DRAFT NISTIR 8170

The Cybersecurity Framework

Implementation Guidance for Federal Agencies

Matt Barrett
Jeff Marron
Victoria Yan Pillitteri
Jon Boyens
Greg Witte
Larry Feldman

National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NISTIR 8170

The Cybersecurity Framework

Implementation Guidance for Federal Agencies

Matt Barrett
Jeff Marron
Applied Cybersecurity Division
Information Technology Laboratory

Victoria Yan Pillitteri
Jon Boyens
Computer Security Division
Information Technology Laboratory

Greg Witte
Larry Feldman
G2 Inc.
Annapolis Junction, Maryland

May 2017

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

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency Report 8170
41 pages (May 2017)

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

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

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

Public comment period: *May 12, 2017* through *June 30, 2017*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: nistir8170@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Acknowledgments

The authors would like to thank our advisors and reviewers including Donna Dodson, Adam Sedgewick, Matt Scholl, Kevin Stine, Kelley Dempsey, Ron Ross, Steve Quinn, Jim Foti, Mat Heyman, and Matt Smith.

Abstract

This publication assists federal agencies in strengthening their cybersecurity risk management by helping them to determine an appropriate implementation of the *Framework for Improving Critical Infrastructure Cybersecurity* (known as the Cybersecurity Framework). Federal agencies can use the Cybersecurity Framework to complement the existing suite of NIST security and privacy risk management standards, guidelines, and practices developed in response to the Federal Information Security Management Act, as amended (FISMA). The relationship between the Cybersecurity Framework and the National Institute of Standards and Technology (NIST) Risk Management Framework are discussed in eight use cases.

Keywords

Cybersecurity Framework; Federal Information Security Management Act (FISMA); Risk Management Framework (RMF); security and privacy controls

Supplemental Content

For additional information on NIST's cybersecurity programs, projects and publications, visit the Computer Security Resource Center, csrc.nist.gov. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is available at www.nist.gov and www.nist.gov/itl.

Note to Reviewers

This document provides guidance on how the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) can be used in the U.S. federal government in conjunction with the current and planned suite of NIST security and privacy risk management publications. The specific guidance was derived from current Cybersecurity Framework use.[1] To provide federal agencies with examples of how the Cybersecurity Framework can augment the current versions of NIST security and privacy risk management publications, this guidance uses common federal information security vocabulary and processes.[2] NIST will engage with agencies to add content based on agency implementation, refine current guidance and identify additional guidance to provide the information that is most helpful to agencies. Feedback will also help to determine which Cybersecurity Framework concepts are incorporated into future versions of the suite of NIST security and privacy risk management publications. NIST would like feedback that addresses the following questions:

- How can agencies use the Cybersecurity Framework, and what are the potential opportunities and challenges?
- How does the guidance presented in this draft report benefit federal agency cybersecurity risk management?
- How does the draft report help stakeholders to better understand federal agency use of the Cybersecurity Framework?
- How does the draft report inform potential updates to the suite of NIST security and privacy risk management publications to promote an integrated approach to risk management?
- Which documents among the suite of NIST security and privacy risk management publications should incorporate Cybersecurity Framework concepts, and where?
- How can this report be improved to provide better guidance to federal agencies?

Conventions

The phrase "federal agencies" in this publication means those agencies responsible for non-national security-related information in federal systems.

FISMA refers to the Federal Information Security Management Act of 2002, as amended.[3]

"Cybersecurity Framework" refers to version 1.0 of the "*Framework for Improving Critical Infrastructure Cybersecurity*, issued in February 2014."[4]

---

[1] Such as use of the Industry Resources located at the Cybersecurity Framework Web site: https://www.nist.gov/cyberframework/industry-resources

[2] The suite of NIST security and privacy risk management publications include: Federal Information Processing Standards (FIPS) Publication 199, FIPS Publication 200, Special Publication (SP) 800-53, SP 800-37, SP 800-137, SP 800-39, and SP 800-30.

[3] *The Federal Information Security Management Act of 2002* was updated through the *Federal Information Security Modernization Act of 2014*.

[4] The *Framework for Improving Critical Infrastructure Cybersecurity* is found at: https://www.nist.gov/cyberframework

The term "Tiers" cited in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, will be referred to as "Levels" in this report to avoid confusion with Cybersecurity Framework Implementation Tiers.

The six steps of the Risk Management Framework described in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* – Categorize, Select, Implement, Assess, Authorize, and Monitor – are indicated using capital letters. This includes all conjugations (e.g., Authorize, Authorizing, and Authorized all refer to step five of the RMF).

The five Functions of the Cybersecurity Framework – Identify, Protect, Detect, Respond, and Recover – are indicated using capital letters. This includes all conjugations (e.g., Detect, Detected, and Detecting all refer to the Detect Function of Cybersecurity Framework).

The terms "enterprise risk management" and "organization-wide risk management" are used interchangeably.

Executive Summary

All federal agencies are charged and entrusted with safeguarding the information that is contained in their systems and with ensuring that these systems operate securely and reliably. In a world where cyber systems are constantly challenged by more frequent and often more creative and sophisticated attacks, it is vital that agency personnel – from the most senior executives to line staff – manage their assets and cybersecurity risks wisely. To do that well, they need the most capable, up-to-date, and easy-to-use approaches and tools, including a holistic approach to risk management.

