deleted: that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile

Step 7: Implement Action Plan. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against 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 may repeat 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 utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.

3.3 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 services. Examples include:

- An organization may utilize 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.

In addition, Implementation Tiers allow organizations to understand how they fit into the larger cybersecurity ecosystem. Organizations can better manage~~r~~ cybersecurity risk among~~st~~ stakeholders by assessing their position in both critical infrastructure and the broader digital economy.

Comment [KB20]: Typo (should be “manage”, not “manager”) in red, word choice in blue: "Organizations can better manager cybersecurity risk amongst stakeholders by assessing their position in both critical infrastructure and the broader digital economy." Say "among" rather than "amongst".

The practice of communicating and verifying cybersecurity requirements among stakeholders is one aspect of cyber supply chain risk management (SCRM). 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.”[10] ~~.”~~ Cyber SCRM activities may include:

- Determining cybersecurity requirements for suppliers and information technology (IT) and operational technology (OT) partners,
- Enacting cybersecurity requirements through formal agreement (e.g. contracts),
- Communicating to suppliers and partners how those cybersecurity requirements will be verified and validated,
- Verify 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 IT and OT suppliers and buyers as well as non-IT and OT partners. These relationships highlight the critical role of cyber SCRM in addressing cybersecurity risk in the critical infrastructure and the broader digital economy. They should be identified and factored into the protective and detective capabilities of organizations, as well as the response and recovery protocols of organizations.

Formatted: Font:(Default) +Theme Headings CS (Times New Roman), Complex Script Font: +Theme Headings CS (Times New Roman)

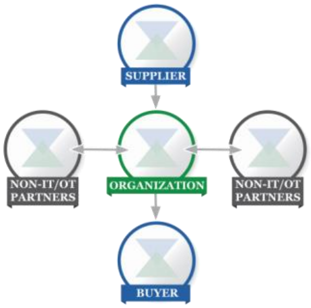

Figure 3: Cyber Supply Chain Relationship

Comment [KB21]: It should be noted that the supplier has a very critical role because its cooperation is essential. Are the suppliers/buyers assumed IT/OT? And why differentiate the Non-IT/OT partners?

Buyer refers to the people or organizations that consume a given product or service from an organization. Suppliers encompass 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. Finally, non-IT and OT partners have access to, or may otherwise be a risk to, the security posture of the organization.

[10] NIST Special Publication 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Whether considering individual Subcategories of the Core, or the comprehensive considerations of a Profile, the Framework offers organizations and their partners a method of ensuring the new product or service meets security outcomes that are prioritized. By first selecting outcomes that are relevant to the context (PII transmission, mission critical service delivery, data verification services, product or service integrity, etc.) the organization can then evaluate partners against those criteria. For example, if a particular system is being purchased that will monitor OT, availability may be a particularly important cybersecurity objective to achieve and thus will drive Subcategory selection (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, etc.).

Comment [KB22]: This section is not the appropriate context for this paragraph, which assumes that robust, widely observed processes are present.

3.4 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 cyber SCRM (Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier. Instead, the objective is to make the best buying decision, optimally between multiple suppliers, given a pre-decided list of cybersecurity requirements. Often, this means some degree of trade-off analysis. Therefore, a product or service is typically purchased with known gaps to the Target Profile.

Once a product or service is purchased, the Profile also ~~can~~ may be used to track 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 incorporate that residual cybersecurity risk into the overall risk management of the larger environment, addressing the residual risk through other management actions. The Profile also allows the organization a method for assuring that the product meets cybersecurity outcomes through periodic review and testing mechanisms.

The organization also recognizes that products and services may include periodic or persistent remote access by the product supplier and/or integration firms. This remote access should be periodically reviewed and assessed with a cybersecurity focus regarding who from the supplier or integrator is able to connect remotely and what are they able to access. Review of the cybersecurity controls of the supplier and/or integrator company are necessary to ensure compromise of their systems does not become an attack vector to the purchasing organization.

3.5 5 Identifying Opportunities for New or Revised Informative References

Deleted: 4

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 6 Methodology to Protect Privacy and Civil Liberties

Deleted: 5

This section describes a methodology as required by the Executive Order to address individual privacy and civil liberties implications that may result from cybersecurity operations. 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 may give rise to these considerations. Consistent with Section 3.4, technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and cybersecurity have a strong nexus. It is well-recognized that cybersecurity plays an important role in protecting individuals' privacy; for example, with respect to the confidentiality of assets containing personal information. Nonetheless, an organization's cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities. Some examples of activities that bear privacy or civil liberties considerations may 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; cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including activities such as some types of incident detection or monitoring that may impact freedom of expression or association.

