# Improving Critical Infrastructure Cybersecurity Executive Order 13636

## Preliminary Cybersecurity Framework

## Note to Reviewers

The *Preliminary Cybersecurity Framework* for improving critical infrastructure cybersecurity is now available for review. The Preliminary Cybersecurity Framework is provided by the National Institute of Standards and Technology (NIST).

If the Cybersecurity Framework is to be effective in helping to reduce cybersecurity risk to the Nation's critical infrastructure, it must be able to assist organizations in addressing a variety of cybersecurity challenges. The National Institute of Standards and Technology (NIST) requests that reviewers consider the following questions:

Does the Preliminary Framework:

- adequately define outcomes that strengthen cybersecurity and support business objectives?
- enable cost-effective implementation?
- appropriately integrate cybersecurity risk into business risk?
- provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?
- provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?
- provide the right level of specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties?
- express existing practices in a manner that allows for effective use?

Will the Preliminary Framework, as presented:

- be inclusive of, and not disruptive to, effective cybersecurity practices in use today, including widely-used voluntary consensus standards that are not yet final?
- enable organizations to incorporate threat information?

Is the Preliminary Framework:

- presented at the right level of specificity?
- sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?

## Disclaimer

Any mention of commercial products is for information only; it does not imply NIST recommendation or endorsement, nor does it imply that the products mentioned are necessarily the best available for the purpose.

## Table of Contents



## List of Figures



## List of Tables

# 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.[1] 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" for assisting organizations responsible for critical infrastructure services to manage 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 threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk.

The critical infrastructure community includes public and private owners and operators, and other supporting entities that play a role in securing the Nation's infrastructure. Each sector performs critical functions that are supported by information technology (IT), industrial control systems (ICS) and, in many cases, both IT and ICS.[2] To manage cybersecurity risks, a clear understanding of the security challenges and considerations specific to IT and ICS is required. Because each organization's risk is unique, along with its use of IT and ICS, the implementation of the Framework will vary.

The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk. A key objective of the Framework is to encourage organizations to consider cybersecurity risk as a priority similar to financial, safety, and operational risk while factoring in larger systemic risks inherent to critical infrastructure.

The Framework relies on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk. By relying on those practices developed, managed, and updated by industry, the Framework will evolve with technological advances and business requirements. The use of standards will enable economies of scale to drive innovation and development of effective products and services that meet identified market needs. Market competition also promotes faster diffusion of these technologies and realization of many benefits by the stakeholders in these sectors.

Building off those standards, guidelines, and practices, the Framework provides a common language 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 risk management; 4) assess progress toward the target state; 5) foster communications among internal and external stakeholders.

---

[1] 78 FR 11737

[2] The DHS CIKR program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure

The Framework complements, and does not replace, an organization's existing business or cybersecurity risk management process and cybersecurity program. Rather, the organization can use its current processes and leverage the Framework to identify opportunities to improve an organization's management of cybersecurity risk. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

The goal of the open process in developing the Preliminary Framework was to develop a robust technical basis to allow organizations to align this guidance with their organizational practices. This Preliminary Framework is being issued for public comment for stakeholders to inform the next version of the Framework that will be completed in February 2014, as required in EO 13636.

## 1.1 Overview of the Framework

The Framework is a risk-based approach composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. These components are detailed below.

- The *Framework Core* is a set of cybersecurity activities and references that are common across critical infrastructure sectors organized around particular outcomes. The Core presents standards and best practices in a manner that allows for communication of cybersecurity risk across the organization from the senior executive level to the implementation/operations level. The Framework Core consists of five Functions—Identify, Protect, Detect, Respond, Recover—which can provide a high-level, strategic view of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each of these Functions, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory. This structure ties the high level strategic view, outcomes and standards based actions together for a cross-organization view of cybersecurity activities. For instance, for the "Protect" Function, categories include: Data Security; Access Control; Awareness and Training; and Protective Technology. *ISO/IEC 27001 Control A.10.8.3* is an informative reference which supports the "Data during transportation/transmission is protected to achieve confidentiality, integrity, and availability goals" Subcategory of the "Data Security" Category in the "Protect" Function.

  Appendix B contains a methodology to protect privacy and civil liberties for a cybersecurity program as required under the Executive Order. Organizations may already have processes for addressing privacy risks such as a process for conducting privacy impact assessments. The privacy methodology is designed to complement such processes by highlighting privacy considerations and risks that organizations should be aware of when using cybersecurity measures or controls. As organizations review and select relevant categories from the Framework Core, they should review the corresponding category section in the privacy methodology. These considerations provide organizations with flexibility in determining how to manage privacy risk.

- A *Framework Profile* ("Profile") represents the outcomes that a particular system or organization has achieved or is expected to achieve as specified in the Framework Categories and Subcategories. The Profile can be characterized as the alignment of

industry standards and best practices to the Framework Core in a particular implementation scenario. Profiles are also used to identify opportunities for improving cybersecurity by comparing a "Current" Profile with a "Target" Profile. The 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. In this sense, Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

- *Framework Implementation Tiers* ("Tiers") describe how cybersecurity risk is managed by an organization. The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics (e.g., risk and threat aware, repeatable, and adaptive) defined in Section 2.3. The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4), progressing from informal, reactive implementations to approaches that are agile and risk-informed.

## 1.2 Risk Management and the Cybersecurity Framework

Risk management is the process of identifying, assessing, and responding to risk. Particularly within critical infrastructure, organizations should understand the likelihood that a risk event will occur and the resulting impact. With this information, organizations determine the acceptable level of risk for IT and ICS assets and systems, expressed as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize systems that require attention. This will enable organizations to optimize cybersecurity expenditures. Furthermore, the implementation of risk management programs offers organizations the ability to quantify and communicate changes to organizational cybersecurity. Risk is also a common language that can be communicated to internal and external stakeholders.

While not a risk management process itself, the Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. The Framework utilizes risk assessment to help organizations select optimized target states for cybersecurity activities. Thus, the Framework gives organizations the ability to dynamically select and direct improvements in both IT and ICS cybersecurity risk management.

A comprehensive risk management approach provides the ability to identify, assess, respond to, and monitor cybersecurity-related risks and provide organizations with the information to make ongoing risk-based decisions. Examples of cybersecurity risk management processes include the International Organization for Standardization (ISO) 31000, ISO 27005, NIST Special Publication (SP) 800-39 and the Electricity Sector Cybersecurity Risk Management Process (RMP) Guideline.

Within the critical infrastructure, organizations vary widely in their business models, resources, risk tolerance, approaches to risk management, and effects on security, national economic security, and national public health or safety. Because of these differences, the Framework is risk-based to provide flexible implementation.

## 1.3 Document Overview

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

- Section 2 describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- Section 3 presents examples of how the Framework can be used.
- Appendix A presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- Appendix B contains a methodology to protect privacy and civil liberties for a cybersecurity program.
- Appendix C discusses areas for improvement in cybersecurity standards and practices identified as a result of the Framework efforts to date.
- Appendix D describes the Framework development methodology.
- Appendix E contains a glossary of selected terms.
- Appendix F lists acronyms used in this document.

# 2.0 Framework Basics

The Framework provides a common language for expressing, understanding, and managing cybersecurity risk, both internally and externally. The Framework can be used to help identify and prioritize actions for reducing cybersecurity risk and is a tool for aligning policy, business, and technological approaches to managing that risk. Different types of entities — including sectors, organizations, and associations — can use the Framework for different means, including the creation of common Profiles.

## 2.1 Framework Core

The *Framework Core* provides references to cybersecurity activities and Informative References. The Framework Core is not a checklist of activities to perform; it presents key cybersecurity outcomes that are aligned with activities known to manage cybersecurity risk. These activities are mapped to a subset of commonly used standards and guidelines. The Framework 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. The functions aid in communicating

the state of an organization's cybersecurity activities 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 can be used to 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 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 subdivide a Category into high-level outcomes, but are not intended to be a comprehensive set of practices to support a category. Examples of subcategories include "Physical devices and systems within the organization are catalogued," "Data-at-rest is protected," and "Notifications from the detection system are investigated."
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors and illustrate a method to accomplish the activities within each Subcategory. The Subcategories are derived from the Informative References. The Informative References presented in the Framework Core are not exhaustive but are example sets, and organizations are free to implement other standards, guidelines, and practices.[3]

See **Appendix A** for the complete Framework Core listing. In addition, **Appendix B** provides an initial methodology to help organizations identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on privacy and civil liberties.

The five Framework Core Functions defined below apply to both IT and ICS.

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

  The Identify Function includes the following categories of outcomes: Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy. The activities in the Identify Function are foundational for effective implementation of the Framework. Understanding the business context, resources that support critical functions and the related cybersecurity risks enable an organization to focus its efforts and resources. Defining a risk management strategy enables risk decisions consistent with the business needs or the organization.

- **Protect** – Develop and implement the appropriate safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure services.

