1

Discussion Draft of the Preliminary Cybersecurity Framework

DRAFT

August 28, 2013

A *Discussion Draft of the Preliminary Cybersecurity Framework* for improving critical infrastructure cybersecurity is now available for review. This draft is provided by the National Institute of Standards and Technology (NIST) in advance of the Fourth Cybersecurity Framework workshop on Sept.11-13, 2013, at the University of Texas at Dallas. Participants are asked to read the Note to Reviewers and review this draft in advance of the workshop.

Note to Reviewers

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 challenges. The National Institute of Standards and Technology (NIST) requests that reviewers consider the following questions:

How can 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 board 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?

Will the Discussion Draft, as presented:

- be inclusive of, and not disruptive to, effective cybersecurity practices in use today?
- enable organizations to incorporate threat information?

Is the Discussion Draft:

- presented at the right level of specificity?
- sufficiently addressing unique privacy and civil liberties needs for critical infrastructure?

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.

DRAFT

Table of Contents

List of Figures

List of Tables

DRAFT

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, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" on February 12, 2013.[1] This directive calls for the development of a 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.[2]

The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk, in a manner similar to financial, safety, and operational risk.[3] The Framework is not a one-size-fits-all approach for all critical infrastructure organizations. Because each organization's risk is unique, along with their implementation of information technology (IT) and operational technology (OT), the implementation of the Framework will vary.

The focus of the Framework is to support the improvement of cybersecurity for the Nation's Critical Infrastructure using industry-known standards and best practices.[4] The Framework provides a common language and mechanism for organizations to: 1) describe 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.

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 cybersecurity risk management. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference when establishing one.

1.1 Overview of the Framework

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

- The *Framework Core* is a compilation of cybersecurity activities and references that are common across critical infrastructure sectors. The Core presents standards and best practices in a manner that allows for communication and risk management across the organization from the senior executive level to the implementation/operations level. The

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

[2] The Executive Order defines critical infrastructure 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."

[3] Appendix D presents the methodology that was used to develop the Cybersecurity Framework based on stakeholder engagement and input.

[4] To assist those organizations that rely on existing processes, the Framework Core in Appendix A provides mappings to commonly-used security control catalogs.

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 then identifies underlying key Categories and Subcategories for each of these Functions, and matches them with Informative References such as existing standards, guidelines, and practices for each Subcategory. For instance, for the "Protect" Function, categories include: Data Security; Access Control; Awareness and Training; and Protective Technology. At the next level down, 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.

- *Framework Implementation Tiers* ("Tiers") demonstrate the implementation of the Framework Core Functions and Categories and indicate how cybersecurity risk is managed. These Tiers range from Partial (Tier 0) to Adaptive (Tier 3), with each Tier building on the previous Tier.

- A *Framework Profile* ("Profile") conveys how an organization manages cybersecurity risk in each of the Framework Core Functions and Categories by identifying the Subcategories that are implemented or planned for implementation. Profiles are also used to identify the appropriate goals for an organization or for a critical infrastructure sector and to assess progress against meeting those goals.

1.2 Risk Management and the Cybersecurity Framework

While not a risk management process itself, the Framework enables the integration of cybersecurity risk management into the organization's overall risk management process.[5] The Framework fosters:

- Cybersecurity risk management approaches that take into account the interaction of multiple risks;
- Cybersecurity risk management approaches that address both traditional information technology and operational technology (industrial control systems);
- Cybersecurity risk management practices that encompass the entire organization, exposing dependencies that often exist within large, mature, and/or diverse entities, and with the interaction between the entities and their partners, vendors, suppliers, and others;
- Cybersecurity risk management practices that are internalized by the organization to ensure that decision making is conducted by a risk-informed process of continuous improvement; and
- Cybersecurity standards that can be used to support risk management activities.

Within the Nation's Critical Infrastructure, organizations vary widely in their business models, risk tolerance, approaches to risk management, and effects on security, national economic security, and national public health or safety. Profiles are the result of organizations, large or

[5] Some actions, such as "Inventory and track physical devices and systems within the organization", are basic and necessary for practically all organizations. Other actions are potentially more costly and are usually only implemented when a risk assessment indicates that they are necessary.

small, implementing a cybersecurity risk management process that aligns with their business mission and objectives.

1.3 Document Overview

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

- Section 2 describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- Section 3 presents examples of how the Framework can be used.
- Section 4 discusses areas for improvement in cybersecurity standards, practices, etc. identified as a result of the Framework efforts to date.
- 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.
- Appendix C describes the Framework development methodology.
- Appendix D contains a glossary of selected terms.
- Appendix E lists acronyms used in this document.

DRAFT

2.0 Framework Basics

The Framework provides a common language for expressing, understanding, and managing cybersecurity risk, both internally and externally. The Framework helps 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 individuals, organizations, and associations — can use the Framework to create one or more Profiles. These Profiles draw from the Functions, Categories, Subcategories, and Tiers.

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 types of 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** provide the highest level of structure, for organizing cybersecurity activities into Categories and Subcategories. These Functions are: Identify, Protect, Detect, Respond, and Recover.
- **Categories** are the subdivisions of a Function into groups of cybersecurity activities, more closely tied to programmatic needs. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."
- **Subcategories** further subdivide a Category into high-level tactical activities to support technical implementation. Examples of subcategories include "Inventory and track physical devices and systems within the organization," "Protect network integrity by segregating networks/implementing enclaves (where appropriate)," and "Assess the impact of detected cybersecurity events to inform response and recovery activity."
- **Informative References** are specific sections of standards 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, and organizations are free to implement other standards, guidelines, and practices.[6]

See **Appendix A** for the complete Framework Core listing. In addition, **Appendix B** provides an initial methodology to address privacy and civil liberties considerations around the deployment of cybersecurity activities.

The five Framework Core Functions defined below apply to both traditional information technology and operational technology.

- **Identify** – Develop the institutional understanding of which organizational systems, assets, data, and capabilities need to be protected, determine priority in light of organizational mission, and establish processes to achieve risk management goals.
- **Protect** – Develop and implement the appropriate safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[7]
- **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.

[6] The Compendium 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.

[7] A cybersecurity event is a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

- **Recover** – 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.