The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines – including minimum requirements – to provide adequate information security for federal information and information systems. This suite of security and privacy risk management standards and guidelines provides guidance for an integrated, organization-wide program to manage information security risk. In response to a new executive order issued by the President on May 11, 2017 and as part of its initiative to continuously improve the risk management resources provided to federal agencies, NIST has produced this report providing federal agencies with guidance on how the *Framework for Improving Critical Infrastructure Cybersecurity* (known as the Cybersecurity Framework) can help agencies to complement existing risk management practices and improve their cybersecurity risk management programs.

Developed by NIST in 2013-2014 working closely with the private and public sectors, the Cybersecurity Framework is a risk management approach used voluntarily by organizations across the United States. It also is receiving attention in other countries and regions around the world. Prepared initially to address cybersecurity challenges in the nation's critical infrastructure sectors, the voluntary Framework aligns with and complements the suite of NIST security and privacy risk management standards and guidelines.

This report illustrates eight use cases in which federal agencies can leverage the Cybersecurity Framework to address common cybersecurity-related responsibilities. By doing so, agencies can seamlessly integrate the Cybersecurity Framework with key NIST cybersecurity risk management standards and guidelines already in wide use at various organizational levels. The result will be a more robust and mature agency-wide cybersecurity risk management program. The eight use cases are:

1. *Integrate Enterprise and Cybersecurity Risk Management*
2. *Manage Cybersecurity Requirements*
3. *Integrate and Align Cybersecurity and Acquisition Processes*
4. *Evaluate Organizational Cybersecurity*
5. *Manage the Cybersecurity Program*
6. *Maintain a Comprehensive Understanding of Cybersecurity Risk*
7. *Report Cybersecurity Risks*
8. *Inform the Tailoring Process*

The key concepts of the Cybersecurity Framework and the proposed federal cybersecurity uses described in this document are intended to promote the dialog with federal agencies. This will inform near-term updates to the suite of applicable NIST cybersecurity and privacy risk management publications, including updates to Special Publications 800-37 and 800-53. Recognizing the importance of clear, timely guidance to assist agencies in carrying out their

cybersecurity-related responsibilities, NIST will use federal agency feedback to inform and prioritize accelerated updates of those documents.

Table of Contents

Executive Summary v
1 Introduction 8
1.1 Audience 8
1.2 Organization of this Report 9
2 Guidance 10
1. Integrate Enterprise and Cybersecurity Risk Management 11
2. Reconcile, Integrate, and Prioritize Cybersecurity Requirements 12
3. Integrate and Align Cybersecurity and Acquisition Processes 14
4. Evaluate Organizational Cybersecurity 15
5. Manage the Cybersecurity Program 16
6. Maintain a Comprehensive Understanding of Cybersecurity Risk 17
7. Report Cybersecurity Risks 18
8. Inform the Tailoring Process 19
3 Plans for an Integrated Federal Approach 21

List of Appendices

Appendix A— Summary of NIST Risk Management Publications 22
Appendix B— Acronyms 32
Appendix C— Glossary 33
Appendix D— References 38

List of Figures

Figure 1: Relationships of Key NIST Risk Management Guidance 23
Figure 2: Special Publication 800-39 Multi-Level Risk Management 24
Figure 3: Cybersecurity Risk Management Framework described in NIST SP 800-37 . 25
Figure 4: Balancing Organizational Focus with Cybersecurity Framework Functions ... 28
Figure 5: The Cybersecurity Framework Core 29
Figure 6: Notional Information and Decision Flows within an Organization 31

1 Introduction

As part of its statutory responsibilities under the Federal Information Security Management Act as amended (FISMA), NIST develops standards and guidelines – including minimum requirements – to provide adequate information security for all agency operations and assets. Fulfilling the requirements of FISMA and OMB Circular A-130[5], these documents include Federal Information Processing Standards (FIPS), Special Publications (SPs), and NIST Interagency Reports (NISTIRs), which are used by agencies to develop, implement, and maintain cybersecurity and privacy programs

The Cybersecurity Enhancement Act of 2014 formally updated NIST's role to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure (CI) owners and operators. That statute's assignments included work NIST had begun in February 2013 as a result of Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*.[6] The EO tasked the Department of Commerce to lead the development of a framework to reduce CI cybersecurity risks. NIST convened industry, academia, and government to develop a voluntary *Framework for Improving Critical Infrastructure Cybersecurity* (known as the Cybersecurity Framework) that consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cybersecurity risks. It offers a high-level vocabulary for cybersecurity risk management, a taxonomy of cybersecurity outcomes, and a methodology to assess and manage those outcomes.