[3] NIST developed a compendium of informative references gathered from the RFI input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process 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 stakeholder input.

The Protect function includes the following categories of outcomes: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, and Protective Technology. The Protect activities are performed consistent with the organization's risk strategy defined in the Identify function.

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

  The Detect function includes the following categories of outcomes: Anomalies and Events, Security Continuous Monitoring, and Detection Processes. The Detect function enables timely response and the potential to limit or contain the impact of potential cyber incidents.

- **Respond** – Develop and implement the appropriate activities, prioritized through the organization's risk management process (including effective planning), to take action regarding a detected cybersecurity event.

  The Respond function includes the following categories of outcomes: Response Planning, Analysis, Mitigation, and Improvements. The Respond function is performed consistent with the business context and risk strategy defined in the Identify function. The activities in the Respond function support the ability to contain the impact of a potential cybersecurity event.

- **Recover** – Develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a cybersecurity event.

  The Recover function includes the following categories of outcomes: Recovery Planning, Improvements, and Communications. The activities performed in the Recover function are performed consistent with the business context and risk strategy defined in the Identify function. The activities in the Recover function support timely recovery to normal operations to reduce the impact from a cybersecurity event.

## 2.2 Framework Profile

A Framework Profile ("Profile") is a tool to enable organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organization and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. A Framework Profile can be used to describe both the current state and the desired target state of specific cybersecurity activities, thus revealing gaps that should be addressed to meet cybersecurity risk management objectives. **Figure 2** shows the two types of Profiles: Current and Target. 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. The Target Profile is built to support business/mission requirements and aid in the communication of risk within and between organizations.

The Profile is the alignment of the Functions, Categories, Subcategories and industry standards and best practices with the business requirements, risk tolerance, and resources of the organization. Identifying the gaps between the Current Profile and the Target Profile allows the creation of a prioritized roadmap that organizations will implement to reduce cybersecurity risk. The prioritization of the gaps is driven by the organization's Risk Management Processes and

serve as an essential part for resource and time estimates needed that are critical to prioritization decisions.

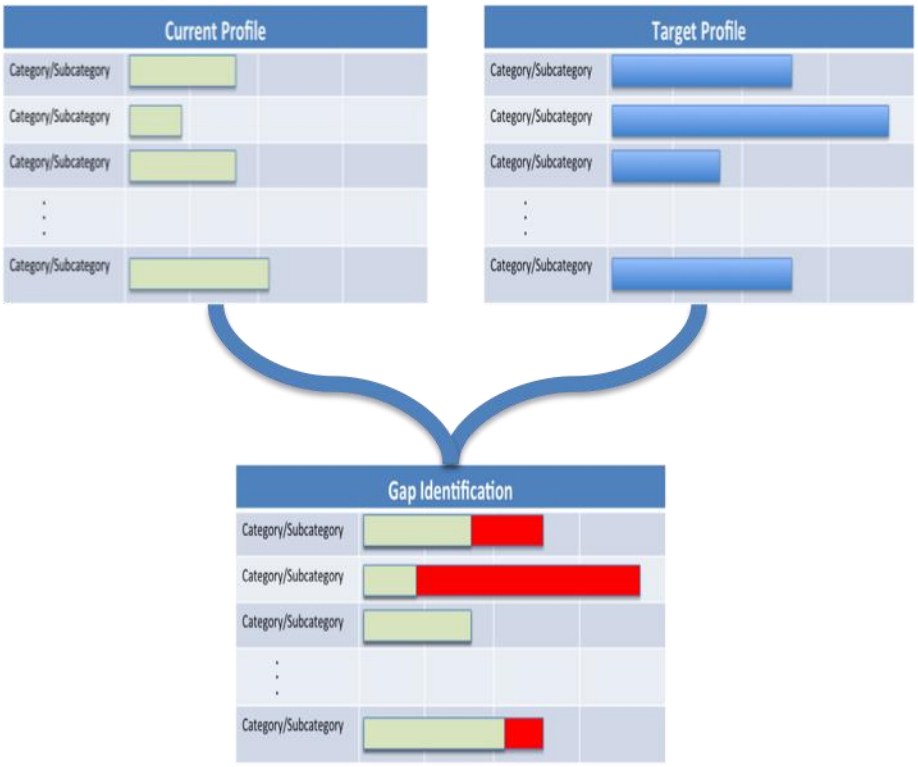


**Figure 2: Profile Comparisons**

The Framework provides a mechanism for organizations, sectors, and other entities to create their own Target Profiles. It does not provide Target Profile templates; rather, sectors and organizations should identify existing Target Profiles that could be customized for their purposes and needs.

## 2.3 Coordination of Framework Implementation

**Figure 3** describes the notional flow of information and decisions within an organization: at the senior executive level, at the business/process level, and at the implementation/operations level.

The senior 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 their risk management process, and then collaborates with the implementation/operations level to create a Profile. The implementation/operation level communicates the Profile implementation to the business/process level. The business/process level uses this information to perform an impact assessment. The outcomes of that impact assessment are reported to the senior executive level to inform the organization's overall risk management process.

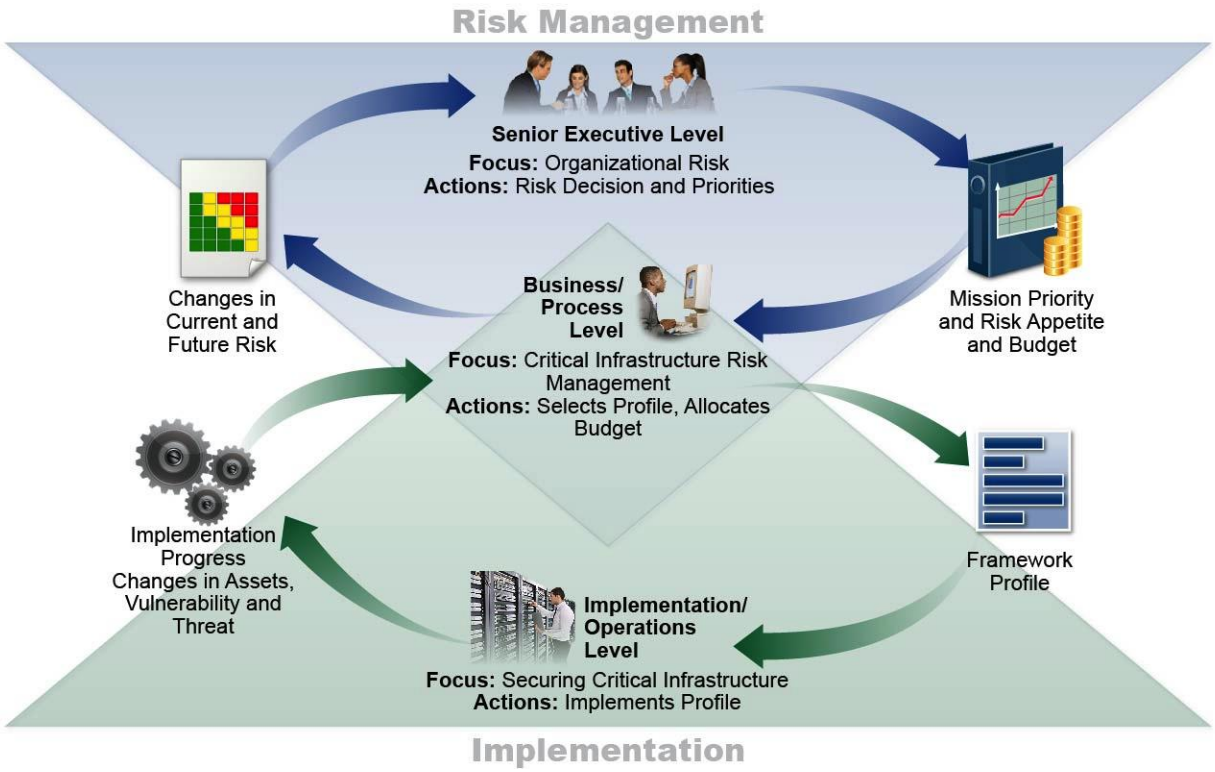


**Figure 3: Notional Information and Decision Flows within an Organization**

## 2.4 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") describe how an organization manages its cybersecurity 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 integrated into an organization's overall risk management practices. The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected levels meet the organizational goals, reduce cybersecurity risk to critical infrastructure, and are feasible and cost-effective to implement. 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 Program – There is a limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. 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.

- **Tier 2: Risk-Informed**
  - Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy.
  - Integrated 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. Risk-informed, management-approved processes and procedures are defined and implemented and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.
  - External Participation – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.
- **Tier 3: Risk-Informed and 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 a changing threat and technology landscape.
  - Integrated Program – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. Consistent methods are in place to effectively respond to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
  - External Participation – The organization understands its dependencies and partners and receives information from these partners enabling collaboration and risk-based management decisions within the organization in response to events.
- **Tier 4: Adaptive**
  - Risk Management Process – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous cybersecurity activities. Through a process of continuous improvement, the organization actively adapts to a changing cybersecurity landscape and responds to emerging/evolving threats in a timely manner.
  - Integrated Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.