Deleted: and civil liberties implications may arise

The government and agents of the government have a direct responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or agents of the government 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, in circumstances where such measures are appropriate, 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 foregoing organizational measures and controls

Approaches to identifying and authorizing individuals to access organizational assets and systems

- Steps are taken to identify and address the privacy implications of 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

3.7 7 Federal Alignment

~~For Federal information systems, including those systems that are part of the critical infrastructure,~~ Federal agencies are required to fulfill the security requirements defined in the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) policies, and NIST standards and guidelines as expressed in Federal Information Processing Standards and Special Publications. The Cybersecurity Framework complements existing federal risk management approaches. Federal agencies may find the Framework a valuable addition by using:

- □ Implementation Tiers to express risk disposition,
- □ The Core to organize and communicate cybersecurity concepts, activities, and outcomes
- □ Profiles to inform prioritization decisions, and
- □ The Seven-Step Process to organize assessment and remediation activities.

Additionally, OMB has organized recent FISMA reporting[11] and improvement initiatives (e.g., Cybersecurity Strategy and Implementation Plan[12]) according to Framework Functions. Federal organizations may find value in gaining a working understanding of the Framework Core to ensure precise and efficient high-level cybersecurity dialog with Federal and non-Federal partners.

[11] OMB Memorandum M-16-03, *FY 2015-16 Guidance on Federal Information Security and Privacy Management Requirements*, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

[12] OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan*, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

4.0 Measuring and Demonstrating Cybersecurity

It can be challenging to apply security metrics to certain performance aspects of the Framework. Although the Framework aims to enumerate differences in maturity levels within an organization, the actual metrics and measurements may be less precise than desired. However, Framework measurement as a baseline resource provides a basis for strong trusted relationships, both inside and outside of an organization. Measuring state and trends over time, internally, through external audit, and through conformity assessment, enables an organization to understand and convey meaningful risk information to dependents, partners, and customers.

In combination with Informative References, the Framework can be used as the basis for comprehensive measurement. The key terms for measuring with Framework are "metrics" and "measures.[13]" Metrics are used to "facilitate decision making and improve performance and accountability." The Implementation Tiers, Subcategories, and Categories are examples of metrics. Metrics create meaning and awareness of organizational security postures by aggregating and correlating measures. Measures are "quantifiable, observable, objective data supporting metrics." Measures are most closely aligned with technical controls, such as the Informative References.

The information harvested from security metrics is indicative of different aspects of organizational cyber risk posture. As such, tracking both security metrics and business outcomes may provide meaningful insight as to how changes in granular security controls impact the completion of business objectives. While it is important to measure whether or not a business objective was achieved through lagging measurement, it is typically more important to understand the likelihood of achieving a future objective through a leading measurement.

The ability of an organization to determine cause-and-effect relationships between cybersecurity and business outcomes is dependent on the accuracy and precision of the measurement systems (i.e., composed of the "resources" highlighted in ID.AM-5). Therefore, the measurement system should be designed with business requirements and operating expense in mind. The expense of a measurement system may increase as the accuracy of measurement increases. To mitigate undue cost to the organization, the accuracy and expense of a system need only match the required measurement accuracy of the corresponding business objective.

4.1 Correlation to Business Results

The objective of measuring cybersecurity is to correlate cybersecurity with business objectives (ID.BE-3), to understand and quantify cause-and-effect. Common business objectives include driving business/mission results, increasing cost effectiveness, and reducing enterprise risk. The aggregate of these business objectives may be measured in earnings per share and price/earnings multiple at the board level: revenue and net profits by senior executives; and in more specific measures such as number of products or hours delivered by those that report to senior executives.

Correlating cybersecurity metrics to business objectives is often more complex than simply measuring one cybersecurity result. There are a large number and variety of contributing factors to a given business objective. For instance, a retail bank wanting to increase the number of on-line banking customers may seek to do so by implementing stronger authentication. However, achieving an increase in on-line banking customers is also contingent upon developing the messages regarding trusted on-line transactions, targeting specific demographics of consumers,

[13] *Cybersecuritry Metrics and Measures*, Black et al, March 2009, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51292

Comment [KB23]: Section 4.0, *Measuring and Demonstrating Cybersecurity* - The section works well to establish definitions, particularly in differentiating between metrics and measures. In practice, though, the difference seems fuzzy. Metrics can be a very difficult topic when applied to cybersecurity. Even though a good effort is made on p. 23 to further clarify use cases for metrics and measures, it feels like the bottom line is that metrics are general in nature while measures are technical - and this may not have been the intent of the authors of this section.

Comment [KB24]: Suggest to remove "lagging measurement" and replace with more clear terminology selecting communication channels that are most meaningful to those demographics, and marketing those communication channels over a duration necessary to achieve the objective. In short, achieving customer growth is contingent on messaging, marketing, advertising cybersecurity, and other factors.

The relative cost effectiveness of various cybersecurity activities is an important consideration. Cost effectiveness means achieving a given business objective using minimum cybersecurity effort and expense. To examine cost effectiveness, an organization must first have a clear understanding of the business objectives, an understanding of the relationship between business objectives and the cybersecurity metrics, and an understanding of the relationship between business objectives and non-cybersecurity factors.