The increasing frequency, creativity, and variety of cyber attacks means that a greater emphasis must be placed by all organizations on managing cybersecurity risk as a part of their enterprise risk management programs to fulfill their mission and business objectives. By seamlessly integrating the Cybersecurity Framework and key NIST cybersecurity risk management standards and guidelines already in wide use at various organizational levels, agencies can develop, implement, and continuously improve agency-wide cybersecurity risk management processes that inform strategic, operational, and other enterprise risk decisions.[7]

1.1 Audience

This document is intended for those who are responsible for overseeing, leading, and managing information systems within their agencies. That includes senior executives and line managers and staff – and every level in between. It is especially relevant for personnel who develop,

[5] https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource

[6] https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[7] While this report is intended to help federal agencies to incorporate key Cybersecurity Framework elements into their programs, *publication of this document will not affect the Cybersecurity Framework's primary focus on private sector critical infrastructure owners and operators.*

implement, report, and improve enterprise and cybersecurity risk management processes within their organizations. While the focus is on federal users, NIST expects that many public and private sector organizations that choose to use the NIST cybersecurity risk management suite of standards and guidelines will benefit from this document, including the use cases that are presented.

1.2 Organization of this Report

The remainder of this document is structured as follows:

- Section 2 provides guidance that includes eight descriptions of how federal agencies can effectively use the Cybersecurity Framework in conjunction with existing NIST standards and guidelines to develop, implement, and continuously improve their cybersecurity risk management programs.
- Section 3 describes plans for an integrated federal approach to cybersecurity risk management.
- Appendix A summarizes NIST cybersecurity risk management standards and guidelines.
- Appendix B lists and explains acronyms that appear in the document.
- Appendix C defines key terms.
- Appendix D lists references with additional information.

2 Guidance

Using eight common government cybersecurity needs, this section provides guidance that can assist federal agencies as they develop, implement, and continuously improve their cybersecurity risk management programs. It is consistent with OMB's policy guidance to federal agencies contained in OMB Circular A-130, *Managing Information as a Strategic Resource*. That circular provides guidance regarding the Risk Management Framework (described in NIST SP 800-37), associated documents, and the Cybersecurity Framework.

OMB Circular A-130 Appendix I, Section 5.q

Responsibiities for Protecting and Managing Federal Information Resources

The [Cybersecurity] Framework is not intended to duplicate the current information security and risk management practices in place within the Federal Government. However, in the course of managing information security risk using the established NIST Risk Management Framework and associated security standards and guidelines required by FISMA, agencies can leverage the Cybersecurity Framework to complement their current information security programs.

NIST will work with federal agencies to assess the relative value of these eight proposed uses, identify additional uses, and understand how to better illustrate applications of the Cybersecurity Framework. The feedback received will guide and inform NIST as it incorporates Cybersecurity Framework concepts into its various cybersecurity risk management publications. These uses illustrate how agencies can leverage both the Cybersecurity Framework and the NIST Risk Management Framework to:

- Measure and improve cybersecurity performance at various organizational levels;
- Organize communication about cybersecurity risk, activities, and results across the organization-wide risk management program; and
- Align and prioritize cybersecurity requirements for use in the acquisition process and to inform the tailoring of controls.

Figure 1 depicts federal cybersecurity risk management needs (middle column) superimposed on the three-level pyramid found in one of the primary NIST cybersecurity documents used by federal agencies – *Managing Information Security Risk: Organization, Mission, and Information System View* (SP 800-39). Most of the uses addressed in this publication fit in the "Mission/Business Processes" (Level 2). One use is offered that illustrates the "Organization" function (Level 1) and another addresses the "System" (Level 3). In the right column, Figure 1 also depicts the most applicable Cybersecurity Framework component – Core, Profile(s), or Implementation Tiers – for a given federal use.

Special Publication 800-39	**Level 1** Organization	**Integrate enterprise and cybersecurity risk management** by communicating with universally understood risk terms.	Core	Cybersecurity Framework Components
	Level 2 Mission/ Business Processes	**Manage cybersecurity requirements** using a construct that enables integration and prioritization of *all* requirements.	Profile(s)	
		Integrate and align cybersecurity and acquisition processes by relaying cybersecurity requirements and priorities in a common and concise language	Profile(s)	
		Evaluate organizational cybersecurity using a standardized and straightforward measurement scale and set of self-assessment criteria.	Implementation Tiers	
		Manage the cybersecurity program by determining which cybersecurity outcomes necessitate common controls, and apportioning work and responsibility for those cybersecurity outcomes (supports RMF Implement & Monitor).	Profile(s)	
		Maintain a comprehensive understanding of cybersecurity risk using a standardized organizing structure (supports RMF Authorize).	Core	
		Report cybersecurity risks using a universal and understandable reporting structure.	Core	
	Level 3 System	**Inform the tailoring process** using a comprehensive reconciliation of *all* cybersecurity requirements (supports RMF Implement).	Profile(s)	

Figure 1: Federal Cybersecurity Uses

Federal agencies may determine additional ways the integrated federal approach can or should enhance their cybersecurity risk management programs. NIST intends to develop additional examples of uses based in part on feedback from federal agencies.

1. Integrate Enterprise and Cybersecurity Risk Management

Organizations manage many types of risk and develop specific policies to identify, assess, and help mitigate adverse effects across a wide range of risks, with cybersecurity among them. Some of the other typical risks include: safety, operations, financial, program, acquisitions, customer interactions, supply chain, and privacy. Some of these areas employ different terminologies and risk management approaches to make decisions within the risk area and across the organization as part of an enterprise-wide management process. The Cybersecurity Framework provides organizations the ability to leverage a common language that reaches beyond cybersecurity and across the organization, while allowing these other risk management disciplines to incorporate the Framework's terms or to continue using existing processes.