- 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 an event occurs.

Organizations should consider leveraging external guidance, such as information that could be obtained from Federal government departments and agencies, an Information Sharing and Analysis Center (ISAC), existing maturity models, or other sources to assist in determining their desired tier.

# 3.0 How to Use the Framework

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. The following examples present several options for using the Framework.

## 3.1 Basic Overview of Cybersecurity Practices

Organizations can examine what capabilities they have implemented in the five high-level Functions identified in the Framework Core: Identify, Protect, Detect, Respond, and Recover. Organizations should have at least basic capabilities implemented in each of these areas, and can begin to review what particular categories and subcategories they currently use to help achieve those outcomes.

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

## 3.2 Establishing or Improving a Cybersecurity Program

The following recommended recursive steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing cybersecurity program.

Step 1: **Identify**. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach.

Step 2: **Create a Current Profile**. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

Step 3: **Conduct a Risk Assessment**. 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 critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

Step 4: **Create a Target Profile**. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

Step 5: **Determine, Analyze, and Prioritize Gaps**. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

Step 6: **Implement Action Plan**. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies Informative References regarding the practices described in the Categories and Subcategories. Appendix B, the Privacy Methodology, provides guidance on privacy and civil liberties considerations for the selected Categories and Subcategories.

## 3.3 Communicating Cybersecurity Requirements with Stakeholders

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

- An organization may utilize a Target Profile to express 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 for comparison 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 Categories and Subcategories.
- A critical infrastructure sector may establish a baseline Target Profile that can be used among its constituents as an initial baseline.

## 3.4 Identifying Opportunities for New or Revised Informative References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging threats. An organization implementing a given 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 to address the needs of potential adopters.

# 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 Framework Core presented in this appendix is not exhaustive; it is extensible, allowing organizations, sectors, and other entities to add Subcategories and Informative References that are relevant to them and enable them to more effectively 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.