The effect of cybersecurity outcomes on a business objective may often be unclear. Cybersecurity's primary role is the preservation of the businesses value through the protection of the confidentiality, integrity, and availability (CIA) of the organization's information, operations, and processes. As such, even when cost effectiveness or the effect of cybersecurity outcomes on a business objective ~~are~~ is unclear, organizations should exercise prudence when modifying their cybersecurity program. Often, cybersecurity outcomes cannot be accurately measured, such as the prevention of ~~are preventing a bad~~ negative business circumstances, ~~like~~ such as ~~a~~ data breaches.

Enterprise risk management is the consideration of all risks to achieving a given business objective. Ensuring cybersecurity is factored into enterprise risk consideration is integral to achieving business objectives. This includes the positive effects of cybersecurity as well as the negative effects should cybersecurity be subverted. The Management metrics highlighted below are a way of aggregating cybersecurity risk using the Framework Core, enabling cybersecurity to ~~can~~ be factored into enterprise risk management.

The ability of an organization to determine cause-and-effect relationships between cybersecurity outcomes and business objectives also depends on the ability to adequately isolate those cybersecurity outcomes and business objectives. This is one of the largest challenges affecting measurement of cybersecurity. Ideally, ~~Special care must be taken to ensure that a given~~ cybersecurity outcomes and business objectives truly correlate, however they may not appear to upon initial consideration, or at all. Generally, correlating cybersecurity measures to higher-level cybersecurity metrics is easier than correlating cybersecurity metrics to business metrics.

Comment [KB25]: Speculative language. Compliance does not equal security and vice versa. Remove sentence, or use suggested clarifying statement.

Comment [KB26]: Something isn't right here. Do they mean "ensuring" instead of "enabling"? Or should it be "enabling cybersecurity *to* be factored into …"?

4.2 Types of Cybersecurity Measurement

A summary of metrics and measures relating to the Framework is displayed in Table 1.

Table 1: Types of Framework Measurement

Measurement	What is Measured	Corresponding Framework Component	Measurement Type
Practices	General risk management behaviors	Implementation Tiers	Metric
Process	Specific risk management activities	Prose of Framework including the Seven-Step Process (Section 3.2) and use case specific process (e.g., Section 3.3 & 3.6)	Measure
Management	Fulfillment of general cybersecurity outcomes	Core/Profile Functions, Categories, and Subcategories	Metric
Technical	Achievement of specific cybersecurity outcomes	Informative References	Measure

Framework Implementation Tiers are a qualitative metric of overall cybersecurity risk management practices. Beyond an overarching 1 – 4 qualitative metric, the individual Implementation Tier properties of Risk Management Process, Integrated Risk Management Program, External Participation, and Cyber Supply Chain Risk Management also comprise practice metrics.

Whereas practices such as those in Implementation Tiers are general trends in high-level organizational behavior, those practices are composed of ~~discrete~~ processes that represent specific risk management activities. For instance, the periodicity of a process for updating Framework Profiles (Step 3) is a measure that is reflected in the metric, Risk Management Process. Similarly, a measure of the extent that governance and risk management processes address cybersecurity risk (ID.GV-4) is reflected in the metric, Integrated Risk Management Program. Finally, the volume of threat and vulnerability information received from information sharing forums and sources (ID.RA-2) is reflected in the metric, External Participation.

Comment [KB27]: Suggest to remove “discrete.”

The cybersecurity outcomes of the Framework Core are the basis for a comprehensive set of cybersecurity management metrics. The evaluation ~~aggregate~~ of these metrics may assist organizations in more clearly identifying and providing understanding of ~~equals a reduction (or not) of~~ the organization's cybersecurity risk.

□ For instance, the outcome of the Protect Function is to "develop and implement the appropriate safeguards to *ensure delivery*…" A Senior executive held accountable to this outcome might be measured using a lagging metric of percentage uptime of system(s) (i.e. ensuring delivery), with a leading metric of creating and communicating *strategy* for development and implementation for data security.

□ Correspondingly, a Business Process person might be held accountable to the Data Security Category of the Protect Function (PR.DS) and Subcategories thereof. Data Security reads "information and records (data) are managed consistent with the organization's risk strategy to protect the CIA of information." A Business Process person accountable for all Data Security could be measured using the leading metric of whether *policies* are published and communicated commensurate with both the organizations risk strategy and the goals of CIA. Lagging metrics for this Business Process person might be a composite of lagging metrics of how CIA is managed by those responsible for the Data Security Subcategories.

□ Similarly, the Implementation/Operations person accountable for protecting data-at-rest (PR.DS-1) might be measured on the leading metric of implementing protective mechanisms, with the lagging metric being whether data was protected as evidenced by the lack of unauthorized modification, deletion, or theft of organizational data. That Implementation/Operations person might fulfill the objective of PR.DS-1 using applicable Informative References and corresponding measures.