2.2 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") reflect how an organization implements the Framework Core functions and categories and manages its risk. Section 2.3 provides additional information on how the Tiers apply to the Framework Core. The Tiers are progressive, ranging from Partial (Tier 0) to Adaptive (Tier 3), with each Tier building on the previous Tier. A Tier represents the stage of the implementation of the Framework Profile and the organization's cybersecurity risk management process. The Tier characteristics are defined at the organizational level. These characteristics are applied to the Framework Core to determine how a category is implemented. The Tier definitions follow:

- **Tier 0: Partial** – The organization has not yet implemented a formal, threat-aware risk management process to determine a prioritized list of cybersecurity activities. The organization may implement some portions of the Framework on an irregular, case-by-case basis due to varied experience or information gained from outside sources. An organization at Tier 0 might not have the processes in place to share cybersecurity information internally between its organizational layers and might not have the processes in place to participate in coordination or collaboration with other entities.

- **Tier 1: Risk-Informed** – The organization uses a formal, threat-aware risk management process to develop a Profile of the Framework. In addition, risk-informed, management-approved processes and procedures are defined and implemented and staff has adequate resources to perform their cybersecurity duties. The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

- **Tier 2: Repeatable** – The organization updates its Profile based on regular application of its risk management process to respond to a changing cybersecurity landscape. Risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. The organization will also have consistent methods in place to provide updates when a risk change occurs. Personnel have adequate knowledge and skills to perform their defined roles and responsibilities. The organization understands its dependencies and partners and can consume information from these partners to help prevent and improve its reaction to events.

- **Tier 3: Adaptive** – The organization updates its Profile based on predictive indicators derived from previous and anticipated cybersecurity activities. These updates to the Profile enable the organization to actively adapt to a changing cybersecurity landscape and emerging/evolving threats. Risk-informed policies, processes, and procedures are part of the organizational culture and evolve from previous activities (and from information shared by other sources) to predict and address potential cybersecurity events. 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.

DRAFT

Organizations should determine the desired Tiers at the Category level, ensuring that the selected levels meet the organizational goals, reduce cybersecurity risk to critical infrastructure, and are feasible to implement. External guidance will be helpful, such as information that could be obtained from the Department of Homeland Security (DHS), an Information Sharing and Analysis Center (ISAC), or other sources. The Framework implementer selects the appropriate Categories and target Tiers through the use of the Profile.

2.3 Framework Profile

A Framework Profile ("Profile") enables organizations to establish a roadmap for reducing cybersecurity risk that is well-aligned with organization and sector goals, considers legal/regulatory requirements, 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: Target and Current. The Target Profile indicates the cybersecurity goal state, and the Current Profile indicates the current state.

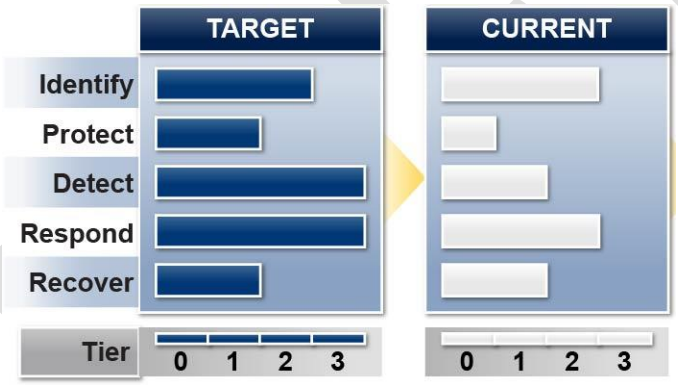

Figure 2: Profile Comparisons

Figure 3 shows the basic steps involved in Target Profile creation.

Figure 3: Target Profile Creation Process

The Profile is the selection of the Functions, Categories, and Subcategories that are aligned with the business requirements, risk tolerance, and resources of the organization. The Target Profile should support business/mission requirements and aid in the communication of risk within and between organizations. Identifying the gaps between the Current Profile and the Target Profile allows the creation of a roadmap that organizations should implement to reduce cybersecurity risk.

The Framework provides a mechanism for organizations, sectors, and other entities to create their own Target Profiles. It does not provide Target Profile templates, nor does it identify Tier

requirements that an organization should meet. In the future, organizations should identify existing Target Profiles that could be customized for their purposes and needs.

2.4 Putting It Together

Figure 4 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. This figure depicts the overall Framework usage and where Profiles fit in.

Starting at the top of the figure and proceeding clockwise, 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. Implementation of the Profile is communicated by the implementation/operations level to the business/process level, where an impact assessment is made. The outcomes of that impact assessment are reported to the senior executive level to inform the organization's overall risk management process.