**Table 1: Framework Core**

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| **IDENTIFY** (ID) | **Asset Management (AM):** The 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 | • **ISA 99.02.01** 4.2.3.4<br>• **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05<br>• **ISO/IEC 27001** A.7.1.1, A.7.1.2<br>• **NIST SP 800-53 Rev. 4** CM-8<br>• **CCS CSC**1 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | • **ISA 99.02.01** 4.2.3.4<br>• **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05<br>• **ISO/IEC 27001** A.7.1.1, A.7.1.2<br>• **NIST SP 800-53 Rev. 4** CM-8<br>• **CCS CSC** 2 |
| | | **ID.AM-3:** The organizational communication and data flow is mapped | • **ISA 99.02.01** 4.2.3.4<br>• **COBIT** DSS05.02<br>• **ISO/IEC 27001** A.7.1.1<br>• **NIST SP 800-53 Rev. 4** CA-3, CM-8, CA-9<br>• **CCS CSC** 1 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | **ID.AM-4:** External information systems are mapped and catalogued | • **NIST SP 500-291** 3, 4<br>• **NIST SP 800-53 Rev. 4** AC-20, SA-9 |
| | | **ID.AM-5:** Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software | • **ISA 99.02.01** 4.2.3.6<br>• **COBIT** APO03.03, APO03.04, BAI09.02<br>• **NIST SP 800-53 Rev. 4** RA-2, CP-2<br>• **NIST SP 800-34** Rev 1<br>• **ISO/IEC 27001** A.7.2.1 |
| | | **ID.AM-6:** Workforce roles and responsibilities for business functions, including cybersecurity, are established | • **ISA 99.02.01** 4.3.2.3.3<br>• **COBIT** APO01.02, BAI01.12, DSS06.03<br>• **ISO/IEC 27001** A.8.1.1<br>• **NIST SP 800-53 Rev. 4** CP-2, PM-11<br>• **NIST SP 800-34** Rev 1 |
| | **Business Environment (BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized, and inform cybersecurity roles, responsibilities, and risk decisions. | **ID.BE-1:** The organization's role in the supply chain and is identified and communicated | • **COBIT** APO08.01, APO08.02, APO08.03, APO08.04, APO08.05, APO10.03, DSS01.02<br>• **ISO/IEC 27001** A.10.2<br>• **NIST SP 800-53 Rev. 4** CP-2 |
| | | **ID.BE-2:** The organization's place in critical infrastructure and their industry ecosystem is identified and communicated | • **COBIT** APO02.06, APO03.01<br>• **NIST SP 800-53 Rev. 4** PM-8 |
| | | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established | • **ISA 99.02.01** 4.2.2.1, 4.2.3.6<br>• **COBIT** APO02.01, APO02.06, APO03.01<br>• **NIST SP 800-53 Rev. 4** PM-11 |
| | | **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established | • **COBIT** DSS01.03<br>• **ISO/IEC 27001** 9.2.2<br>• **NIST SP 800-53 Rev 4** CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PM-8 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | **ID.BE-5**: Resilience requirements to support delivery of critical services are established | • **NIST SP 800-53 Rev. 4** CP-2, SA-14 |
| | **Governance (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 | • **ISA 99.02.01** 4.3.2.6<br>• **COBIT** APO01.03, EA01.01<br>• **ISO/IEC 27001** A.6.1.1<br>• **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1) |
| | | **ID.GV-2:** Information security roles & responsibility are coordinated and aligned | • **ISA 99.02.01** 4.3.2.3.3<br>• **ISO/IEC 27001** A.6.1.3<br>• **NIST SP 800-53 Rev. 4** AC-21, PM-1, PS-7 |
| | | **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | • **ISA 99.02.01** 4.4.3.7<br>• **COBIT** MEA03.01, MEA03.04<br>• **ISO/IEC 27001** A.15.1.1<br>• **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 | • **NIST SP 800-53 Rev. 4** PM-9, PM-11 |
| | **Risk Assessment (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 | • **ISA 99.02.01** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12<br>• **COBIT** APO12.01, APO12.02, APO12.03, APO12.04<br>• **ISO/IEC 27001** A.6.2.1, A.6.2.2, A.6.2.3<br>• **CCS CSC**4<br>• **NIST SP 800-53 Rev. 4** CA-2, RA-3, RA-5, SI-5 |
| | | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources. | • **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12<br>• **ISO/IEC 27001** A.13.1.2<br>• **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | **ID.RA-3:** Threats to organizational assets are identified and documented | • **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12<br>• **COBIT** APO12.01, APO12.02, APO12.03, APO12.04<br>• **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-16 |
| | | **ID.RA-4:** Potential impacts are analyzed | • **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12<br>• **NIST SP 800-53 Rev. 4** RA-3 |
| | | **ID.RA-5**: Risk responses are identified. | • **NIST SP 800-53 Rev. 4** PM-9 |
| | **Risk Management Strategy (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 managed and agreed to | • **ISA 99.02.01** 4.3.4.2<br>• **COBIT** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02<br>• **NIST SP 800-53 Rev. 4** PM-9<br>• **NIST SP 800-39** |
| | | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | • **ISA 99.02.01** 4.3.2.6.5<br>• **COBIT** APO10.04, APO10.05, APO12.06<br>• **NIST SP 800-53 Rev. 4** PM-9<br>• **NIST SP 800-39** |
| | | **ID.RM-3**: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis | • **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11 |
| **PROTECT (PR)** | **Access Control (AC):** Access to information resources and associated facilities are limited to authorized users, processes or devices (including other information systems), and to authorized activities and transactions. | **PR.AC-1:** Identities and credentials are managed for authorized devices and users | • **ISA 99.02.01** 4.3.3.5.1<br>• **COBIT** DSS05.04, DSS06.03<br>• **ISO/IEC 27001** A.11<br>• **NIST SP 800-53 Rev. 4** AC-2, AC-5, AC-6, IA Family<br>• **CCS CSC** 16 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | **PR.AC-2:** Physical access to resources is managed and secured | • **ISA 99.02.01** 4.3.3.3.2, 4.3.3.3.8<br>• **COBIT** DSS01.04, DSS05.05<br>• **ISO/IEC 27001** A.9.1, A.9.2, A.11.4, A.11.6<br>• **NIST SP 800-53 Rev 4** PE-2, PE-3, PE-4, PE-6, PE-9 |
| | | **PR.AC-3:** Remote access is managed | • **ISA 99.02.01** 4.3.3.6.6<br>• **COBIT** APO13.01, DSS01.04, DSS05.03<br>• **ISO/IEC 27001** A.11.4, A.11.7<br>• **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20 |
| | | **PR.AC-4:** Access permissions are managed | • **ISA 99.02.01** 4.3.3.7.3<br>• **ISO/IEC 27001** A.11.1.1<br>• **NIST SP 800-53 Rev. 4** AC-3, AC-4, AC-6, AC-16<br>• **CCS CSC** 12, 15 |
| | | **PR.AC-5:** Network integrity is protected | • **ISA 99.02.01** 4.3.3.4<br>• **ISO/IEC 27001** A.10.1.4, A.11.4.5<br>• **NIST SP 800-53 Rev 4** AC-4 |
| | **Awareness and Training (AT):** The organization's personnel and partners are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. | **PR.AT-1:** General users are informed and trained | • **ISA 99.02.01** 4.3.2.4.2<br>• **COBIT** APO07.03, BAI05.07<br>• **ISO/IEC 27001** A.8.2.2<br>• **NIST SP 800-53 Rev. 4** AT-2<br>• **CCS CSC** 9 |
| | | **PR.AT-2:** Privileged users understand roles & responsibilities | • **ISA 99.02.01** 4.3.2.4.2, 4.3.2.4.3<br>• **COBIT** APO07.02<br>• **ISO/IEC 27001** A.8.2.2<br>• **NIST SP 800-53 Rev. 4** AT-3<br>• **CCS CSC** 9 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | **PR.AT-3:** Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities | • **ISA 99.02.01** 4.3.2.4.2<br>• **COBIT** APO07.03, APO10.04, APO10.05<br>• **ISO/IEC 27001** A.8.2.2<br>• **NIST SP 800-53 Rev. 4** AT-3<br>• **CCS CSC** 9 |
| | | **PR.AT-4: S**enior executives understand roles & responsibilities | • **ISA 99.02.01** 4.3.2.4.2<br>• **COBIT** APO07.03<br>• **ISO/IEC 27001** A.8.2.2<br>• **NIST SP 800-53 Rev. 4** AT-3<br>• **CCS CSC** 9 |
| | | **PR.AT-5:** Physical and information security personnel understand roles & responsibilities | • **ISA 99.02.01** 4.3.2.4.2<br>• **COBIT** APO07.03<br>• **ISO/IEC 27001** A.8.2.2<br>• **NIST SP 800-53 Rev. 4** AT-3<br>• **CCS CSC** 9 |
| | **Data Security (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 | • **COBIT** APO01.06, BAI02.01, BAI06.01, DSS06.06<br>• **ISO/IEC 27001** A.15.1.3, A.15.1.4<br>• **CCS CSC** 17<br>• **NIST SP 800-53 Rev 4** SC-28 |
| | | **PR.DS-2:** Data-in-motion is secured | • **COBIT** APO01.06, BAI02.01, BAI06.01, DSS06.06<br>• **ISO/IEC 27001** A.10.8.3<br>• **NIST SP 800-53 Rev. 4** SC-8<br>• **CCS CSC** 17 |
| | | **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition | • **COBIT** BAI09.03<br>• **ISO/IEC 27001** A.9.2.7, A.10.7.2<br>• **NIST SP 800-53 Rev 4** PE-16, MP-6, DM-2 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | **PR.DS-4:** Adequate capacity to ensure availability is maintained. | • **COBIT** APO13.01<br>• **ISO/IEC 27001** A.10.3.1<br>• **NIST SP 800-53 Rev 4** CP-2, SC-5 |
| | | **PR.DS-5:** There is protection against data leaks | • **COBIT** APO01.06<br>• **ISO/IEC 27001** A.12.5.4<br>• **CCS CSC** 17<br>• **NIST SP 800-53 Rev 4** AC-4, PE-19, SC-13, SI-4, SC-7, SC-8, SC-31, AC-5, AC-6, PS-6 |
| | | **PR.DS-6:** Intellectual property is protected | • **COBIT** APO01.03, APO10.02, APO10.04, MEA03.01 |
| | | **PR.DS-7:** Unnecessary assets are eliminated | • **COBIT** BAI06.01, BAI01.10<br>• **ISO/IEC 27001** A.10.1.3<br>• **NIST SP 800-53 Rev. 4** AC-5, AC-6 |
| | | **PR.DS-8:** Separate testing environments are used in system development | • **COBIT** BAI07.04<br>• **ISO/IEC 27001** A.10.1.4<br>• **NIST SP 800-53 Rev. 4** CM-2 |
| | | **PR.DS-9:** Privacy of individuals and personally identifiable information (PII) is protected | • **COBIT** BAI07.04, DSS06.03, MEA03.01<br>• **ISO/IEC 27001** A.15.1.3<br>• **NIST SP 800-53** Rev 4, Appendix J |
| | **Information Protection Processes and Procedures (IP):** Security policy (that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems | **PR.IP-1:** A baseline configuration of information technology/operational technology systems is created | • **ISA 99.02.01** 4.3.4.3.2, 4.3.4.3.3<br>• **COBIT** BAI10.01, BAI10.02, BAI10.03, BAI10.05<br>• **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-7, CM-9, SA-10<br>• **CCS CSC** 3, 10 |
| | | **PR.IP-2:** A System Development Life Cycle to manage systems is implemented | • **ISA 99.02.01** 4.3.4.3.3<br>• **COBIT** APO13.01 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | and assets. | | • **ISO/IEC 27001** A.12.5.5<br>• **NIST SP 800-53 Rev 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17, PL-8<br>• **CCS CSC** 6 |