Informative References, such as controls catalogs, offer detailed technical measures that work modularly to complement Framework. For instance, an organization using the NIST Special Publication 800-53[14] security control SP-28 to implement the PR.DS-1 Subcategory might be held accountable to measures of design, development/purchase, implementation, management, evolution, and sunset of:

□ Cryptographic mechanisms across a variety of media storage (internally-hosted hard drives, cloud hard drives, portable storage devices, mobile devices)

□ Full disk encryption versus specific data structures (e.g., files, records, or fields),

□ File share scanning,

□ Write-Once-Read-Many technologies, and

□ Secure off-line storage in lieu of online storage.

Comment [KB28]: Recommend to strike, the lagging metric requires proving a negative.

Comment [KB29]: Recommend to strike. Risk management frameworks will ideally help organizations to consider and manage risk going forward. Some of these examples may not be helpful due to changes in secure technology and could materially change in the near term, becoming outdated.

[14] NIST Special Publication 800-53 Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations*, Joint Task Force Transformation Initiative Interagency Working Group, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

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 relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.

Table 2: Function and Category Unique Identifiers

Deleted: 1

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	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

Table 3: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** 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 business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

Deleted: 2

Comment [KB30]: ID.AM-5 – what does time refer to?

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): 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.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	• **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 • **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **CSC(V6)** 19.2 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7

Deleted: 1

Function	Category	Subcategory	Informative References
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7 • **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 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 • **NIST SP 800-53 Rev. 4** PM-9, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber and other threat intelligence vulnerability information is received from information sharing forums and sources	• **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	• **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1

Deleted: Threat and vulnerability information

Function	Category	Subcategory	Informative References
		determine risk	• **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	• **COBIT 5** APO12.05, APO13.02 • CSC(V6) 4.8 • **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	• **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply in place the processes to identify, ~~assess and manage supply chain~~ risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	• **CIS CSC:** 4.8 • **COBIT 5:** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009**: 4.3.4.2 • **ISA 62443-3-3:2013:** • ~~**ISO/IEC 27001:2013:**~~ A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
		ID.SC-2: ~~Identify, prioritize and assess~~ ~~s~~Suppliers and partners of critical information systems, components and services are identified, prioritized, and assessed using a cyber supply chain risk	□ **CIS CSC:** • **COBIT 5:** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02,

Comment [KB31]: The "Subcategory" language describing ID.SC-2 should be written in passive voice, if possible (I have proposed one option), in order to match the structure of the rest of the framework.

Function	Category	Subcategory	Informative References
		assessment process	BAI02.03 • **ISA 62443-2-1:2009:** 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 • **ISA 62443-3-3:2013:** • **ISO/IEC 27001:2013:** A.15.2.1, A.15.2.2 • **NIST SP 800-53**: RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.	□ **•CIS CSC:** • **COBIT 5:** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009:** 4.3.2.6.4, 4.3.2.6.7 • **ISA 62443-3-3:2013:** • **ISO/IEC 27001:2013:** A.15.1.1, A.15.1.2, A.15.1.3 • **NIST SP 800-53:** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted	□ **CIS CSC:** • **COBIT 5:** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 • **ISA 62443-2-1:2009:** 4.3.2.6.7 • **ISA 62443-3-3:2013:** SR 6.1 • **ISO/IEC 27001:2013:** A.15.2.1, A.15.2.2 • **NIST SP 800-53**: AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers	• **CIS CSC:** 19.7, 20.3 • **COBIT 5:** DSS04.04 • **ISA 62443-2-1:2009:** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013:** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53**: CP-2, CP-4, IR-3, IR-4, IR-6,

Comment [KB32]: Too prescriptive. Remove “required.” This is a voluntary adoption and should not be read as regulation.

Consider something like this: Suppliers and partners may consider contractually obligating the other party to implement...

Comment [KB33]: Too prescriptive. Consider the following: Suppliers and partners may arrange to monitor the other party to confirm...

Remove “required.” This is a voluntary adoption and should not be read as regulation.

Comment [KB34]: May prevent smaller companies from achieving the desired tier as worded. Consider the following: Suppliers and partners verify each other's response and recovery plans.

Function	Category	Subcategory	Informative References
			IR-8, IR-9
PROTECT (PR)	**Identity Management and Access Control (PR.AC):** 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.	**PR.AC-1:** Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	• **CCS CSC** 12, 15 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3,

Deleted: managed

Deleted: and

Deleted: associated

Deleted: or

Deleted: to authorized activities and transactions.