More specifically, the Cybersecurity Framework Core's five "Functions" offer a way to organize cybersecurity risk management activities at their highest levels using words that can be applied across risk management disciplines: Identify, Protect, Detect, Respond, and Recover. Many stakeholders from varied parts of an organization can understand and already use these five words in the context of risk decisions. While the Cybersecurity Framework links them to specific cybersecurity outcomes, other disciplines heavily dependent on risk management such as

finance and physical security may choose to integrate their unique processes and terminologies into the Framework's Functions to facilitate communication.

For example, CISOs and other cybersecurity professionals in federal agencies can use these five Functions as a way to engage, organize and explain their cybersecurity approaches to agency external stakeholders, executive leadership, and employees and to integrate cybersecurity concepts into other organizational areas. The Functions provide an understandable and intuitive language for CISOs to gather risk tolerance perspectives from their peers and leadership team. The Functions are also a simple way to organize and express a risk strategy to address those risk tolerances. This helps CISOs to collaborate with stakeholders from various parts of the organization (e.g. human resources, finance, legal, acquisition) in identifying common priorities and assets and the risk-based strategies to address those common priorities. When representatives across an organization are engaged and instrumental in identifying and prioritizing organizational assets and determining risk management strategies, the results are more likely to achieve the desired outcomes.

Integrate Enterprise and Cybersecurity Risk Management

Benefit(s): • Facilitate communication, • Provide common language that reaches beyond cybersecurity risk management and encompasses other risk management disciplines.	**Primary SP 800-39 Level:** 1 - Organization **Primary Cybersecurity Framework Component:** Core
Summary: Using the Cybersecurity Framework's Functions (Identify, Protect, Detect, Respond, and Recover) as the basis for risk management dialogs, organizations can raise awareness of cybersecurity and other risks to be managed and facilitate communication among agency stakeholders, including executive leadership.[8] This is enabled when other disciplines participating in the enterprise risk management dialog link their existing approaches to the Functions. This Use example aggregates the activities of Uses 2-8.	
Typical Participants: Head of Agency (Chief Executive Officer), Risk Executive (Function), Chief Information Officer, Senior Information Security Officer/Chief Information Security Officer (CISO), stakeholders representing other risk management disciplines (e.g., Finance, Human Resources, Acquisition).	
Primary NIST Documents: NIST Special Publication 800-39, Cybersecurity Framework	

2. Manage Cybersecurity Requirements

Federal agencies, like private sector organizations, are subject to multiple cybersecurity requirements. For agencies, these may include (but are not limited to) laws, regulations, oversight by and reports to Congress, internal policy, and Office of Management and Budget policies. The Cybersecurity Framework can be used by federal agencies for requirements management through the process of integration and prioritization.

[8] Source: OMB A-130

Agencies can integrate requirements by aligning and de-conflicting using the structure of the Core. For instance, a federal agency may need to abide by FISMA, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, the Payment Card Industry Data Security Standard, as well as their own cybersecurity policy, all while accomplishing a mission objective. Applicable excerpts of these laws, guidelines, policy, and objectives can be aligned with the various Functions, Categories, and Subcategores of the Core. By reconciling cybersecurity requirements in this manner, a federal agency can determine where requirements overlap and/or conflict, and consider alternative approaches, perhaps including modification of cybersecurity requirements in that agency's control, to address those requirements. In turn, this offers the agency the opportunity to improve its efficiency as well as its effectiveness.

By integrating requirements into the Core, agencies stage efficient prioritization. For instance, it may be apparent that certain Subcategory outcomes are meaningful for multiple requirements. It may also be clear that a short list of Subcategories are essential for successful achievement of mission objectives. Priorities can be captured in the structure of the Core and used as inputs to drive cybersecurity investments, effort, and focus.

The work product of cybersecurity requirements management using Cybersecurity Framework is referred to as a Profile. See Appendix A for additional description and uses of Cybersecurity Framework Profiles.

Manage Cybersecurity Requirements

Benefit(s): • Determine where cybersecurity requirements overlap and/or conflict in order to ensure compliance and improve efficiency and effectiveness. • Prioritize Subcategory outcomes based on the reconciliation of requirements, as well as mission priorities and the operational environment/threat information. • Operationalize cybersecurity activities based on the Cybersecurity Framework Profile.	**Primary SP 800-39 Level:** 2 – Mission/Business Processes **Primary Cybersecurity Framework Components:** Core, Profile(s)
Summary: Federal agencies can use the Cybersecurity Framework Core Subcategories to align and de-conflict cybersecurity requirements applicable to their organizations. This reconciliation of requirements helps to ensure compliance and provides input in prioritizing requirements across the organization using the subcategory outcomes. This becomes a means of operationalizing cybersecurity activities and a tool for iterative, dynamic, and prioritized risk management for the agency.	
Typical Participants: Risk Executive, Chief Information Officer, Senior Information Security Officer/Chief Information Security Officer (CISO)	
Primary NIST Documents: NIST Special Publication 800-39, Cybersecurity Framework	

3. Integrate and Align Cybersecurity and Acquisition Processes

Federal agencies and contractors must adhere to both common and unique cybersecurity and acquisition requirements[9]. In the acquisition process, this often causes a misunderstanding of expectations between federal agencies and offerors and may limit government access to the best products and services, while increasing costs to offerors, agencies, and taxpayers.