| | | **PR.IP-3:** Configuration change control processes are in place | • **ISA 99.02.01** 4.3.4.3.2, 4.3.4.3.3<br>• **COBIT** BAI06.01, BAI01.06<br>• **ISO/IEC 27001** A.10.1.2<br>• **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10 |
| | | **PR.IP-4:** Backups of information are managed | • **ISA 99.02.01** 4.3.4.3.9<br>• **COBIT** APO13.01<br>• **ISO/IEC 27001** A.10.5.1<br>• **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** DSS01.04, DSS05.05<br>• **ISO/IEC 27001** 9.1.4<br>• **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 |
| | | **PR.IP-6:** Information is destroyed according to policy and requirements | • **COBIT** BAI09.03<br>• **ISO/IEC 27001** 9.2.6<br>• **NIST SP 800-53 Rev 4** MP-6 |
| | | **PR.IP-7:** Protection processes are continuously improved | • **COBIT** APO11.06, DSS04.05<br>• **NIST SP 800-53 Rev 4** PM-6, CA-2, CA-7, CP-2, IR-8, PL-2 |
| | | **PR.IP-8:** Information sharing occurs with appropriate parties | • **ISO/IEC 27001** A.10<br>• **NIST SP 800-53 Rev. 4** AC-21 |
| | | **PR.IP-9:** Response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) are in place and managed | • **COBIT** DSS04.03<br>• **ISO/IEC 27001** A.14.1<br>• **NIST SP 800-53 Rev. 4** CP-2, IR-8 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | **PR.IP-10:** Response plans are exercised | • **NIST SP 800-53 Rev.4** IR-3 |
| | | **PR.IP-11:** Cybersecurity is included in human resources practices (de-provisioning, personnel screening, etc.) | • **COBIT** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05<br>• **ISO/IEC 27001** 8.2.3, 8.3.1<br>• **NIST SP 800-53 Rev 4** PS Family |
| | **Maintenance (MA):** Maintenance and repairs of operational and information system components is performed consistent with policies and procedures. | **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | • **ISO/IEC 27001** A.9.1.1, A.9.2.4, A.10.4.1<br>• **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 and supports availability requirements for important operational and information systems. | • **COBIT 5**<br>• **ISO/IEC 27001** A.9.2.4, A.11.4.4<br>• **NIST SP 800-53 Rev 4** MA-4 |
| | **Protective Technology (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 and log records are stored in accordance with audit policy | • **ISA 99.02.01** 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<br>• **COBIT** APO11.04<br>• **ISO/IEC 27001** A.10.10.1, A.10.10.3, A.10.10.4, A.10.10.5, A.15.3.1<br>• **NIST SP 800-53 Rev. 4** AU Family<br>• **CCS CSC** 14 |
| | | **PR.PT-2: R**emovable media are protected according to a specified policy | • **COBIT** DSS05.02, APO13.01<br>• **ISO/IEC 27001** A.10.7<br>• **NIST SP 800-53 Rev. 4** AC-19, MP-2, MP-4, MP-5, MP-7 |
| | | **PR.PT-3:** Access to systems and assets is appropriately controlled | • **CCS CSC** 6<br>• **COBIT** DSS05.02<br>• **NIST SP 800-53 Rev 4** CM-7 |
| | | **PR.PT-4:** Communications networks are secured | • **COBIT** DSS05.02, APO13.01<br>• **ISO/IEC 27001** 10.10.2<br>• **NIST SP 800-53 Rev 4** AC-18 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | | • **CCS CSC** 7 |
| | | **PR.PT-5:** Specialized systems are protected according to the risk analysis (SCADA, ICS, DLS) | • **COBIT** APO13.01,<br>• **NIST SP 800-53 Rev 4** |
| **DETECT (DE)** | **Anomalies and Events (AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood. | **DE.AE-1: A** baseline of normal operations and procedures is identified and managed | • **ISA 99.02.01** 4.4.3.3<br>• **COBIT** DSS03.01<br>• **NIST SP 800-53 Rev. 4** AC-2, SI-3, SI-4, AT-3, CM-2 |
| | | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | • **NIST SP 800-53 Rev. 4** SI-4, IR-4 |
| | | **DE.AE-3:** Cybersecurity data are correlated from diverse information sources | • **NIST SP 800-53 Rev. 4** SI-4 |
| | | **DE.AE-4:** Impact of potential cybersecurity events is determined. | • **NIST SP 800-53 Rev. 4** IR-4, SI -4 |
| | | **DE.AE-05:** Incident alert thresholds are created | • **ISA 99.02.01** 4.2.3.10<br>• **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-9<br>• **NIST SP 800-61** Rev 2 |
| | **Security Continuous Monitoring (CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | **DE.CM-1:** The network is monitored to detect potential cybersecurity events | • **COBIT** DSS05.07<br>• **ISO/IEC 27001** A.10.10.2, A.10.10.4, A.10.10.5<br>• **NIST SP 800-53 Rev. 4** CM-3, CA-7, AC-2, IR-5, SC-5, SI-4<br>• **CCS CSC** 14, 16 |
| | | **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events | • **NIST SP 800-53 Rev. 4** CM-3, CA-7, IR-5, PE-3, PE-6, PE-20 |
| | | **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events | • **NIST SP 800-53 Rev. 4** AC-2, CM-3, CA-7 |
| | | **DE.CM-4:** Malicious code is detected | • **COBIT** DSS05.01<br>• **ISO/IEC 27001** A.10.4.1<br>• **NIST SP 800-53 Rev 4** SI-3 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | | • **CCS CSC** 5 |
| | | **DE.CM-5:** Unauthorized mobile code is detected | • **ISO/IEC 27001** A.10.4.2<br>• **NIST SP 800-53 Rev 4** SC-18 |
| | | **DE.CM-6:** External service providers are monitored | • **ISO/IEC 27001** A.10.2.2<br>• **NIST SP 800-53 Rev 4** CA-7, PS-7, SI-4, SA-4, SA-9 |
| | | **DE.CM-7:** Unauthorized resources are monitored | • **NIST SP 800-53 Rev. 4** CM-3, CA-7, PE-3, PE-6, PE-20, SI-4 |
| | | **DE.CM-8:** Vulnerability assessments are performed | • **NIST SP 800-53 Rev. 4** CM-3, CA-7, CA-8, RA-5, SA-11, SA-12 |
| | **Detection Processes (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 | • **ISA 99.02.01** 4.4.3.1<br>• **COBIT** DSS05.01<br>• **NIST SP 800-53 Rev 4** IR-2, IR-4, IR-8<br>• **CCS CSC** 5 |
| | | **DE.DP-2:** Detection activities comply with all applicable requirements, including those related to privacy and civil liberties | • **ISA 99.02.01** 4.4.3.2<br>• **NIST SP 800-53 Rev 4** CA-2, CA-7 |
| | | **DE.DP-3:** Detection processes are exercised to ensure readiness | • **ISA 99.02.01** 4.4.3.2<br>• **NIST SP 800-53 Rev 4** PM-14 |
| | | **DE.DP-4:** Event detection information is communicated to appropriate parties | • **NIST SP 800-53 Rev. 4** CP-2, IR-8 |
| | | **DE.DP-5:** Detection processes are continuously improved | • **COBIT** APO11.06, DSS04.05<br>• **NIST SP 800-53 Rev 4** PM-6, CA-2, CA-7, CP-2, IR-8, PL-2 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| **RESPOND (RS)** | **Response Planning (RP):** Response processes and procedures are maintained and tested to ensure timely response of detected cybersecurity events. | **RS.PL-1:** Response plan is implemented during or after an event. | • **ISA 99.02.01** 4.3.4.5.1<br>• **NIST SP 800-53 Rev. 4** CP-10, IR-4<br>• **CCS CSC** 18 |
| | **Communications (CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies. | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | • **ISO/IEC 27001** A.13.2.1<br>• **ISA 99.02.01** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4<br>• **NIST SP 800-53 Rev 4** CP-2, IR-8 |
| | | **RS.CO-2:** Events are reported consistent with established criteria | • **ISO/IEC 27001** A.13.1.1, A.13.1.2<br>• **ISA 99.02.01** 4.3.4.5.5<br>• **NIST SP 800-53 Rev 4** IR-6, IR-8 |
| | | **RS.CO-3:** Detection/response information, such as breach reporting requirements, is shared consistent with response plans, including those related to privacy and civil liberties | • **ISO/IEC 27001** A.10 |
| | | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties | • **ISO/IEC 27001** A.8.1.1, A.6.1.2, A.6.1.6, A.10.8.2<br>• **NIST SP 800-53 Rev. 4** CP-2, IR-8 |
| | | **RS.CO-5:** Voluntary coordination occurs with external stakeholders (ex, business partners, information sharing and analysis centers, customers) | • **NIST SP 800-53 Rev. 4** PM-15, SI-5 |
| | **Analysis (AN):** Analysis is conducted to ensure adequate response and support recovery activities. | **RS.AN-1:** Notifications from the detection system are investigated | • **ISO/IEC 27001** A.6.2.1<br>• **NIST SP 800-53 Rev. 4** IR-4, IR-5, PE-6, SI-4, AU-13 |
| | | **RS.AN-2:** Understand the impact of the incident | • **ISO/IEC 27001** A.6.2.1<br>• **NIST SP 800-53 Rev. 4** CP-10, IR-4 |
| | | **RS.AN-3:** Forensics are performed | • **ISO/IEC 27001** A.13.2.2, A.13.2.3<br>• **NIST SP 800-53 Rev. 4** IR-4 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | | **RS.AN-4:** Incidents are classified consistent with response plans | • **ISO/IEC 27001** A.13.2.2<br>• **ISA 99.02.01** 4.3.4.5.6<br>• **NIST SP 800-53 Rev. 4** IR-4 |
| | **Mitigation (MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. | **RS.MI-1:** Incidents are contained | • **ISO/IEC 27001** A.3.6, A.13.2.3<br>• **ISA 99.02.01** 4.3.4.5.6<br>• **NIST SP 800-53 Rev. 4** IR-4 |
| | | **RS.MI-2:** Incidents are eradicated | • **ISA 99.02.01** 4.3.4.5.6, 4.3.4.5.10<br>• **NIST SP 800-53 Rev. 4** IR-4 |
| | **Improvements (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 | • **ISO/IEC 27001** A.13.2.2<br>• **ISA 99.02.01** 4.3.4.5.10, 4.4.3.4<br>• **NIST SP 800-53 Rev. 4** CP-2, IR-8 |
| | | **RS.IM-2:** Response strategies are updated | • **NIST SP 800-53 Rev. 4** CP-2, IR-8 |
| **RECOVER (RC)** | **Recovery Planning (RP):** Recovery processes and procedures are maintained and tested to ensure timely restoration of systems or assets affected by cybersecurity events. | **RC.RP-1:** Recovery plan is executed | • **COBIT** DSS02.05, DSS03.04<br>• **ISO/IEC 27001** A.14.1.3, A.14.1.4, A.14.1.5<br>• **NIST SP 800-53 Rev. 4** CP-10, CP-2<br>• **CCS CSC** 8 |
| | **Improvements (IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-1:** Plans are updated with lessons learned | • **ISA 99.02.01** 4.4.3.4<br>• **COBIT** BAI05.07<br>• **ISO/IEC 27001** 13.2.2<br>• **NIST SP 800-53 Rev. 4** CP-2 |
| | | **RC.IM-2:** Recovery strategy is updated | • **COBIT** APO05.04, BAI07.08<br>• **NIST SP 800-53 Rev. 4** CP-2 |
| | **Communications (CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet | **RC.CO-1:** Public Relations are managed | • **COBIT** MEA03.02<br>• **NIST SP 800-53 Rev. 4** IR-4, IR-8 |
| | | **RC.CO-2:** Reputation after an event is repaired | • **COBIT** MEA03.02 |