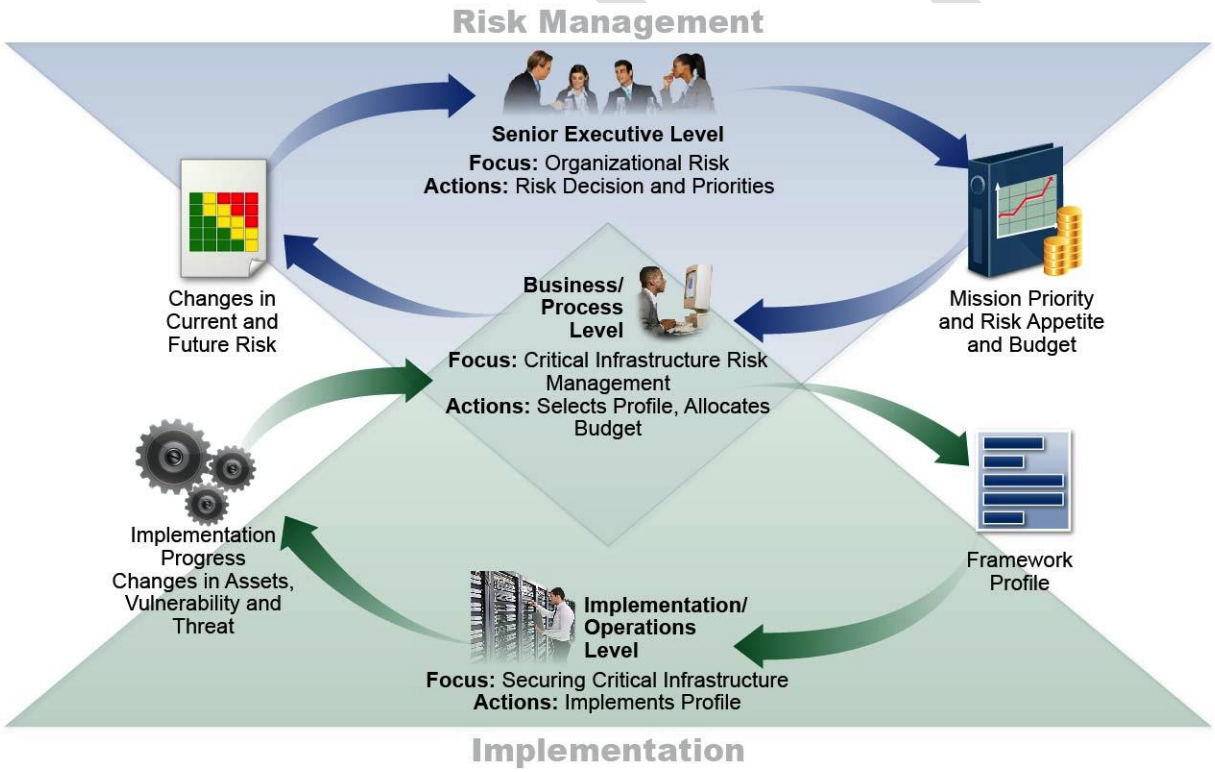

Figure 4: Notional Information and Decision Flows within an Organization

3.0 How to Use the Framework

The Framework structure is designed to support existing aspects of business operations, and can be used as the basis for creating a new cybersecurity program for an organization that does not already have one. The following examples provide several options for using the Framework.

3.1 Establishing or Improving a Cybersecurity Program

An organization should use the Framework as the basis for establishing a new cybersecurity program or improving an existing cybersecurity program. First, the organization uses its risk management process to create a Target Profile that reflects the desired Tiers for each selected Category, and then assesses its cybersecurity posture as a Current Profile. The organization uses the Target Profile to assess progress, making adjustments to it as needed to reflect ongoing changes in risk. Used in this way, the Profiles are a helpful organizational tool for improving cybersecurity within an organization.

The following is an example illustrating how an organization may use the Framework to create or improve a cybersecurity program. Organizations should communicate effectively with pertinent organizational levels when meaningful information becomes available.

Step 1: Make Organization Wide Decisions. The senior executive level clearly communicates high-level understanding of business/mission drivers, regulatory requirements, and overall risk posture to those developing the organization's Framework Profile, to ensure the appropriate selection of Categories and Tiers. They provide business objectives and risk tolerance guidance to the business/process level to inform effective decision making that supports the organization's priorities.

Step 2: Establish a Target Profile. With an understanding of the priorities and constraints within their organization, the business/process level creates a Target Profile that considers both internal and external factors. When selecting the Profile for their areas of responsibility, the business/process level considers the level of cybersecurity needed to achieve the objectives determined in Step 1. Risk and priority information, provided by the senior executive level, allows the business/process level to invest resources in a manner that increases cybersecurity and supports the broader strategic direction.

Step 3: Establish a Current Profile. The business/process level assesses the current cybersecurity state of the organization by establishing a Current Profile, based on the Categories included in the Target Profile.

Step 4: **Compare Target and Current Profiles.** Once the Target and Current Profiles have been established, the business/process level compares the Target Profile to the Current Profile. The differences between the Tiers of the Profiles indicate areas for improvement or areas of where resources could be reallocated to address other parts of the Profile. The utilization of Current Profiles and Target Profiles help the business/process level to make informed decisions about cybersecurity activities and streamline improvement.

Step 5: Implement Target Profile. The implementation/operations level is responsible for the implementation and ongoing monitoring of the cybersecurity activities identified as outcomes of Step 4. For further guidance, the Framework identifies Informative References regarding the practices described in the Categories and Subcategories.

3.2 Communicating Cybersecurity Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent partners responsible for the delivery of critical infrastructure. 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, Subcategories and Tiers that will ensure the appropriate level of resilience.
- A critical infrastructure sector may establish a baseline Target Profile.

3.3 Identifying Gaps

The Framework can be used to identify gaps where additional Informative References would help organizations implement technologies or better 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, guidance, and practices to address the needs of potential adopters.

DRAFT

4.0 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 have been identified. Collaboration and cooperation must increase for these areas to further understanding and/or the development of new or revised standards. The initial Areas for Improvement are as follows:

- Authentication
- Automated Indicator Sharing
- Conformity Assessment
- Data Analytics
- International Aspects, Impacts, and Alignment
- Privacy
- Supply Chains and Interdependencies

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.

4.1 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 (MFA) 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 privately-led Identity Ecosystem Steering Group (IDESG) established to

support the NSTIC can inform advances in authentication for critical infrastructure going forward.

4.2 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 historic attacks, identify compromised systems, and support the detection of future attacks.

4.3 Conformity Assessment

Industry has a long history of developing conformity assessment programs to meet society's needs. 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.

4.4 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 in a forward-looking basis.

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.

4.5 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 effectively manage new and evolving risk. The Framework has been designed to allow for the use of international standards that can scale internationally.

4.6 Privacy

The Fair Information Practice Principles (FIPPs) are a longstanding framework for evaluating and mitigating privacy impacts around the collection, use, disclosure, and retention of personally identifiable information (PII). They are the basis for a number of laws and regulations, as well as various sets of privacy principles and frameworks. Although the FIPPs provide a process for how PII should be treated, they do not provide standardized guidance on implementation methods or best practices. This lack of standardization 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.

4.7 Supply Chains and Interdependencies

Although many organizations have robust internal risk management processes, there remain challenges related to collaboration, information sharing, and trust mechanisms throughout the supply chain. As a result, the weakest links are susceptible to penetration and disruption, affecting the overall supply chain. 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.

Similar to global supply chains, all critical infrastructures have sector and subsector interdependencies. Disruptions in one sector may have a cascading and adverse impact on the operations of another. Impacts on one sector can also provide advanced warning of potential risks to another. While some dependencies are readily apparent, others are not and many organizations continue to struggle to identify their risks and prioritize their actions due to these operational interdependencies.