The Cybersecurity Framework can be used to translate among a variety of risk management practices and support federal agencies as they interact with a wide variety of suppliers. These include service providers, product vendors, systems integrators, organizations within a regulated sector, and other private sector partners.

For example, an agency could use the Cybersecurity Framework during market research by asking respondents to a Request For Information or Sources Sought Notice to include their Cybersecurity Framework Profile or to express the cybersecurity capabilities of their product in responses. This information would help the agency to better compare and contrast the cybersecurity capabilities of organizations, products and services of respondents.

By using Profiles, the Cybersecurity Framework can be incorporated into the acquisition process as the underpinning of: evaluation criteria (agency), solicitation response (supplier), proposal/quote review (agency), minimum contract requirements (agency), contract compliance evidence (supplier), and contract compliance verification (agency). The use of Profiles allows suppliers the flexibility to select from among various standards and practices to meet federal agency specific requirements, while communicating their cybersecurity posture in a consistent way. It also provides agencies a means to consistently and objectively assess the cybersecurity posture of potential partners.

Integrate and Align Cybersecurity and Acquisition Processes

<table>
<tr><td rowspan="2">Benefit(s):
• Ability to determine which cybersecurity standards and practices to incorporate into contracts.
• Provides a common language to communicate requirements to offerors and awardees (agreement/contract)
• Allows offerors to express their cybersecurity posture and related standards and practices.</td><td>Primary SP 800-39 Level:
2 – Mission/Business Processes</td></tr>
<tr><td>Primary Cybersecurity Framework Component:
Profile(s)</td></tr>
<tr><td colspan="2">Summary: For acquisitions that present cybersecurity risks, federal agencies can choose to do business with organizations that meet minimum cybersecurity requirements in their operations and in the products and services they deliver. Cybersecurity Framework Profiles can be used by federal agencies to express technical requirements; offerors can demonstrate how they meet or exceed these requirements.</td></tr>
<tr><td colspan="2">Typical Participants: Risk Executive (Function), Chief Information Officer, Senior Information Security Officer/Chief Information Security Officer (CISO), General Counsel, Contracting Office, Mission/Business owner</td></tr>
<tr><td colspan="2">Primary NIST Documents: NIST Special Publications 800-39, 800-161, 800-171, Cybersecurity Framework</td></tr>
</table>

[9] Compare, e.g., FAR § 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems* (common), with DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* (unique), and OMB Circular No. A-130, *Managing Information as a Strategic Resource* (common), with DoD Instruction 8500.01, *Cybersecurity* (unique).

4. Evaluate Organizational Cybersecurity

The Implementation Tiers are designed as an overarching measurement of cybersecurity risk management behaviors within an organization. They help an organization to consider the maturity of each of the following cybersecurity properties on a scale from 1-4 (Partial, Risk Informed, Repeatable, and Adaptive):

- Risk Management Process - Does our organization have a cybersecurity risk management process that is functioning and repeatable?
- Integrated Risk Management Program – To what extent is cybersecurity risk management integrated into enterprise risk management?
- External Participation – To what degree is our organization (or units within the organization) sharing with and receiving cybersecurity information from outside parties?

Unlike some maturity models, the Implementation Tiers are not prescriptive. In other words, there is no set requirement for an organization and all of its sub-organizations to operate at Implementation Tier 4. Rather, Implementation Tiers can be used for informed trade-off analysis, since there is a corresponding cost and risk tolerance associated with each Implementation Tier. For example, to balance finite resources across all agency cybersecurity considerations, it may be appropriate to operate at Implementation Tier 2 in one part of an agency in order to afford to operate at Implementation Tier 4 elsewhere. One way that federal agencies may apply these trade-offs is via FIPS-199 categorizations. An agency might view FIPS-199 High Impact and High Value Asset[10] (HVA) systems as appropriate for higher Implementation Tiers. Conversely, the agency may determine that operating at a lower Implementation Tier for FIPS-199 Low Impact categorized systems is acceptable.

Agencies can evaluate the Implementation Tier at which they are operating in comparison to the desired Tier. This process may identify gaps between the current and the target Implementation Tier, as well as steps that the organization can take to progress to a desired Tier. These gaps indicate there is a difference between current and optimal cybersecurity risk management behaviors. Agency Implementation Tier targets may be influenced by external requiremnts, including OMB policies and OMB cross-agency priorities.