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. | | |

Informative References:

- ISA 99.02.01 (2009), Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FISA%2099.02.01-2009
- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103
- NIST Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org

478 For ease of use, each component of the Framework Core is given unique identifiers. Functions
479 and categories each have a unique two-character identifier, as shown in the Table 1 below.
480 Subcategories within each category are referenced numerically; the unique identifier for the
481 Subcategory is included in Table 2.
482
483 **Table 2: Function and Category Unique Identifiers**

484

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

# Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program

This appendix presents a methodology to address privacy and civil liberties considerations around the deployment of cybersecurity activities and in the protection of PII. This Privacy Methodology is based on the Fair Information Practice Principles (FIPPs) referenced in the Executive Order. It is organized by Function and Category to correspond with the Framework Core. Every Category may not be represented as not all Categories give rise to privacy and civil liberties risks.

**Table 3: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program**

| Function | Category | Methodology | Informative References |
|---|---|---|---|
| **IDENTIFY** | **Asset Management** | Identify PII of employees, customers, or other individuals that may be impacted by or connected to cybersecurity procedures, including PII that an organization processes or analyzes, or that may transit the organization's systems, even if the organization does not retain such information. | NIST SP 800-53 Rev. 4 Appendix J<br>• SE-1 Inventory of Personally Identifiable Information |
| | **Business Environment** | N/A | N/A |
| | **Governance** | Identify contractual, regulatory and legal, including Constitutional, requirements that cover:<br>i) PII identified under the Assets category; and<br>ii) Any cybersecurity measures that may implicate protected activities, for example, interception of electronic communications under the Electronic Communications Privacy Act, or other civil liberties considerations. | NIST SP 800-53 Rev. 4 Appendix J<br>• AP-1 Authority to Collect<br>• AP-2 Purpose Specification<br>• AR-1 Governance and Privacy Program<br>• AR-3 Privacy Requirements for Contractors and Service Providers |
| | | Identify policies and procedures that address privacy or PII management practices for the PII identified under the Assets category. In connection with the organization's cybersecurity procedures, assess whether or under which circumstances such policies and procedures:<br>I) provide notice to and enable consent by affected individuals regarding collection, use, dissemination, and maintenance of PII, as well as mechanisms for appropriate access, correction, and redress regarding use of PII;<br>ii) articulate the purpose or purposes for which the PII is intended to be used; | NIST SP 800-53 Rev. 4 Appendix J<br>• AP-2 Purpose Specification<br>• AR-1 Governance and Privacy Program<br>• AR-2 Privacy Impact and Risk Assessment<br>• AR-3 Privacy Requirements for Contractors and Service Providers<br>• AR-4 Privacy Monitoring and Auditing |

| Function | Category | Methodology | Informative References |
|---|---|---|---|
| | | iii) provide that collection of PII be directly relevant and necessary to accomplish the specified purpose(s) and that PII is only retained for as long as is necessary and permitted to fulfill the specified purpose(s);<br>iv) provide that use of PII be solely for the specified purpose(s) and that sharing of PII should be for a purpose compatible with the purpose for which the PII was collected; and<br>v) to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. | • AR-5 Privacy Awareness and Training<br>• AR-7 Privacy-Enhanced System Design and Development<br>• AR-8 Accounting of Disclosures<br>• IP-1 Consent<br>• IP-2 Individual Access<br>• IP-3 Redress<br>• IP-4 Complaint Management<br>• TR Transparency<br>• TR-1 Privacy Notice<br>• TR-3 Dissemination of Privacy Program Information<br>• UL-1 Internal Use<br>• UL-2 Information Sharing with Third Parties<br>• DI-1 Data Quality<br>• DM-1 Minimization of Personally Identifiable Information<br>• DM-2 Data Retention and Disposal<br>• DM-3 Minimization of PII Used in Testing, Training, and Research<br>ISO/IEC 29100 |
| | **Risk Assessment** | Identify whether there are threats and vulnerabilities around PII as an asset. For example, PII may be targeted as the primary commodity of value or it may be targeted as a means to access other assets within the organization. | NIST SP 800-53 Rev. 4 Appendix J<br>• SE-1 Inventory of Personally Identifiable Information<br>• AR-2 Privacy Impact and Risk Assessment<br>ISO/IEC 29100 |
| | **Risk Management Strategy** | Determine that processes identified under the Governance category that use of PII be solely for the specified purpose(s) are part of the organization's risk management strategy. | NIST SP 800-53 Rev. 4 Appendix J<br>• AP-2 Purpose Specification<br>• AR-1 Governance and Privacy Program |

| Function | Category | Methodology | Informative References |
|---|---|---|---|
| | | | • DM-1 Minimization of Personally Identifiable Information |
| **PROTECT** | **Access Control** | Limit the use and disclosure of PII to the minimum amount necessary to provide access to applications, services, and facilities. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-7 Privacy-Enhanced System Design and Development<br>• DM-1 Minimization of Personally Identifiable Information |
| | **Awareness and Training** | Senior executive support is critical for building a cybersecurity culture that is respectful of privacy and civil liberties. Assign responsibility to designated personnel to implement and provide oversight for privacy policies and practices designed to minimize the impact of cybersecurity activities on privacy and civil liberties. Have regular training for employees and contractors on following such policies and practices. Make users aware of the steps they can take to protect their PII and the content of their communications, and increase transparency around privacy impacts and security practices. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy Program<br>• AR-2 Privacy Impact and Risk Assessment<br>• AR-3 Privacy Requirements for Contractors and Service Providers<br>• AR-4 Privacy Monitoring and Auditing<br>• AR-5 Privacy Awareness and Training<br>• AR-6 Privacy Reporting<br>ISO/IEC 29100 |
| | **Data Security** | Implement appropriate safeguards at all stages of PII's lifecycle within the organization and proportionate to the sensitivity of the PII to protect against loss, theft, unauthorized access or acquisition, disclosure, copying, use, or modification. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-4 Privacy Monitoring and Auditing<br>• AR-7 Privacy-Enhanced System Design and Development<br>• AR-8 Accounting of Disclosures<br>• DM-1 Minimization of Personally Identifiable Information<br>• DM-2 Data Retention and Disposal<br>• DM-3 Minimization of PII Used in Testing, Training, and Research |
| | **Information Protection Processes and** | Securely dispose of, de-identify, or anonymize PII that is no longer needed. Regularly audit stored PII and the need for its | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy |

| Function | Category | Methodology | Informative References |
|---|---|---|---|
| | **Procedures** | retention. Have policies and procedures in place to protect data and communications as appropriate according to the law during incidents and investigations handled jointly with law enforcement/government agencies. | Program<br>• AR-2 Privacy Impact and Risk Assessment<br>• DM-1 Minimization of Personally Identifiable Information<br>• DM-2 Data Retention and Disposal<br>ISO/IEC 29100 |
| | **Protective Technology** | Audit access to databases containing PII. Consider whether PII is being logged as part of an independent audit function, and how such PII could be minimized while still implementing the cybersecurity activity effectively. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-4 Privacy Monitoring and Auditing<br>• DM-1 Minimization of Personally Identifiable Information |
| **DETECT** | **Anomalies and Events** | When detecting anomalies and events, regularly review the scope of detection and filtering methods to minimize the collection or retention of PII and communications content that is not necessary to detecting the cybersecurity event. Have policies so that any PII that is collected, used, disclosed, or retained is accurate and complete. | NIST SP 800-53 Rev. 4 Appendix J<br>• DI-1 Data Quality<br>• DM-1 Minimization of Personally Identifiable Information<br>• DM-3 Minimization of PII Used in Testing, Training, and Research<br>• UL-1 Internal Use<br>• UL-2 Information Sharing with Third Parties |
| | **Security Continuous Monitoring** | When performing monitoring that involves individuals or PII, regularly evaluate the effectiveness of procedures and tailor the scope to produce minimally intrusive methods of monitoring. Provide transparency into the practices. | NIST SP 800-53 Rev. 4 Appendix J<br>• DM-1 Minimization of Personally Identifiable Information<br>• DM-3 Minimization of PII Used in Testing, Training, and Research<br>• UL-1 Internal Use<br>• UL-2 Information Sharing with Third Parties |
| | **Detection Processes** | Establish a process to coordinate privacy personnel participation in the review of policy compliance and enforcement for detect activities. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy Program |

| Function | Category | Methodology | Informative References |
|---|---|---|---|
| | | | • AR-2 Privacy Impact and Risk Assessment<br>• AR-3 Privacy Requirements for Contractors and Service Providers<br>• AR-4 Privacy Monitoring and Auditing<br>• AR-5 Privacy Awareness and Training<br>• AR-7 Privacy-Enhanced System Design and Development<br>• AR-8 Accounting of Disclosures<br>ISO/IEC 29100 |