Function	Category	Subcategory	Informative References
			A.13.2.1 - **NIST SP 800-53 Rev. 4** AC-4, SC-7
		PR.AC-6: Identities are ~~proofed~~ verified, with a one-to-one relationship ~~and bound~~ to credentials, and ~~asserted~~ are provided in interactions where~~n~~ it is appropriate to require proof of identify	- **CIS CSC: CSC 5, 12, 14, 16** - **COBIT 5: DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03** - **ISA 62443-2-1:2009: 4.3.2.4.2, 4.3.3.2.2, 4.3.3.2.3, 4.3.3.5.2, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4** - **ISA 62443-3-3:2013: SR 1.4, SR 1.5, SR 2.1, SR 2.2, SR 2.3** - **ISO/IEC 27001:2013: A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4** - **NIST SP 800-53: AC-2, AC-3, AC-5, AC-6, AC-16, AC-19, AC-24, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3**
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	- **CCS CSC** 9 - **COBIT 5** APO07.03, BAI05.07 - **ISA 62443-2-1:2009** 4.3.2.4.2 - **ISO/IEC 27001:2013** A.7.2.2 - **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	- **CCS CSC** 9 - **COBIT 5** APO07.02, DSS06.03 - **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 - **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 - **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	- **CCS CSC** 9 - **COBIT 5** APO07.03, APO10.04, APO10.05 - **ISA 62443-2-1:2009** 4.3.2.4.2 - **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 - **NIST SP 800-53 Rev. 4** PS-7, SA-9
		PR.AT-4: Senior executives understand	- **CCS CSC** 9

Comment [KB35]: PR.AC-6, - "Identities are proofed and bound to credentials, and asserted in interactions when appropriate" - This wording is not clear. Possible suggestion: "Identities are verified, with a one-to-one relationship to credentials, and are provided in interactions where it is appropriate to require proof of identity."

Function	Category	Subcategory	Informative References
		roles & responsibilities	• **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13
	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.	**PR.DS-1:** Data-at-rest is protected	• **CCS CSC** 17 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Rev. 4** SC-28
		PR.DS-2: Data-in-transit is protected	• **CCS CSC** 17 • **COBIT 5** APO01.06, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SC-8
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2

Function	Category	Subcategory	Informative References
			• **ISO/IEC 27001:2013** A.12.3.1 • **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** 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.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	□ **CIS CSC: CSC 3.3** • **COBIT 5: BAI03.05.4** • **ISA 62443-2-1:2009: 4.3.4.4.4** • **ISA 62443-3-3:2013:** • **ISO/IEC 27001:2013: A.11.2.4** • **NIST SP 800-53: SA-10, SI-7**
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities),	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)	• **CCS CSC** 3, 10 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1,

Comment [KB36]: Too prescriptive. Consider the following: Hardware integrity validation is considered through configuration or through a checking mechanism.

Deleted: , separation of duties

Function	Category	Subcategory	Informative References
	processes, and procedures are maintained and used to manage protection of information systems and assets.		A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	• **COBIT 5** BAI06.01, BAI01.06 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 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 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2

Function	Category	Subcategory	Informative References
			• **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Protection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 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 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10: Response and recovery plans are tested	• **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4,

Function	Category	Subcategory	Informative References
	system components is performed consistent with policies and procedures.	and controlled tools	A.11.2.5 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 • **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **CCS CSC** 14 • **COBIT 5** APO11.04 • **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 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	• **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	• **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 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 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3,

Deleted: Access to systems and assets is controlled, incorporating the principle of least functionality

Comment [KB37]: This re-wording of makes it sound like a rehash of PR.IP-1 (i.e., secure baseline configuration). Securely configuring systems is not really a "Protective Technology" per se. The original language, or some variant thereof ("controlling access", as opposed to secure configuration) seems more appropriate for a "Protective *Technology*", IMO.

Function	Category	Subcategory	Informative References
			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 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	• **CCS CSC** 7 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** 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 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
		PR.PT-5: Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations).	□ **CIS CSC:** • **COBIT 5: BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05** • **ISA 62443-2-1:2009: 4.3.2.5.2** • **ISA 62443-3-3:2013: SR 7.1, SR 7.2** • **ISO/IEC 27001:2013: A.17.1.2, A.17.2.1** • **NIST SP 800-53: CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and	• **ISA 62443-3-3:2013** SR 6.1

Comment [KB38]: I'm not quite sure how this fits in the "Protective Technology" section, as currently worded. Not sure where else it would belong, though. Perhaps it would help to somehow reference there being some 'technology' involved? Maybe add language at the start to say "Failsafe protections exist that enable systems to operate in pre-defined functional states …." (in which case the "failsafe protections" would represent the "Protective Technology" in question).

Function	Category	Subcategory	Informative References
		correlated from multiple sources and sensors	• **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	• **ISA 62443-2-1:2009** 4.3.3.3.8 • **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1 • **NIST SP 800-53 Rev. 4** SI-3
		DE.CM-5: Unauthorized mobile code is detected	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44

Function	Category	Subcategory	Informative References
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• **COBIT 5** APO07.06 • **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7,

Function	Category	Subcategory	Informative References
			RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• **COBIT 5** DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

Function	Category	Subcategory	Informative References
		RS.AN-2: The impact of the incident is understood	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	• **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Incidents are mitigated	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets	**RC.RP-1:** Recovery plan is executed during or after an event	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8

Function	Category	Subcategory	Informative References
🟩	affected by cybersecurity events.		
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	• **COBIT 5** EDM03.02
		RC.CO-2: Reputation after an event is repaired	• **COBIT 5** MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	• **NIST SP 800-53 Rev. 4** CP-2, IR-4

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
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
- 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*: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- 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 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Deleted: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243

Deleted: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420

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

Appendix B: Glossary

This appendix defines selected terms used in the publication.