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 Categories, 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):** Identify and manage the personnel, devices, systems, and facilities that enable the organization to achieve business purposes, including their relative importance to business objectives, in support of effective risk decisions.	**ID.AM-1**: Inventory and track physical devices and systems within the organization	• **ISA 99.02.01** 4.2.3.4 • **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05 • **ISO/IEC 27001** A.7.1.1, A.7.1.2 • **NIST SP 800-53 Rev. 4** CM-8 • **CCS CSC**1
		ID.AM-2: Inventory software platforms and applications within the organization	• **ISA 99.02.01** 4.2.3.4 • **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05 • **ISO/IEC 27001** A.7.1.1, A.7.1.2 • **NIST SP 800-53 Rev. 4** CM-8 • **CCS CSC** 2
		ID.AM-3: Identify organizational network components and connections	• **ISA 99.02.01** 4.2.3.4 • **COBIT** DSS05.02 • **ISO/IEC 27001** A.7.1.1 • **NIST SP 800-53 Rev. 4** CA-3, CM-8 • **CCS CSC** 1
		ID.AM-4: Identify external information systems including processing, storage, and service location	• **NIST SP 500-291** 3, 4 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Identify classification / criticality / business value of hardware, devices, and software	• **ISA 99.02.01** 4.2.3.6 • **COBIT** APO03.03, APO03.04,

DRAFT

			BAI09.02 • **NIST SP 800-53 Rev. 4** RA-2, CP-2 • **NIST SP 800-34** Rev 1 • **ISO/IEC 27001** A.7.2.1
		ID.AM-6: Identify business value of workforce functions by role	• **ISA 99.02.01** 4.3.2.3.3 • **COBIT** APO01.02, BAI01.12, DSS06.03 • **ISO/IEC 27001** A.8.1.1 • **NIST SP 800-53 Rev. 4** CP-2, PM-11 • **NIST SP 800-34** Rev 1
	Business Environment (BE): Identify and prioritize organizational mission, objectives, stakeholders, and activities to support cybersecurity roles, responsibilities, and risk decisions.	**ID.BE-1:** Identify third-party stakeholders (business partners, suppliers, customers) and interdependencies among those relationships	• **COBIT** APO08.01, APO08.02, APO08.03, APO08.04, APO08.05, APO10.03, DSS01.02 • **ISO/IEC 27001** A.10.2 • **NIST SP 800-53 Rev. 4** CP-2
		ID.BE-2: Identify organization's role within the industry, sector, and national critical infrastructure	• **COBIT** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Identify and prioritize organizational mission, objectives, and activities	• **ISA 99.02.01** 4.2.2.1, 4.2.3.6 • **COBIT** APO02.01, APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-11
	Governance (GV): Identify the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements.	**ID.GV-1:** Identify organizational information security policy	• **ISA 99.02.01** 4.3.2.6 • **COBIT** APO01.03, EA01.01 • **ISO/IEC 27001** A.6.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-2: Identify information security roles & responsibility, coordination	• **ISA 99.02.01** 4.3.2.3.3 • **ISO/IEC 27001** A.6.1.3 • **NIST SP 800-53 Rev. 4** AC-21, PM-1
		ID.GV-3: Identify legal/regulatory requirements	• **ISA 99.02.01** 4.4.3.7 • **COBIT** MEA03.01, MEA03.04 • **ISO/IEC 27001** A.15.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
	Risk Assessment (RA): Periodically assess risk to organizational operations	**ID.RA-1:** Identify vulnerabilities to organizational assets (both internal and external)	• **ISA 99.02.01** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **COBIT** APO12.01, APO12.02,

DRAFT

	(including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.		APO12.03, APO12.04 • **ISO/IEC 27001** A.6.2.1, A.6.2.2, A.6.2.3 • **CCS CSC**4 • **NIST SP 800-53 Rev. 4** CA-2, RA-3, SI-5
		ID.RA-2: Identify providers of threat information	• **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001** A.13.1.2 • **NIST SP 800-53 Rev. 4** PM-15, PM-16
		ID.RA-3: Identify threats to organizational assets (both internal and external)	• **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 • **COBIT** APO12.01, APO12.02, APO12.03, APO12.04 • **NIST SP 800-53 Rev. 4** RA-3, SI-5
		ID.RA-4: Identify the potential impacts and likelihoods	• **ISA 99.02.01** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3
	Risk Management Strategy (RM): Identify the specific assumptions, constraints, risk tolerances, and priorities/trade-offs used within the organization to support operational risk decisions.	**ID.RM-1:** Identify and establish risk management processes at the organizational level	• **ISA 99.02.01** 4.3.4.2 • **COBIT** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **NIST SP 800-53 Rev. 4** PM-9 • **NIST SP 800-39**
		ID.RM-2: Determine organizational risk tolerance level	• **ISA 99.02.01** 4.3.2.6.5 • **COBIT** APO10.04, APO10.05, APO12.06 • **NIST SP 800-53 Rev. 4** PM-9 • **NIST SP 800-39**
		ID.RM-3: Determine thresholds for incident alerts	• **ISA 99.02.01** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-9 • **NIST SP 800-61** Rev 2
PROTECT (PR)	**Access Control (AC):** Limit facility and information access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	**PR.AC-1:** Perform identity and credential management (including account management, separation of duties, etc.) for devices and users	• **ISA 99.02.01** 4.3.3.5.1 • **COBIT** DSS05.04, DSS06.03 • **ISO/IEC 27001** A.11 • **NIST SP 800-53 Rev. 4** AC-2, AC-5, AC-6, IA Family • **CCS CSC** 16
		PR.AC-2: Enforce physical access control for buildings, stations, substations, data centers, and other locations that house logical and virtual	• **ISA 99.02.01** 4.3.3.3.2, 4.3.3.3.8 • **COBIT** DSS01.04, DSS05.05 • **ISO/IEC 27001** A.9.1, A.9.2, A.11.4,