Evaluate Organizational Cybersecurity

<table>
<tr><td rowspan="2">Benefit(s):
• Assist agencies in critically evaluating their cybersecurity risk management behaviors and identifying opportunities for improvement.
• Enable agencies to make informed trade-offs concerning the appropriateness of and investments in the cybersecurity of particular organizational units or systems.</td><td>Primary SP 800-39 Level:
2 – Mission/Business Processes</td></tr>
<tr><td>Primary Cybersecurity Framework Component:
Implementation Tiers</td></tr>
<tr><td colspan="2">Summary: Implementation Tiers provide agencies a basis for rationalizing different modes of cybersecurity operations across an organization. That is based on trade-off analysis of target Implementation Tiers for various agency business units or specific assets. Gap analysis between the current and Target Implementation Tier will reveal opportunities for prioritizing improvement investments.</td></tr>
</table>

[10] High Value Asset as first referenced in OMB Memorandum M-16-04 and defined in M-17-09

Typical Participants: Head of Agency (Chief Executive Officer), Agency Deputy (Chief Operating Officer) Risk Executive, Chief Information Officer, Senior Information Security Officer/Chief Information Security Officer (CISO), stakeholders representing other risk management disciplines (e.g., Finance, Human Resources, Acquisition)
Primary NIST Documents: NIST Special Publication 800-39, Cybersecurity Framework

5. Manage the Cybersecurity Program

The Core taxonomy of cybersecurity outcomes that are captured in subcategories provides a logical structure to organize cybersecurity operations within an agency – specifically, how work gets assigned, tracked, and measured, and how personnel empowerment and accountability is managed.

The Cybersecurity Framework provides a way to assign cybersecurity responsibility to units or individuals in an organization. When doing so, executives can specify tasks, responsibilities, and authorities of the cybersecurity program and its associated strategies. This also allows executives to empower units and individuals and to reward them appropriately. If parts of cybersecurity operations are not performing as intended or risk is beyond set threshold levels, the Cybersecurity Framework structure enables managers to trace and investigate the situation and to hold relevant units and individuals accountable.

The Cybersecurity Framework provides a manageable way to apportion responsibility for cybersecurity – most importantly for the desired outcomes associated with assigned Core Functions, Categories, or Subcategories. Since controls in SP 800-53 map to the Cybersecurity Framework, responsibility for the corresponding controls can also be assigned to these individuals.

When analyzing the desired cybersecurity outcomes associated with Core Categories and Subcategories, certain outcomes may be more cost-effectively managed for the entire agency by one unit rather than by each organizational unit separately. For example, an agency may determine that responsibility for Subcategory PR.AC-2 “Physical access to assets is managed and protected” is most cost-effectively made the responsibility of the Physical Security unit for the benefit of the entire agency. Conversely, the agency may decide that responsibility for the cybersecurity outcomes of other Subcategories is shared between business units and/or systems. These determinations can assist federal agencies in identifying candidate common and hybrid controls as specified in SP 800-53.

Another way for federal agencies to identify common cybersecurity controls is by identifying common assets and business processes. Managers of various business units within agencies have a key role in identifying high value assets and business processes. The ensuing discussions among the business unit managers, CISO, and other stakeholders of how to prioritize and protect these assets will likely indicate business units which have similar assets or business processes and which can utilize shared services to protect these high value assets. That can logically lead to

the identification of common controls to secure assets and business processes across business units. It also can yield significant cost savings.

Manage the Cybersecurity Program

Benefit(s): • Provide a way to apportion responsibility and authority for cybersecurity outcomes to business units and/or individuals using the Core. • Provide a way to empower, reward, and hold accountable units and individuals charged with certain cybersecurity responsibilities. • Identify common controls and hybrid controls via analysis of the cybersecurity outcomes in the Core and apportion responsibility for these outcomes to business units and/or individuals. • Save significant resources by identifying common controls.	**Primary SP 800-39 Level:** 2 – Business/Mission Processes **Primary Cybersecurity Framework Component:** Core
Summary: The Core taxonomy of cybersecurity outcomes in Subcategories provides a way to apportion responsibility for these cybersecurity outcomes to organizational business units or individuals. Analysis of the cybersecurity outcomes in the Cybersecurity Framework Core also can assist agencies in identifying common and hybrid controls and saving resources.	
Typical Participants: Chief Information Officer, Senior Information Security Officer/Chief Information Security Officer (CISO), Common Control Provider	
Primary NIST Documents: NIST Special Publication 800-37, Cybersecurity Framework	

6. Maintain a Comprehensive Understanding of Cybersecurity Risk

By aggregating cybersecurity findings, gaps and vulnerabilities into a centralized record, agencies can gain a single view of cybersecurity risk at an aggregate level. That understanding can better inform risk decisions. Examples include determining how a system Authorization decision might affect the agency as a whole or how broader risk decisions might play out in a complex and connected infrastructure. An organization-wide record of risk will also enable consistent reporting. In some organizations, this centralized record is referred to as a "risk register."

Agencies currently track managed vulnerabilities, vulnerability mitigation plans, and accepted vulnerabilities on a system-by-system basis. This information is in the system Security Authorization Package, which includes the system security plan (SSP), the security assessment report (SAR), and the plan of action and milestones (POA&Ms)[11]. Through these artifacts, agencies: track planned security and privacy controls, assess the implementation of controls, annotate weaknesses or deficiencies in security controls, identify residual vulnerabilities in the system, and highlight mitigation plans. The information in these key documents is used by Authorizing Officials (AO) to make risk-based Authorization decisions.