Buyer The people or organizations that consume a given product or service

Category The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."

Critical Infrastructure 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.

Cybersecurity The process of protecting information by preventing, detecting, and responding to attacks.

Cybersecurity Event A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

Detect (function) Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Framework 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."

Framework Core 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.

Framework Implementation Tier 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.

Framework Profile A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.

Function 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,

Comment [KB39]: Terms used in the document that need to be defined:

- **Organizational asset**
- **Risk tolerance**

Comment [KB40]: Term build/buy was used earlier in the document. Suggest to include a definition for "builder" since "buyer" is included in the glossary.

Protect, Detect, Respond, and Recover.

Identify (function) Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Informative Reference 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.

Lagging Measurement A measurement of whether an outcome was fulfilled or not. Since this measure is taken after an outcome is achieved, it cannot be used to guide fulfillment of that outcome.

Leading Measurement A predictive measurement of whether an outcome is likely or not to be achieved. It may guide future activities to ensure a specific outcome is achieved.

Measures Quantifiable, observable, objective data supporting Metrics. Typically, Measures align with technical controls, such as the Informative References.

Metrics Used to facilitate decision making and improve performance and accountability. Typically, Metrics are higher level, qualitative, and an aggregate of several Measures.

Mobile Code 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.

Non-IT/OT Partner Product or service providers that do not provide IT or OT to a given organization, but who do affect the security of that organization

Operational Technology The collection of systems, control and instrumentation equipment, and networks specifically designed to maintain industrial-based operations. OT provides a supporting role for managing computing resources for ICS.

Organizational Asset All assets, human and non-human, that an organization has available to fulfill its mission, objectives, and goals.

Protect (function) Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Privileged User A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Recover (function) 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.

Respond (function) Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Risk 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

Comment [KB41]: Should be "achieved", I think (the 'd' is missing).

Comment [KB42]: "Non-IT/OT Partner" - Essentially this is intended to encompass all service providers that do not involve technology but that still have an impact on organizational security (just cybersecurity or security in general?). The negative phrasing sounds odd but may be unavoidable. It might be advisable to define a hierarchy of suppliers and define them accordingly:

- Partner
  - Technology Partner
    - IT Partner
    - OT Partner
  - Other Partner

(includes providers of service other than technology)

Formatted: Space Before: 0 pt

Formatted: Font: Not Bold

Formatted: Space Before: 0 pt

Formatted: Font: Not Bold

Formatted: Font: Not Bold

impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Management The process of identifying, assessing, and responding to risk.

Risk Tolerance Risk tolerance is the level of risk that organizations are willing to accept in pursuit of strategic goals and objectives.

Subcategory 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."

Supplier 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

Formatted: Font: Not Bold

Comment [KB43]: As defined in NIST Special Publication 800-39: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Comment [KB44]: More definition around what constitutes a "supplier," lots of activities can be bundled into the term. Is the intent primarily critical services (risk based) or everything including mundane business services?

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

CCS	Council on CyberSecurity
CIA	Confidentiality, Integrity, and Availability
COBIT	Control Objectives for Information and Related Technology
CPS	Cyber-Physical Systems
DCS	Distributed Control System
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PII	Personally Identifiable Information
RFI	Request for Information
RMP	Risk Management Process
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SP	Special Publication

Appendix D: Errata

Changes to Framework version 1.0 incorporated into NIST Cybersecurity Framework Version 1.1 are displayed in Table 4.

Table 4: Changes in Framework Version 1.1

PAGE(S)	**CHANGE**
N/A	Framework version and release date were updated on the title page and in the header/footer
N/A	Table of Contents was modified to reflect the all changes relative to this update
p. 6	Section 1.3 'Document Overview' was modified to reflect the additional section and appendix added with this update
p. 7	Figure 1: 'Framework Core Structure' was added
p. 9	Section 2.2 'Framework Implementation Tiers' - Paragraph 2 was modified to read: "The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, ***information sharing practices,*** business/mission objectives, ***cyber supply chain risk management needs,*** and organizational constraints. Organizations should determine… "
p. 9	Section 2.2 'Framework Implementation Tiers' - Paragraph 3 was modified to include: "*However, Tier selection and designation naturally affect Framework Profiles. The risk disposition expressed in a desired Tier should influence prioritization within a Target Profile. Similarly, the organizational state represented in an assessed Tier will indicate the likely findings of an assessed Profile, as well as inform realistic progress in addressing Profile gaps.*"
pp. 10-12	Section 2.2 'Framework Implementation Tiers' - An additional property (SCRM) was added to each of the Implementation Tiers
p. 10	Section 2.2 'Framework Implementation Tiers' - Tier 2 'Risk Informed' - Paragraph 2 was modified to include: "*Consideration of cybersecurity in mission/business objectives may occur at some levels of the organization, but not at all levels. Cyber risk assessment of organizational assets is not typically repeatable or reoccurring.*"