DRAFT

		information technology and operational technology	A.11.6 • **NIST SP 800-53 Rev 4** PE-2, PE-3, PE-4, PE-6, PE-9
		PR.AC-3: Protect remote access to organizational networks to include telework guidance, mobile devices access restrictions, and cloud computing policies/procedures	• **ISA 99.02.01** 4.3.3.6.6 • **COBIT** APO13.01, DSS01.04, DSS05.03 • **ISO/IEC 27001** A.11.4, A.11.7 • **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Enforce access restrictions including implementation of Attribute-/Role-based access control, permission revocation, and network access control technology	• **ISA 99.02.01** 4.3.3.7.3 • **ISO/IEC 27001** A.11.1.1 • **NIST SP 800-53 Rev. 4** AC-3, AC-4, AC-6, AC-16 • **CCS CSC** 12, 15
		PR.AC-5: Protect network integrity by segregating networks/implementing enclaves (where appropriate)	• **ISA 99.02.01** 4.3.3.4 • **ISO/IEC 27001** A.10.1.4, A.11.4.5 • **NIST SP 800-53 Rev 4** AC-4
	Awareness and Training (AT): Ensure that organizational personnel and partners are adequately trained to carry out their assigned information security-related duties and responsibilities through awareness and training activities.	**PR.AT-1:** Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly	• **ISA 99.02.01** 4.3.2.4.2 • **COBIT** APO07.03, BAI05.07 • **ISO/IEC 27001** A.8.2.2 • **NIST SP 800-53 Rev. 4** AT-2 • **CCS CSC** 9
		PR.AT-2: Provide awareness and training that ensures that privileged users (e.g., system, network, industrial control system, database administrators) understand roles & responsibilities and act accordingly	• **ISA 99.02.01** 4.3.2.4.2, 4.3.2.4.3 • **COBIT** APO07.02 • **ISO/IEC 27001** A.8.2.2 • **NIST SP 800-53 Rev. 4** AT-3 • **CCS CSC** 9
		PR.AT-3: Provide awareness and training that ensures that third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities and act accordingly	• **ISA 99.02.01** 4.3.2.4.2 • **COBIT** APO07.03, APO10.04, APO10.05 • **ISO/IEC 27001** A.8.2.2 • **NIST SP 800-53 Rev. 4** AT-3 • **CCS CSC** 9
		PR.AT-4: Provide awareness and training that ensures that senior executives understand roles &	• **ISA 99.02.01** 4.3.2.4.2 • **COBIT** APO07.03 • **ISO/IEC 27001** A.8.2.2

DRAFT

		responsibilities and act accordingly	• **NIST SP 800-53 Rev. 4** AT-3 • **CCS CSC** 9
		PR.AT-5: Provide awareness and training that ensures that physical and information security personnel understand roles & responsibilities and act accordingly	• **ISA 99.02.01** 4.3.2.4.2 • **COBIT** APO07.03 • **ISO/IEC 27001** A.8.2.2 • **NIST SP 800-53 Rev. 4** AT-3 • **CCS CSC** 9
	Data Security (DS): Protect information and records (data) from natural and man-made hazards to achieve organizational confidentiality, integrity, and availability requirements.	**PR.DS-1:** Protect data (including physical records) during storage (aka "data at rest") to achieve confidentiality, integrity, and availability goals	• **COBIT** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISO/IEC 27001** A.15.1.3, A.15.1.4 • **CCS CSC** 17 • **NIST SP 800-53 Rev 4** SC-28
		PR.DS-2: Protect data (including physical records) during transportation/ transmission (aka "data in motion") to achieve confidentiality, integrity, and availability goals	• **COBIT** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISO/IEC 27001** A.10.8.3 • **NIST SP 800-53 Rev. 4** SC-8 • **CCS CSC** 17
		PR.DS-3: Protect organizational property and information through the formal management of asset removal, transfers, and disposition	• **COBIT** BAI09.03 • **ISO/IEC 27001** A.9.2.7, A.10.7.2 • **NIST SP 800-53 Rev 4** PE-16, MP-6, DM-2
		PR.DS-4: Protect availability of organizational facilities and systems by ensuring adequate capacity availability (physical space, logical storage/memory capacity)	• **COBIT** APO13.01 • **ISO/IEC 27001** A.10.3.1 • **NIST SP 800-53 Rev 4** CP-2, SC Family
		PR.DS-5: Protect confidentiality and integrity of organizational information and records by preventing intentional or unintentional release of information to an unauthorized and/or untrusted environment (information/data leakage)	• **COBIT** APO01.06 • **ISO/IEC 27001** A.12.5.4 • **CCS CSC** 17 • **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: Protect intellectual property in accordance with organizational requirements	• **COBIT** APO01.03, APO10.02, APO10.04, MEA03.01
		PR.DS-7: Reduce potential for abuse of authorized privileges by eliminating unnecessary assets, separation of duties procedures, and least privilege requirements	• **COBIT** BAI06.01, BAI01.10 • **ISO/IEC 27001** A.10.1.3 • **NIST SP 800-53 Rev. 4** AC-5, AC-6
		PR.DS-8: Establish separate development, testing,	• **COBIT** BAI07.04

		and operational environments to protect systems from unplanned/unexpected events related to development and testing activities	• **ISO/IEC 27001** A.10.1.4
		PR.DS-9: Protect the privacy of individuals and personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by organizational programs and systems	• **COBIT** BAI07.04, DSS06.03, MEA03.01 • **ISO/IEC 27001** A.15.1.3 • **NIST SP 800-53** Rev 4, Appendix J
	Information Protection Processes and Procedures (IP): Ensure adequate protection through security planning policy (that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities) and procedures to facilitate implementation.	**PR.IP-1:** Develop, document, and maintain under configuration control a current baseline configuration of information technology/operational technology systems	• **ISA 99.02.01** 4.3.4.3.2, 4.3.4.3.3 • **COBIT** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-9, SA-10 • **CCS CSC** 3, 10
		PR.IP-2: Develop, document, and maintain a System Development Life Cycle (including secure software development and system engineering and outsourced software development requirements)	• **ISA 99.02.01** 4.3.4.3.3 • **COBIT** APO13.01 • **ISO/IEC 27001** A.12.5.5 • **NIST SP 800-53 Rev 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17 • **CCS CSC** 6
		PR.IP-3: Determine, document, and implement configuration change controls for organizational systems	• **ISA 99.02.01** 4.3.4.3.2, 4.3.4.3.3 • **COBIT** BAI06.01, BAI01.06 • **ISO/IEC 27001** A.10.1.2 • **NIST SP 800-53 Rev. 4** CM-3, SA-10
		PR.IP-4: Protect organizational information by conducting backups that ensure appropriate confidentiality, integrity, and availability of backup information, storing the backed-up information properly, and testing periodically to ensure recoverability of the information	• **ISA 99.02.01** 4.3.4.3.9 • **COBIT** APO13.01 • **ISO/IEC 27001** A.10.5.1 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Ensure appropriate environmental requirements are met for personnel and technology	• **COBIT** DSS01.04, DSS05.05 • **ISO/IEC 27001** 9.1.4 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Destroy/dispose of assets (to include data destruction) in a manner that prevents disclosure of information to unauthorized entities	• **COBIT** BAI09.03 • **ISO/IEC 27001** 9.2.6 • **NIST SP 800-53 Rev 4** MP-6
		PR.IP-7: Achieve continued improvement (lessons learned, best practices, feedback, etc.)	• **COBIT** APO11.06, DSS04.05