Using the Cybersecurity Framework, an organization can assemble system-level weaknesses or deficiencies into an enterprise-wide understanding of cybersecurity vulnerabilities. Including

[11] Security Authorization artifacts and process detailed in SP 800-37rev1 Appendix F

weaknesses or deficiencies across the enterprise can provide a comprehensive understanding of vulnerabilities and planned mitigations. This information can be viewed at the Subcategory, Category, or Function level to provide agencies additional context before making risk decisions and associated resource investments.

Further, aggregating essential information from SARs, POA&Ms, and SSPs enables security Authorization decisions through continuous monitoring. Security control assessments, remediation actions, and key updates to the SARs, POA&Ms and SSPs for the system-at-hand can be considered in the context of the organization's aggregate risk. The risk register is also curated using the on-going risk changes tracked through Risk Management Framework (RMF) Monitor activities. The risk register is a tool that helps the AO understand if accepting the system risk will drive overall risk beyond organizational tolerance. Organizing the risk register according to the language of the Core also enables a larger group of people to participate in and inform the Authorization decision. In particular, the understandable language of Functions and Categories of the Core enables non-cybersecurity experts to participate.

Maintain a Comprehensive Understanding of Cybersecurity Risk

Benefits): • Assist federal agencies to obtain a better understanding of aggregate risk to enable RMF Authorization decisions.	**Primary SP 800-39 Level:** 2 – Mission/Business Processes **Primary Cybersecurity Framework Component:** Core
Summary: The Cybersecurity Framework Core can help agencies to better organize the risks they have accepted and the risks they are working to remediate across all systems. This aggregate and comprehensive understanding of risk enables more informed and effective RMF Authorization decisions.	
Typical Participants: Senior Information Security Officer/Chief Information Security Officer (CISO), Authorizing Official	
Primary NIST Documents: NIST Special Publication 800-37, Cybersecurity Framework	

7. Report Cybersecurity Risks

With the risk register structured according to the Cybersecurity Framework Core, an organization can very efficiently generate risk reports. Reports often need to be distributed to a variety of audiences including: business process personnel, who manage risks as a part of their daily responsibilities; senior executives, who approve and are responsible for agency operations and investment strategies based on risk; other internal units; and external organizations. This means reports need to vary significantly in both transparency and detail, depending on the recipient and report requirement. At the same time, reports need to be clear and understandable. A standardized reporting format can assist agencies in multiple cybersecurity reporting needs

Additionally, the timeliness of reports is critical for two reasons. First, reporting needs to match the timeline expectations of the receiving parties. Second, reports often need to represent current state, so the time between risk measurement and report delivery needs to be minimized.

Today, risk reporting within federal organizations is performed using a variety of technologies and reporting formats due to different sources requesting information for different purposes and with a high degree of variability in reporting timelines. In recent years, the Office of Management and Budget has requested annual FISMA metrics organized using the structure of the Cybersecurity Framework's Core. With an increasing number of federal organizations, partners, and suppliers using the Cybersecurity Framework, it is more efficient to use the Framework's approach to meet these multiple reporting needs.

Structuring a risk register according to the hierarchy of cybersecurity outcomes in the Core allows organizations to generate reports at varying levels of detail. Specifically, relating the hierarchy of five Functions, Categories, and Subcategories to SP 800-53 controls allows maximum flexibility in the level of detail of a given report, and can make those reports more useful to varied audiences. That level of detail can be achieved quickly using the Core, minimizing time and resources invested in generating the report.

Report Cybersecurity Risks

Benefit(s): • Provide expeditious, audience-appropriate, easy-to-understand, standardized reporting	**Primary SP 800-39 Level:** 2 – Mission/Business Processes **Primary Cybersecurity Framework Component:** Core
Summary: The Cybersecurity Framework Core provides a reporting structure and language that aligns to SP 800-53 controls. This enables easy roll-up of control status into a reporting structure that is appropriate to and understandable by a given audience.	
Typical Participants: Head of Agency (Chief Executive Officer), Deputy Head of Agency (Chief Operating Officer) Risk Executive (Function), Chief Information Officer, Information Owner/Steward, Senior Information Security Officer/Chief Information Security Officer (CISO), stakeholders representing other risk management disciplines (e.g., Finance, Human Resources, Acquisition)	
Primary NIST Documents: NIST Special Publication 800-37rev1, Cybersecurity Framework	

8. Inform the Tailoring Process

Information systems are most valuable when their features explicitly support an organization's mission objectives and requirements.

In the RMF, after the system is categorized based on FIPS 199/SP 800-60, organizations leverage FIPS 200 to identify minimum security requirements associated with the system impact level. They then use the SP 800-53 tailoring process to apply any other needed security to address specific mission objectives, operational constraints, cybersecurity requirements, and

other organizational considerations. This process is used to customize the controls baseline for each system.

The Cybersecurity Framework offers a mechanism for reconciling mission objectives and cybersecurity requirements into Profiles, making them an important work product using a top-down approach to inform the tailoring. In developing a Profile, organizations can align and de-conflict all mission objectives and cybersecurity requirements into a singular structure according to the taxonomy of the Core. That allows organizations to easily prioritize the cybersecurity outcomes of the Subcategories. Since Profiles can be a reconciliation of cybersecurity requirements and associated priorities from many sources, Profiles can be used as a concise and important artifact for consideration when tailoring SP 800-53 initial control baselines to final control baselines. Specifically, considering organizational Subcategory priorities and knowing the associated SP 800-53 controls may lead to precise adjustments to the initial controls baseline in ways that best support the organizational mission.