PAGE(S)	**CHANGE**
p. 11	Section 2.2 ‘Framework Implementation Tiers’ - Tier 3 ‘Repeatable’ - Paragraph 2 was modified to include: “*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.*”
p. 11	Section 2.2 ‘Framework Implementation Tiers’ - Tier 4 ‘Adaptive’ - Paragraph 2 was modified to include: “*The relationship between cybersecurity risk and mission/business 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 understanding of current and predicted risk environment and future risk appetites. Business units implement executive vision and analyze system level risks in the context of the organizational risk appetite and tolerances.*”
p. 12	Section 2.2 ‘Framework Implementation Tiers’ - Tier 4 ‘Adaptive’ - Paragraph 2 was modified to include: “*Cybersecurity risk is clearly articulated and understood across all strata of the enterprise. The organization can quickly and efficiently account for changes to business/mission objectives and threat and technology landscapes in the risk disposition and approach.*”
p. 13	Figure 2: ‘Notional Information and Decision Flows within an Organization’ was modified to include additional ‘Actions’
p. 14	Section 3.0 ‘How to Use the Framework’ was modified to include the following: “*The Framework can be applied in design, build/buy, deploy, operate, and decommission system lifecycle phases. The design phase must account for cybersecurity requirements as a part of a larger multi-disciplinary systems engineering process. A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as summarized in a Framework Profile. The cybersecurity outcomes prioritized in a Profile must be enacted during either a) development of the system during the build phase or b) purchase or outsourcing of the system during the buy phase. In the system deploy phase, the cybersecurity features of the system should be assessed to verify the design was enacted. The cybersecurity outcomes of Framework then serve as a basis for on-going operation of the system, including occasional re-assessment to verify cybersecurity requirements are still fulfilled. Owed to an inevitable Web of dependencies amongst systems, Framework outcomes must be carefully considered as one or more systems are decommissioned.*”

PAGE(S)	CHANGE
p. 15	Section 3.2 'Establishing or Improving a Cybersecurity Program' - Step 1: 'Prioritize and Scope' was modified to include: "*Implementation Tiers may be used to express varying risk tolerances.*"
p. 15	Section 3.2 'Establishing or Improving a Cybersecurity Program' - Step 2: 'Orient' was modified to now read as follows: "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.***"
p. 15	Section 3.2 'Establishing or Improving a Cybersecurity Program' - Step 3: 'Create a Current Profile' was modified to include: "*If an outcome is partially achieved, noting this fact will help support subsequent steps.*"
p. 15	Section 3.2 'Establishing or Improving a Cybersecurity Program' - Step 4: 'Conduct a Risk Assessment' was modified to now read as follows: "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 both internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.***"
pp. 15-16	Section 3.2 'Establishing or Improving a Cybersecurity Program' - Step 5: 'Create a Target Profile' was modified to include: "*When used in conjunction with an Implementation Tier, characteristics of the Tier level should be reflected in the desired cybersecurity outcomes.*"
p. 16	Section 3.2 'Establishing or Improving a Cybersecurity Program' - Step 6: 'Determine, Analyze, and Prioritize Gaps' was modified to now read as follows: "The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address those gaps ***drawing upon mission drivers, a cost/benefit analysis, and risk understanding to achieve the outcomes in the Target Profile.*** The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements."

PAGE(S)	CHANGE
pp. 16-18	Section 3.3 'Communicating Cybersecurity Requirement with Stakeholders' was modified to include Supply Chain Risk Management.
p. 17	Figure 3: 'Cyber Supply Chain Relationships' was added
p. 18	Section 3.4 'Buying Decisions' was added
p. 18	Section 3.5 'Identifying Opportunities for New or Revised Informative References' (previously Section 3.4) was moved to accommodate an additional section.
p. 18	Section 3.6 'Methodology to Protect Privacy and Civil Liberties' (previously Section 3.5) was moved to accommodate an additional section.
p. 19	Section 3.6 'Methodology to Protect Privacy and Civil Liberties' - a portion of this section was modified to now read as follows: "Privacy ***and cybersecurity have a strong nexus. It is well-recognized that cybersecurity plays an important role in protecting individuals' privacy; for example, with respect to the confidentiality of assets containing personal information. Nonetheless, an organization's cybersecurity activities also can create risks to privacy and civil liberties*** when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities. Some examples of activities that bear privacy or civil liberties considerations may 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; cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including activities such as some types of incident detection or monitoring that may impact freedom of expression or association."
p. 20	Section 3.7 'Industrial Control and Cyber-Physical Systems' was added
p. 21	Section 3.8 'Federal Alignment' was added
p. 22	Section 4.0 'Measuring and Demonstrating Cybersecurity' was added
pp. 22-23	Section 4.1 'Correlation to Business Results' was added
pp. 24-25	Section 4.2 'Types of Cybersecurity Measurement' was added
p. 24	Table 1: 'Types of Framework Measurement' was added
p. 27	Table 2: 'Function and Category Unique Identifiers' (previously Table 1) was moved to accommodate an additional table.