		PR.IP-8: Develop, document, and communicate response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	• **COBIT** DSS04.03 • **ISO/IEC 27001** A.14.1 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-9: Plan for what it takes to deliver critical infrastructure services for which the organization is responsible, including the identification of dependencies that might prevent delivery of those services	• **COBIT** DSS01.03 • **ISO/IEC 27001** 9.2.2 • **NIST SP 800-53 Rev 4** CP-8, PE-9, PE-10, PE-11, PE-12, PE-14
		PR.IP-10: Integrate cybersecurity practices/procedures with human resources management (personnel screenings, departures, transfers, etc.)	• **COBIT** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISO/IEC 27001** 8.2.3, 8.3.1 • **NIST SP 800-53 Rev 4** PS Family
	Protective Technology (PT): Implement technical security solutions that supplement processes and procedures to ensure ongoing cybersecurity and resilience commensurate with organizational risk decisions.	**PR.PT-1:** Determine, document, and implement physical and logical system audit and log records in accordance with organizational auditing 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 • **COBIT** APO11.04 • **ISO/IEC 27001** A.10.10.1, A.10.10.3, A.10.10.4, A.10.10.5, A.15.3.1 • **NIST SP 800-53 Rev. 4** AU Family • **CCS CSC** 14
		PR.PT-2: Restrict the use of removable media (including writable portable storage devices), personally/externally owned devices, and network accessible media locations	• **COBIT** DSS05.02, APO13.01 • **ISO/IEC 27001** A.10.7 • **NIST SP 800-53 Rev. 4** AC-19, MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Implement and maintain technology that enforces policies to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on organizational systems (aka whitelisting of applications and network traffic)	• **CCS CSC** 6 • **COBIT** DSS05.02 • **NIST SP 800-53 Rev 4** CM-7
		PR.PT-4: Protect wireless network security including monitoring for unauthorized devices/networks, processes for authorization and authentication for wireless networks, adequate encryption to protect information transmitted	• **COBIT** DSS05.02, APO13.01 • **ISO/IEC 27001** 10.10.2 • **NIST SP 800-53 Rev 4** AC-18 • **CCS CSC** 7

DRAFT

		wirelessly	
		PR.PT-5: Manage risk to specialized systems, including operational technology (e.g., ICS, SCADA, DCS, and PLC) consistent with risk analysis.	• **COBIT** APO13.01, BAI03.02
DETECT (DE)	**Anomalies and Events (AE):** Detect anomalous activity and determine the potential impact of events to achieve the organization's goals as determined in the Protect function.	**DE.AE-1:** Identify and determine normal organizational behaviors and expected data flow of personnel, operational technology, and information systems	• **ISA 99.02.01** 4.4.3.3 • **COBIT** DSS03.01 • **NIST SP 800-53 Rev. 4** AC-2, SI-3, SI-4, AT-3, CM-2
		DE.AE-2: Characterize detected events (including through the use of traffic analysis) to understand attack targets and how a detected event is taking place	• **NIST SP 800-53 Rev. 4** SI-4
		DE.AE-3: Perform data correlation to improve detection and awareness by bringing together information from different information sources or sensors	• **NIST SP 800-53 Rev. 4** SI-4
		DE.AE-4: Assess the impact of detected cybersecurity events to inform response & recovery activity	• **NIST SP 800-53 Rev. 4** IR-4, SI -4
	Security Continuous Monitoring (CM): Track, control, and manage cybersecurity aspects of development and operation (e.g., products, services, manufacturing, business processes, and information technology) to identify cybersecurity events.	**DE.CM-1:** Perform network monitoring for cybersecurity events flagged by the detection system or process	• **COBIT** DSS05.07 • **ISO/IEC 27001** A.10.10.2, A.10.10.4, A.10.10.5 • **NIST SP 800-53 Rev. 4** CM-3, CA-7, AC-2, IR-5, SC-5, SI-4 • **CCS CSC** 14, 16
		DE.CM-2: Perform physical monitoring for cybersecurity events flagged by the detection system or process	• **NIST SP 800-53 Rev. 4** CM-3, CA-7, IR-5, PE-3, PE-6, PE-20
		DE.CM-3: Perform personnel monitoring for cybersecurity events flagged by the detection system or process	• **NIST SP 800-53 Rev. 4** AC-2, CM-3, CA-7
		DE.CM-4: Employ malicious code detection mechanisms on network devices and systems to detect and eradicate malicious code	• **COBIT** DSS05.01 • **ISO/IEC 27001** A.10.4.1 • **NIST SP 800-53 Rev 4** SI-3 • **CCS CSC** 5
		DE.CM-5: Detect the use of mobile code and implement corrective actions (blocking, quarantine, or alerting administrators) when	• **ISO/IEC 27001** A.10.4.2 • **NIST SP 800-53 Rev 4** SC-18