| Function | Category | Methodology | Informative References |
|---|---|---|---|
| **RESPOND** | **Response Planning** | Distinguish between an incident that puts PII at risk and one for which the organization will use PII to assist in responding to the incident. An organization may need to take different steps in its response plan depending on such differences. For example, when PII is at risk, an organization may need to consider which security activities to perform, whereas when PII is used for response, an organization may need to consider how to minimize the use of PII to protect an individual's privacy or civil liberties. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy Program<br>• AR-2 Privacy Impact and Risk Assessment<br>• AR-4 Privacy Monitoring and Auditing<br>• AR-5 Privacy Awareness and Training<br>• SE-2 Privacy Incident Response<br>• IR-1 Incident Response Policy and Procedures<br>• IR-2 Incident Response Training<br>• IR-3 Incident Response Testing<br>• IR-4 Incident Handling<br>• IR-5 Incident Monitoring<br>• IR-6 Incident Reporting<br>ISO/IEC 29100 |
| | **Communications** | Understand any mandatory obligations for reporting breaches of PII. When voluntarily sharing information about cybersecurity incidents, limit disclosure of PII or communications content to that which is necessary to describe or mitigate the incident. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy Program<br>• AR-7 Privacy-Enhanced System Design and Development<br>• AR-8 Accounting of Disclosures<br>• DM-1 Minimization of Personally Identifiable Information |
| | **Analysis** | When performing forensics, only retain PII or communications content that is necessary to the investigation. Have policies so that any PII that is collected, used, disclosed, or retained is accurate and complete. | NIST SP 800-53 Rev. 4 Appendix J<br>• DM-1 Minimization of Personally Identifiable Information<br>• DM-2 Data Retention and Disposal<br>• DM-3 Minimization of PII Used in Testing, Training, and Research<br>• DI-1 Data Quality |

| Function | Category | Methodology | Informative References |
|---|---|---|---|
| | **Mitigation** | When considering methods of incident containment, assess the impact on individuals' privacy and civil liberties, particularly for containment methods that may involve the closure of public communication or data transmission systems. Provide transparency concerning such methods. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy Program<br>• AR-2 Privacy Impact and Risk Assessment<br>• AR-7 Privacy-Enhanced System Design and Development<br>• SE-2 Privacy Incident Response<br>ISO/IEC 29100 |
| | **Improvements** | When considering improvements in responding to incidents involving PII, distinguish whether the incident put PII at risk, whether the organization used PII in responding to the incident, or whether the executed response plan may have otherwise impacted privacy or civil liberties. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy Program<br>• AR-2 Privacy Impact and Risk Assessment<br>• AR-4 Privacy Monitoring and Auditing<br>• AR-5 Privacy Awareness and Training<br>• AR-7 Privacy-Enhanced System Design and Development<br>• AR-8 Accounting of Disclosures<br>• SE-2 Privacy Incident Response<br>ISO/IEC 29100 |
| **RECOVER** | **Recovery Planning** | Distinguish between an incident that puts PII at risk and one for which the organization will use PII to assist in recovering from the incident. An organization may need to take different steps in its recovery plan depending on such differences. For example, when PII is at risk, an organization may need to consider which security activities to perform, whereas when PII is used for recovery, an organization may need to consider how to minimize the use of PII to protect an individual's privacy or civil liberties. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy Program<br>• AR-2 Privacy Impact and Risk Assessment<br>• AR-4 Privacy Monitoring and Auditing<br>• AR-7 Privacy-Enhanced System Design and Development<br>• AR-8 Accounting of Disclosures |

| Function | Category | Methodology | Informative References |
|---|---|---|---|
| | | | • SE-2 Privacy Incident Response<br>• DM-1 Minimization of Personally Identifiable Information<br>ISO/IEC 29100 |
| | **Improvements** | When considering improvements in recovering from incidents involving PII, distinguish whether the incident put PII at risk, whether the organization used PII in recovering from the incident, or whether the executed recovery plan may have otherwise impacted privacy or civil liberties. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-1 Governance and Privacy Program<br>• AR-2 Privacy Impact and Risk Assessment<br>• AR-4 Privacy Monitoring and Auditing<br>• AR-8 Accounting of Disclosures<br>• IP-4 Complaint Management<br>• SE-2 Privacy Incident Response<br>ISO/IEC 29100 |
| | **Communications** | Communicate the use or disclosure of PII as part of the incident and any risk mitigation strategies to maintain or rebuild trust with affected individuals, relevant stakeholders, or the wider public. | NIST SP 800-53 Rev. 4 Appendix J<br>• AR-8Accounting of Disclosures<br>• IP-4 Complaint Management<br>• SE-2 Privacy Incident Response<br>• TR-1 Privacy Notice<br>• TR-3 Dissemination of Privacy Program Information |

492

# Appendix C: Areas for Improvement for the Cybersecurity Framework

Executive Order 13636 states that the Cybersecurity Framework will "identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations." Based on stakeholder input, several high-priority Areas for Improvement are currently identified. These initial Areas for Improvement provide a roadmap for stakeholder collaboration and cooperation to further understand and/or develop new or revised standards. The initial areas for improvement are as follows:

- Authentication
- Automated Indicator Sharing
- Conformity Assessment
- Cybersecurity Workforce
- Data Analytics
- International Aspects, Impacts, and Alignment
- Privacy Standards
- Supply Chains Risk Management

This is not intended to be an exhaustive list, but these are highlighted as important areas that should be addressed in future versions of the Framework.

These Areas for Improvement require continued focus; they are important but evolving areas that have yet to be developed or require further research and understanding. While tools, methodologies, and standards exist for some of the areas, they need to become more mature, available, and widely adopted. To address the Areas for Improvement the community must identify primary challenges, solicit input from stakeholders to address those identified challenges, and collaboratively develop and execute action plans for addressing the challenges.

## C.1 Authentication

Authentication challenges continue to exist across the critical infrastructure. As a result, inadequate authentication solutions are a commonly exploited vector of attack by adversaries. Multi-Factor Authentication can assist in closing these attack vectors by requiring individuals to augment passwords ("something you know") with "something you have," such as a token, or "something you are," such as a biometric.

While new solutions continue to emerge, there is only a partial framework of standards to promote security and interoperability. In addition, usability has remained a significant challenge for many control systems, as many of the solutions that are available today in the marketplace are for standard computing platforms. Moreover, many solutions are geared only toward identification of individuals; there are fewer standards-based approaches for automated device authentication.

The inadequacy of passwords to fulfill authentication needs was a key driver behind the 2011 issuance of the National Strategy for Trusted Identities in Cyberspace (NSTIC), which calls upon the private sector to collaborate on development of an Identity Ecosystem that raises the level of

trust associated with the identities of individuals, organizations, networks, services, and devices online. While NSTIC is heavily focused on consumer use cases, the standards and policies that emerge from the private sector-led Identity Ecosystem Steering Group (IDESG) established to support the NSTIC can inform advances in authentication for critical infrastructure going forward.

## C.2 Automated Indicator Sharing

The automated sharing of indicator information is an important tool to provide organizations with timely, actionable information that they can use to detect and respond to cybersecurity events as they are occurring. Current sharing communities use a combination of standard and proprietary mechanisms to exchange indicators. These mechanisms have differing strengths and weaknesses. Standard approaches must be developed that incorporate successful practices to enable sharing within and among sectors. This shared subset of indicators needs to allow for extraction of indicator data as part of the analysis of cybersecurity incidents, sharing of data that does not expose the organization to further risks, and automated action by receiving organizations. When indicators are received by an organization, security automation technologies should be able to detect past attacks, identify compromised systems, and support the detection of future attacks.

## C.3 Conformity Assessment

Industry has a long history of developing conformity assessment programs to meet society's needs. For example, the independent non-profit, Snell Memorial Foundation that was established in 1957 tests and certifies helmets used in motor sports for conformity to safety performance standards. Snell's conformity assessments are recognized by many U.S. racing associations.

An organization can use conformity assessment activities to assess the implementation of requirements related to managing cybersecurity risk. The output of conformity assessment activities can enhance an organization's understanding of its implementation of a Framework profile. The decisions on the type, independence, and technical rigor of conformity assessment should be risk-based. The need for confidence in conformity assessment activities must be balanced with cost to the private and public sectors, including direct program costs, time-to-market delays, diverse global requirements, additional legal obligations, and the cost of non-conformity in the market. Successful conformity assessment provides the needed level of confidence, is efficient, and has a sustainable and scalable business case. Critical infrastructure's evolving implementation of Framework profiles should drive the identification of private sector conformity assessment activities that address the confidence and information needs of stakeholders.

## C.4 Cybersecurity Workforce

A skilled cybersecurity workforce is necessary to meet the unique cybersecurity needs of critical infrastructure. While it is widely known that there is a shortage of general cybersecurity experts, there is also a shortage of qualified cybersecurity experts with an understanding of the specific challenges posed to critical infrastructure. As the critical infrastructure threat and technology landscape evolves, the cybersecurity workforce must continue to adapt to design, develop, implement, maintain and continuously improve the necessary practices within critical infrastructure environments.

Efforts such as the National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) and the National Initiative for Cybersecurity Education (NICE) are currently creating the underpinnings of a cybersecurity workforce for the future, and establishing an operational, sustainable and continually improving cybersecurity education program to provide a pipeline of skilled workers for the private sector and government. While progress has been made through these and other programs, greater attention is needed to help organizations understand their current and future cybersecurity workforce needs, and to develop hiring, acquisition, and training resources to raise the level of technical competence of those who build, operate, and defend systems delivering critical infrastructure services.