PAGE(S)	CHANGE
p. 27	Table 2: ‘Function and Category Unique Identifiers’ was updated to include an additional Category (ID.SC) Supply Chain Risk Management
p. 28	Table 3: ‘Framework Core’ (previously Table 2) was moved to accommodate an additional table.
p. 28	Appendix A: ‘Framework Core’ - Subcategory ID.AM-5 was modified to now read as follows: "Resources (e.g., hardware, devices, data, ***time***, and software) are prioritized based on their classification, criticality, and business value"
p. 29	Appendix A: ‘Framework Core’ - Subcategory ID.BE-5 was modified to now read as follows: “Resilience requirements to support delivery of critical services are established ***for all operating states (e.g. under duress/attack, during recovery, normal operations)***”
p. 29	Appendix A: ‘Framework Core’ - Subcategory ID.GV-1 - Informative Reference was added ‘CSC(V6) 19.2’
p. 30	Appendix A: ‘Framework Core’ - Subcategory ID.RA-2 was modified to now read as follows: “***Cyber threat intelligence*** and vulnerability information is received from information sharing forums and sources”
p. 31	Appendix A: ‘Framework Core’ - Subcategory ID.RA-6 - Informative Reference was added ‘CSC(V6) 4.8’
pp. 31-33	Appendix A: ‘Framework Core’ - Category ID.SC: ‘Supply Chain Risk Management’ and subsequent Subcategories (ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, ID.SC-5) and Informative References were added
p. 33	Appendix A: ‘Framework Core’ - Category PR.AC: ‘Identity Management and Access Control’ was modified to include Identity Management and now reads: “Access to ***physical and logical*** assets and associated facilities is limited to authorized users, processes, or and devices, and ***is managed consistent with the assessed risk of unauthorized access.***”
p. 33	Appendix A: ‘Framework Core’ - Subcategory PR.AC-1 was modified to now read as follows: “Identities and credentials are ***issued, managed, revoked, and audited*** for authorized devices, and users, ***and processes***”
p. 33	Appendix A: ‘Framework Core’ - Subcategory PR.AC-4 was modified to now read as follows: “Access permissions ***and authorizations*** are managed, incorporating the principles of least privilege and separation of duties”

PAGE(S)	CHANGE
p. 34	Appendix A: ‘Framework Core’ - Subcategory PR.AC-6 and subsequent Informative References were added
p. 36	Appendix A: ‘Framework Core’ - Subcategory PR.DS-8 and subsequent Informative References were added
p. 36	Appendix A: ‘Framework Core’ - Subcategory PR.IP-1 was modified to now read as follows: “A baseline configuration of information technology/industrial control systems is created and maintained ***incorporating appropriate security principles (e.g. concept of least functionality)***”
p. 39	Appendix A: ‘Framework Core’ - Subcategory PR.PT-3 was modified to now read as follows: “*The principle of least functionality is incorporated by configuring systems to provide only essential capabilities*”
p. 40	Appendix A: ‘Framework Core’ - Subcategory PR.PT-5 and subsequent Informative References were added
p. 48	Appendix B: ‘Glossary’ - was modified to include the term ‘Buyer’ with the definition: “*The people or organizations that consume a given product of service*”
p. 49	Appendix B: ‘Glossary’ - was modified to include the term ‘Lagging Measurement’ with the definition: “*A measurement of whether an outcome was fulfilled or not*”
p. 49	Appendix B: ‘Glossary’ - was modified to include the term ‘Leading Measurement’ with the definition: “*A predictive measurement that may guide future activities to achieve a specific outcome*”
p. 49	Appendix B: ‘Glossary’ - was modified to include the term ‘Measures’ with the definition: “*Quantifiable, observable, objective data supporting Metrics. Typically, Measures align with technical controls, such as the Informative References.*”
p. 49	Appendix B: ‘Glossary’ - was modified to include the term ‘Metrics’ with the definition: “*Used to facilitate decision making and improve performance and accountability. Typically, Metrics are higher level, qualitative, and an aggregate of several Measures.*”

PAGE(S)	**CHANGE**
p. 49	Appendix B: 'Glossary' - was modified to include the term 'Non-IT/OT Partner' with the definition: "*Product or service providers that do not provide IT or OT to a given organization, but who do affect the security of that organization.*"
p. 50	Appendix B: 'Glossary' - was modified to include the term 'Supplier' with the definition: "*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.*"
p. 51	Appendix C: 'Acronyms' - was modified to include CPS - Cyber-Physical Systems
p. 51	Appendix C: 'Acronyms' - was modified to include OT - Operational Technology
p. 51	Appendix C: 'Acronyms' - was modified to include PII - Personally Identifiable Information
p. 51	Appendix C: 'Acronyms' - was modified to include SCRM - Supply Chain Risk Management