DRAFT

		unacceptable mobile code is detected	
		DE.CM-6: Perform personnel and system monitoring activities over external service providers	• **ISO/IEC 27001** A.10.2.2 • **NIST SP 800-53 Rev 4** CA-7, PS-7, SI-4, SA-4, SA-9
		DE.CM-7: Perform periodic checks for unauthorized personnel, network connections, devices, software	• **NIST SP 800-53 Rev. 4** CM-3, CA-7, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Perform periodic assessment to identify vulnerabilities that could be exploited by adversaries (e.g., vulnerability scanning, penetration testing)	• **NIST SP 800-53 Rev. 4** CM-3, CA-7, CA-8, RA-5, SA-11, SA-12
	Detection Processes (DP): Ensure timely and adequate awareness of anomalous events through tested and implemented detection processes and procedures.	**DE.DP-1:** Ensure accountability by establishing organizational roles, responsibilities for event detection and response	• **ISA 99.02.01** 4.4.3.1 • **COBIT** DSS05.01 • **NIST SP 800-53 Rev 4** IR-2, IR-4, IR-8 • **CCS CSC** 5
		DE.DP-2: Perform policy compliance and enforcement for detect activities (internal, external constraints)	• **ISA 99.02.01** 4.4.3.2
		DE.DP-3: Conduct exercises (e.g., tabletop exercises) to ensure that staff understand roles/responsibilities and to help provide quality assurance of planned processes	• **ISA 99.02.01** 4.4.3.2
		DE.DP-4: Communicate and coordinate cybersecurity event information among appropriate parties	• **NIST SP 800-53 Rev. 4** CP-2, IR-8
RESPOND (RS)	**Response Planning (RP):** Ensure adequate protection through policy, procedures, practice, and coordination, to implement the organizationally agreed-upon actions after detection (or in anticipation of) cybersecurity events	**RS.PL-1:** Implement the agreed-upon steps and actions to meet organizational risk objectives upon detection of (or in anticipation of) cybersecurity events.	• **ISA 99.02.01** 4.3.4.5.1 • **NIST SP 800-53 Rev. 4** CP-10, IR-4 • **CCS CSC** 18
	Communications (CO): Coordinate response with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies.	**RS.CO-1:** Ensure coordinated understanding of dependencies (personnel and systems) to informed prioritized response and support the response plan(s)	• **ISO/IEC 27001** A.13.2.1 **ISA 99.02.01** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4**NIST SP 800-53 Rev 4** CP-2, IR-8

DRAFT

		RS.CO-2: Report physical and logical cybersecurity events in association with pre-established criteria including required timeframes and reporting processes	• **ISO/IEC 27001** A.13.1.1, A.13.1.2 • **ISA 99.02.01** 4.3.4.5.5
		RS.CO-3: Implement necessary communications for sharing of detection/response information such as breach reporting requirements	• **ISO/IEC 27001** A.10
		RS.CO-4: Coordinate authority, roles, implications to stakeholders, agreement criteria, and required reporting criteria	• **ISO/IEC 27001** A.8.1.1, A.6.1.2, A.6.1.6, A.10.8.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		RS.CO-5: Conduct voluntary coordination (with mission/business partners, information sharing and analysis centers (ISACs), customers, and developers) to aid in general cybersecurity awareness and assist with events that transcend a given organization	• **NIST SP 800-53 Rev. 4** PM-15
	Analysis (AN): Conduct ongoing analysis activities, relative to the Respond function, to ensure adequate response and support recovery activities.	**RS.AN-1:** Investigate anomalies, including cybersecurity events (from network, physical, or personnel monitoring) flagged by the detection system or process	• **ISO/IEC 27001** A.6.2.1 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, PE-6, SI-4, AU-13
		RS.AN-2: Conduct an impact assessment (damage/scope)	• **ISO/IEC 27001** A.6.2.1 • **NIST SP 800-53 Rev. 4** CP-10, IR-4
		RS.AN-3: Perform forensics	• **ISO/IEC 27001** A.13.2.2, A.13.2.3 • **NIST SP 800-53 Rev. 4** IR-4
		RS.AN-4: Classify the incident	• **ISO/IEC 27001** A.13, A.13.2, A.3.6 • **ISA 99.02.01** 4.3.4.5.6 • **NIST SP 800-53 Rev. 4** IR-4
	Mitigation (MI): Conduct activities to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Contain the incident	• **ISO/IEC 27001** A.3.6, A.13.2.3 • **ISA 99.02.01** 4.3.4.5.6 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Eradicate the incident (includes strengthening controls to prevent incident recurrence)	• **ISA 99.02.01** 4.3.4.5.6, 4.3.4.5.10 • **NIST SP 800-53 Rev. 4** IR-4
	Improvements (IM): Improve organizational response by incorporating lessons learned (from current and previous detection/response activities).	**RS.IM-1:** Incorporate lessons learned into plans	• **ISO/IEC 27001** A.13.2.2 • **ISA 99.02.01** 4.3.4.5.10, 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		RS.IM-2: Update response strategies	• **NIST SP 800-53 Rev. 4** CP-2, IR-8

RECOVER (RC)	**Recovery Planning (RP):** Execute Recovery Plan activities to achieve restoration of services or functions commensurate with business decisions.	**RC.RP-1:** Execute recover plan	• **COBIT** DSS02.05, DSS03.04 • **ISO/IEC 27001** A.14.1.3, A.14.1.4, A.14.1.5 • **NIST SP 800-53 Rev. 4** CP-10, CP-2 • **CCS CSC** 8
	Improvements (IM): Improve recovery planning and processes by incorporating lessons learned into future activities.	**RC.IM-1:** Incorporate lessons learned into plans	• **ISA 99.02.01** 4.4.3.4 • **COBIT** BAI05.07 • **ISO/IEC 27001** 13.2.2 • **NIST SP 800-53 Rev. 4** CP-2
		RC.IM-2: Update recovery strategies	• **COBIT** APO05.04, BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2
	Communications (CO): Interact with outside parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Communicate with public affairs/media	• **COBIT** MEA03.02 • **NIST SP 800-53 Rev. 4** IR-4
		RC.CO-2: Communicate to perform reputation recovery	• **COBIT** MEA03.02

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.CCS.org/critical-security-controls/

For ease of use, each component of the Framework Core is given unique identifiers. Functions and categories each have a unique two-character, as shown in the Table 1 below. Subcategories within each category are referenced numerically; the unique identifier for the Subcategory is included in Table 2.