## C.5 Data Analytics

Big data and the associated analytic tools coupled with the emergence of cloud, mobile, and social computing offer opportunities to process and analyze structured and unstructured cybersecurity-relevant data on an unprecedented scale and specificity. Issues such as situational awareness of complex networks and large-scale infrastructures can be addressed. Additionally, the analysis of complex behaviors in these large scale-systems can also address issues of provenance, attribution, and discernment of attack patterns.

For the extraordinary potential of analytics to be realized, several challenges must be overcome—for example, the lack of taxonomies of big data; mathematical and measurement foundations; analytic tools; measurement of integrity of tools; and correlation and causation. Additionally, there are privacy implications in the use of these analytic tools, such as data aggregation and PII that must be addressed for legal and public confidence reasons.

## C.6 International Aspects, Impacts, and Alignment

Globalization and advances in technology have benefited governments, economies, and society as a whole, spawning unparalleled increases in innovation, competitiveness, and economic growth. However, the functioning of the critical infrastructure has become dependent on these enabling technologies, spurring governments around the globe to view cybersecurity increasingly as a national priority. Many governments are proposing and enacting strategies, policies, laws, and regulations covering a wide range of issues and placing varying degrees of requirements on organizations. As many organizations, and most sectors, operate globally or rely on the interconnectedness of the global digital infrastructure, many of the requirements are affecting, or may affect, how organizations operate and conduct business. Diverse and unique requirements can impede interoperability, produce duplication, harm cybersecurity, and hinder innovation, significantly reducing the availability and use of innovative technologies to critical infrastructures in all industries. This ultimately hampers the ability of critical infrastructure organizations to operate globally and to effectively manage new and evolving risk. The Framework is designed to allow for the use of international standards that can scale internationally.

## C.7 Privacy Standards

The FIPPs are a set of guidelines for evaluating and mitigating privacy impacts around the collection, use, disclosure, and retention of PII. They are the basis for a number of laws and regulations, as well as various sets of privacy principles and frameworks, including the Privacy

Methodology in Appendix B. Although the FIPPs provide a process for how PII should be treated, they do not provide specific implementation methods or best practices. For example, in Appendix B in RS.CO, it indicates that "When voluntarily sharing information about cybersecurity incidents, limit disclosure of PII or communications content to that which is necessary to describe or mitigate the incident." This concept maps to certain privacy controls in NIST 800-53 Rev. 4, Appendix J, however, there is no identified standard or best practice for a consistent way to distinguish between necessary and unnecessary PII, such as a format standard. Thus, while the Framework Core includes a broad set of informative references, the range of informative references for the Privacy Methodology is limited.

This lack of standardization, and supporting privacy metrics, makes it difficult to assess the effectiveness of organizational implementation methods. Furthermore, organizational policies are often designed to address business risks that arise out of privacy violations, such as reputation or liability risks, rather than focusing on minimizing the risk of harm to individuals. Although research is being conducted in the public and private sectors to improve current privacy practices, many gaps remain. There are few identifiable standards or best practices to mitigate the impact of cybersecurity activities on individuals' privacy and civil liberties.

## C.8 Supply Chain Risk Management

All organizations are part of, and dependent upon, product and service supply chains. Supply chains consist of organizations that design, make, source, and deliver products and services. Disruptions in one part of the supply chain may have a cascading and adverse impact on organizations throughout the supply chain, both up and downstream, and across multiple sectors and subsectors. Although many organizations have robust internal risk management processes, there remain challenges related to criticality and dependency analysis, collaboration, information sharing, and trust mechanisms throughout the supply chain. As a result, organizations continue to struggle to identify their risks and prioritize their actions due to these operational dependencies and the weakest links are susceptible to penetration and disruption. Supply chain risk management, particularly in terms of product and service integrity, is an emerging discipline characterized by diverse perspectives, disparate bodies of knowledge, and fragmented standards and best practices.

# Appendix D: Framework Development Methodology

This Framework was developed in response to Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*[4] and in a manner that is consistent with NIST's mission to promote U.S. innovation and industrial competitiveness.

Initially, NIST issued a Request for Information (RFI) in February 2013 to gather relevant input from industry and other stakeholders, and asking stakeholders to participate in the Cybersecurity Framework development process.[5] The process was designed to identify existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities. NIST shared publicly the 245 responses to the RFI.[6] NIST conducted an analysis of these comments, and shared initial findings on May 15, 2013. [7]

On April 3, 2013 NIST hosted an initial workshop in Washington D.C. to identify existing resources and gaps, and prioritize issues to be addressed as part of the Framework.[8]

At a second workshop hosted by Carnegie Mellon University, NIST worked with stakeholders to discuss the foundations of the Framework and the initial analysis.[9] The feedback from the second workshop led to the development of a draft outline of the Preliminary Framework presented on July 1, 2013.[10]

At a third workshop hosted by the University of California, San Diego,[11] the draft outline was presented for validation and stakeholders contributed input to the Framework Core, which was also shared publicly on July 1st.[12]

At the fourth workshop hosted by the University of Texas at Dallas, the discussion draft of the Preliminary Framework was presented for stakeholder input.

Through the processes, with NIST as a convener and coordinator, the following goals were developed for the Framework:

- Be an adaptable, flexible, and scalable tool for voluntary use;
- Assist in assessing, measuring, evaluating, and improving an organization's readiness to deal with cybersecurity risk;
- Be actionable across an organization;
- Be prioritized, flexible, repeatable, performance-based, and cost-effective;
- Rely on standards, methodologies, and processes that align with policy, business, and technological approaches to cybersecurity;

---

4 http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

5 https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity

6 http://csrc.nist.gov/cyberframework/rfi_comments.html

7 http://csrc.nist.gov/cyberframework/nist-initial-analysis-of-rfi-responses.pdf

8 http://www.nist.gov/itl/csd/cybersecurity-framework-workshop.cfm

9 http://www.nist.gov/itl/csd/cybersecurity-framework-workshop-may-29-31-2013.cfm

10 http://www.nist.gov/itl/upload/draft_outline_preliminary_framework_standards.pdf

11 http://www.nist.gov/itl/csd/3rd-cybersecurity-framework-workshop-july-10-12-2013-san-diego-ca.cfm

12 http://www.nist.gov/itl/upload/draft_framework_core.pdf

- Complement rather than conflict with current regulatory authorities;
- Promote, rather than constrain, technological innovation in this dynamic arena;
- Focus on outcomes;
- Raise awareness and appreciation for the challenges of cybersecurity but also the means for understanding and managing the related risks;
- Be consistent with voluntary international standards.

# Appendix E: Glossary

This appendix defines selected terms used in the publication.

**Category:** The subdivision of a Function into groups of cybersecurity activities, closely tied to programmatic needs. 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 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 reduce cybersecurity risk composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile. Also known as the "Cybersecurity Framework."

**Framework Core:** An outcome-based compilation of cybersecurity activities and references that are common across critical infrastructure sectors. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

**Framework Implementation Tier:** The degree to which an organization's cybersecurity risk management practices exhibit selected desirable characteristics, such as being risk and threat aware, repeatable, and adaptive.

**Framework Profile:** A representation of the outcomes that a particular system or organization has achieved or is expected to achieve as specified in the Framework Categories and Subcategories.

**Function:** One of the main components of the Framework. Functions provide the highest level of structure for organizing cybersecurity activities into Categories and Subcategories. The five functions are: Identify, Protect, Detect, Respond, and Recover.

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

**Informative Reference:** A specific section of existing standards and practices that are common among all critical infrastructure sectors and illustrate a method to accomplish the activities within each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10 - Cryptographic technology, which supports the "Protect Data in Transit" Subcategory of the "Data Security" Category in the "Protect" function.

**Personally Identifiable Information (or PII)**: Information which can be used to distinguish or trace an individual's identity such as the individual's name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

**Protect (function):** Develop and implement the appropriate safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure services.

**Recover (function):** Develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the appropriate capabilities that were impaired through a cybersecurity event.

**Respond (function):** Develop and implement the appropriate activities, prioritized through the organization's risk management process (including effective planning), 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 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.

**Subcategory:** The subdivision of a Category into high-level outcomes. Examples of subcategories include "Physical devices and systems within the organization are catalogued," "Data-at-rest is protected," and "Notifications from the detection system are investigated."

# Appendix F: Acronyms

This appendix defines selected acronyms used in the publication.

| | |
|---|---|
| **CCS** | Council on CyberSecurity |
| **COBIT** | Control Objectives for Information and Related Technology |
| **DHS** | Department of Homeland Security |
| **EO** | Executive Order |
| **FIPPs** | Fair Information Practice Principles |
| **ICS** | Industrial Control Systems |
| **IDESG** | Identity Ecosystem Steering Group |
| **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 |
| **NSTIC** | National Strategy for Trusted Identities in Cyberspace |
| **OT** | Operational Technology |
| **PII** | Personally Identifiable Information |
| **RFI** | Request for Information |
| **RMP** | Risk Management Process |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SP** | Special Publication |