Table 2: Function and Category Unique Identifiers

500

Unique Identifier	Function	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

DRAFT

Appendix B: Methodology to Protect Privacy and Civil Liberties

This appendix presents a methodology to address privacy and civil liberties considerations around the deployment of cybersecurity activities. 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

Function	Category	Methodology
IDENTIFY	Asset Management	Organizations should identify all PII of employees, customers, or other individuals that they collect or retain, or that may be accessible to them. For example, an organization should identify PII that it processes or analyzes, or that may transit the organization's systems, even if the organization does not retain such information.
	Business Environment	N/A
	Governance	Organizations should identify legal and regulatory requirements that cover: i) PII identified under the Assets category; and ii) any cybersecurity measures that may implicate protected activities, for example, interception of electronic communications under the Electronic Communications Privacy Act.
		Organizations should identify policies and procedures that address privacy or PII management practices. Organizations should assess whether or under which circumstances such policies and procedures: 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; ii) articulate the purpose or purposes for which the PII is intended to be used; 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 to fulfill the specified purpose(s); 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 v) to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
	Risk Assessment	Organizations should 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.
	Risk Management Strategy	N/A
PROTECT	Access Control	Organizations should limit the use and disclosure of PII to the

DRAFT

Function	Category	Methodology
		minimum amount necessary to provide access to applications, services, and facilities.
	Awareness and Training	Senior executive support is critical for building a cybersecurity culture that is respectful of privacy and civil liberties. Organizations should 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. Employees should have regular training on following such policies and practices. Users should be made aware of the steps they can take to protect their PII.
	Data Security	Organizations should 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.
	Information Protection Processes and Procedures	Organizations should securely dispose of or de-identify PII that is no longer needed.
	Protective Technology	Organizations should audit access to databases containing PII. Organizations also should 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.
DETECT	**Anomalies and Events**	When detecting anomalies and events, organizations should regularly review the scope of detection and filtering methods to prevent the collection or retention of PII that is not relevant to the cybersecurity event. Organizations should have policies to ensure that any PII that is collected, used, disclosed, or retained is accurate and complete.
	Security Continuous Monitoring	When performing monitoring that involves individuals or PII, organizations should regularly evaluate the effectiveness of their practices and tailor the scope to produce the least intrusive method of monitoring.
	Detection Processes	Organizations should establish a process to coordinate privacy personnel participation in the review of policy compliance and enforcement for detect activities.
RESPOND	**Response Planning**	Organizations should 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.
	Communications	Organizations should understand any mandatory obligations for reporting breaches of PII. When voluntarily sharing information about cybersecurity incidents, organizations should ensure that only PII that is relevant to the incidents is disclosed.
	Analysis	When performing forensics, organizations should only retain PII that is relevant to the investigation. Organizations should have policies to ensure that any PII that is collected, used, disclosed, or retained is accurate and complete.

DRAFT

Function	Category	Methodology
	Mitigation	When considering methods of incident containment, organizations should 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.
	Improvements	When considering improvements in responding to incidents involving PII, organizations should 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.
RECOVER	**Recovery Planning**	Organizations should 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.
	Improvements	When considering improvements in recovering from incidents involving PII, organizations should 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.
	Communications	Organizations should consider how to communicate the use or disclosure of PII as part of the incident to maintain or rebuild trust with relevant stakeholders or the wider public.

507

DRAFT

Appendix C: Framework Development Methodology

This Framework was developed in response to Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*.[8]

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.[9] 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.[10] NIST conducted analysis of these comments, and shared initial findings on May 15, 2013. [11]

On April 3, 2013 NIST hosted an initial workshop to identify existing resources and gaps, and prioritize issues to be addressed as part of the framework.[12]

At a second workshop hosted by Carnegie Mellon University, NIST worked with stakeholders to discuss the foundations of the Framework and the initial analysis.[13] The feedback from the second workshop led to the development of the draft outline of the preliminary Framework presented on July 1, 2013.[14]

At a third workshop in July[15] the draft outline was presented for validation and stakeholders contributed input to the Framework Core, which was also shared publicly on July 1st.[16]

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 which align with policy, business, and technological approaches to cybersecurity;
- 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;

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

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

[10] http://csrc.nist.gov/cyberframework/rfi_comments.html

[11] http://csrc.nist.gov/cyberframework/nist-initial-analysis-of-rfi-responses.pdf

[12] http://www.nist.gov/itl/csd/cybersecurity-framework-workshop.cfm

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

[14] http://www.nist.gov/itl/upload/draft_outline_preliminary_framework_standards.pdf

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

[16] http://www.nist.gov/itl/upload/draft_framework_core.pdf

DRAFT

- Be consistent with voluntary international standards.

NIST has developed the Discussion Draft of the Preliminary Cybersecurity Framework in a manner that is consistent with its mission to promote U.S. innovation and industrial competitiveness.

DRAFT

Appendix D: Glossary

This appendix defines selected terms used in the publication.

Category: The subdivision of a Function into groups of cybersecurity activities, more 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 impact 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 voluntary structure to reduce cybersecurity risk that relies on private sector input and existing standards, guidelines, and practices. Also known as the "Cybersecurity Framework."

Framework Core: A compilation of cybersecurity activities and references. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

Framework Implementation Tier: The degree of progress achieved toward implementation of predictive cybersecurity risk management principles for each Profile-selected Function, Category, and Subcategory.

Framework Profile: A logical construct that defines which Framework Categories are relevant for a particular organization, sector, or other entity. A Profile also defines the expected Framework Implementation Tier for each Subcategory.

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 of which organizational systems, assets, data, and capabilities need to be protected, determine priority in light of organizational mission, and establish processes to achieve risk management goals.

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.

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

DRAFT

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

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

592 **Risk:** The level of impact on organizational operations (including mission, functions, image, or
593 reputation), organizational assets, individuals, other organizations, or the Nation resulting from
594 the operation of an information system given the potential impact of a threat and the likelihood
595 of that threat occurring.

596 **Risk Management:** The process of managing risks to organizational operations (including
597 mission, functions, image, or reputation), organizational assets, individuals, other organizations,
598 or the Nation resulting from the operation or use of an information system, and includes: (1) the
599 conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; (3)
600 employment of techniques and procedures for the continuous monitoring of the security state of
601 the information system; and (4) documenting the overall risk management program.

602 **Subcategory:** The subdivision of a Category into more detailed cybersecurity activities to allow
603 technical implementation. Examples of subcategories include "Inventory and track physical
604 devices and systems within the organization," "Protect network integrity by segregating
605 networks/implementing enclaves (where appropriate)," and "Assess the impact of detected
606 cybersecurity events to inform response & recovery activity."

607

DRAFT

Appendix E: Acronyms

This appendix defines selected acronyms used in the publication.

CCS	Council for CyberSecurity
CNSSI	Committee for National Security Systems Instruction
DCS	Distributed Control System
DHS	Department of Homeland Security
FIPP	Fair Information Practice Principles
ICS	Industrial Control Systems
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PBX	Private Branch Exchange
PII	Personally Identifiable Information
RFI	Request for Information
RMP	Risk Management Process
SCADA	Supervisory Control and Data Acquisition
SP	Special Publication

DRAFT