Inform the Tailoring Process

Benefit(s): • Provide a single document that reflects mission objectives and applicable agency cybersecurity requirements as a basis for tailoring initial system controls baselines.	**Primary SP 800-39 Level:** 3 - System **Primary Cybersecurity Framework Component:** Profile(s)
Summary: Cybersecurity Framework Profiles enable agencies to reconcile mission objectives and cybersecurity requirements into the structure of the Cybersecurity Framework Core. This readily translates to the SP 800-53 controls that are most meaningful to the organization. Profiles can be used to tailor initial SP 800-53 baselines into final baselines, as deployed in the RMF Implementation step.	
Typical Participants: Information Owner/Steward, Information System Owner, Information Security Architect, Information System Security Engineer, stakeholders representing other risk management disciplines (e.g., Finance, Human Resources, Acquisition)	
Primary NIST Documents: NIST Special Publication 800-53rev4, Cybersecurity Framework	

3 Plans for an Integrated Federal Approach

Under FISMA, NIST is clearly assigned to develop and issue "standards [and guidelines] that provide minimum information security requirements," and "improve the efficiency of operation or [the effectiveness of] security of Federal information systems.[12]"

As part of those responsibilities, NIST has been leading an initiative to advance and evolve the integrated federal approach to cybersecurity by placing an increased emphasis on risk management. As drivers for this evolution, this initiative:

- Uses cybersecurity effectiveness, agency efficiency, and repeatable processes,
- Proposes solutions for varied and dynamic federal cybersecurity challenges,
- Identifies, validates, and integrates valuable concepts,
- Streamlines federal cybersecurity risk management standards and guidelines, and
- Relies on OMB A-130 as the primary policy requirement.

The key concepts of the Cybersecurity Framework and the federal cybersecurity uses described in this document are intended to promote the dialog with federal agencies. This exchange will inform near-term updates to the suite of affected NIST cybersecurity and privacy risk management publications. Recognizing the importance of clear, timely guidance to assist federal agencies in carrying out their cybersecurity-related responsibilities, NIST will accelerate the update of those documents, beginning with publication of this draft report. As a next step, consistent with NIST's practices, federal agency feedback will be used to inform and prioritize these updates. NIST also may use mechanisms that are more formal in order to gain wider input. These may include the option of issuing a Request for Comment (RFC) or a Request for Information (RFI) for certain elements of the suite of federal standards, guidelines, and publications. NIST will select the most effective and expeditious path forward.

[12] https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

Appendix A—Summary of NIST Risk Management Publications

This appendix describes several NIST cybersecurity risk management publications referenced throughout this document.

Brief Overview of Key Publications

NIST cybersecurity risk management (RM) standards, guidelines and other documents set out RM processes and guide continual improvement of cybersecurity. Three of these are:

- The *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework)
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

The *Framework for Improving Critical Infrastructure Cybersecurity* (generally referred to as the Cybersecurity Framework) provides a flexible, repeatable and cost effective risk-based approach to implementing security practices. Developed initially for use by critical infrastructure (CI) owners and operators but now used more broadly, the Framework is based on existing standards, guidelines, and practices. It helps an organization to better understand, manage, and reduce its cybersecurity risks and can assist in determining which activities are most important to assure critical operations and service delivery. In turn, that will help to prioritize investments and maximize the impact of each dollar spent on cybersecurity. By providing a common language to address cybersecurity risk management, it is especially helpful in communicating inside and outside the organization. That includes improving communications, awareness, and understanding between and among IT, planning, and operating units, as well as senior executives. Organizations also can readily use the Framework to communicate the current or desired cybersecurity posture between a buyer or supplier.

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, describes a process to manage cybersecurity risk. The process details individual steps to Frame, Assess, Respond, and Monitor cybersecurity risk, in alignment with ISO 31000, 31010, 27001, and 27005. The process is supported by descriptions of key high-level cybersecurity risk management roles and responsibilities. Similar to the Cybersecurity Framework, SP 800-39 defines cybersecurity risk management at enterprise, business process, and system levels. The publication is foundational for coordinating those multiple levels of personnel to manage cybersecurity risk.

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, details a process to provision secure systems. The six-step Risk Management Framework (RMF) coordinates inter-related risk management standards and guidelines to provision appropriate security controls for a given system. The process shows detailed steps and substeps to implement, authorize, and manage system security controls. The

RMF utilizes the SP 800-39 roles to coordinate multiple Levels of personnel to provision secure systems.

Preliminary Guidance Analysis

As displayed in Figure 1, the requirements reconciliation process is critical for managing cybersecurity risk. Many cybersecurity requirements originate from mission objectives, laws, regulation, and policy. These must be aligned and deconflicted so that organizational cybersecurity dependencies become apparent. The requirements are then integrated into organizational cybersecurity risk management strategy and supportive activities. Those same requirements inform decision making about provisioning secure systems. Finally, provisioning secure systems is a foundational component to managing cybersecurity risk.

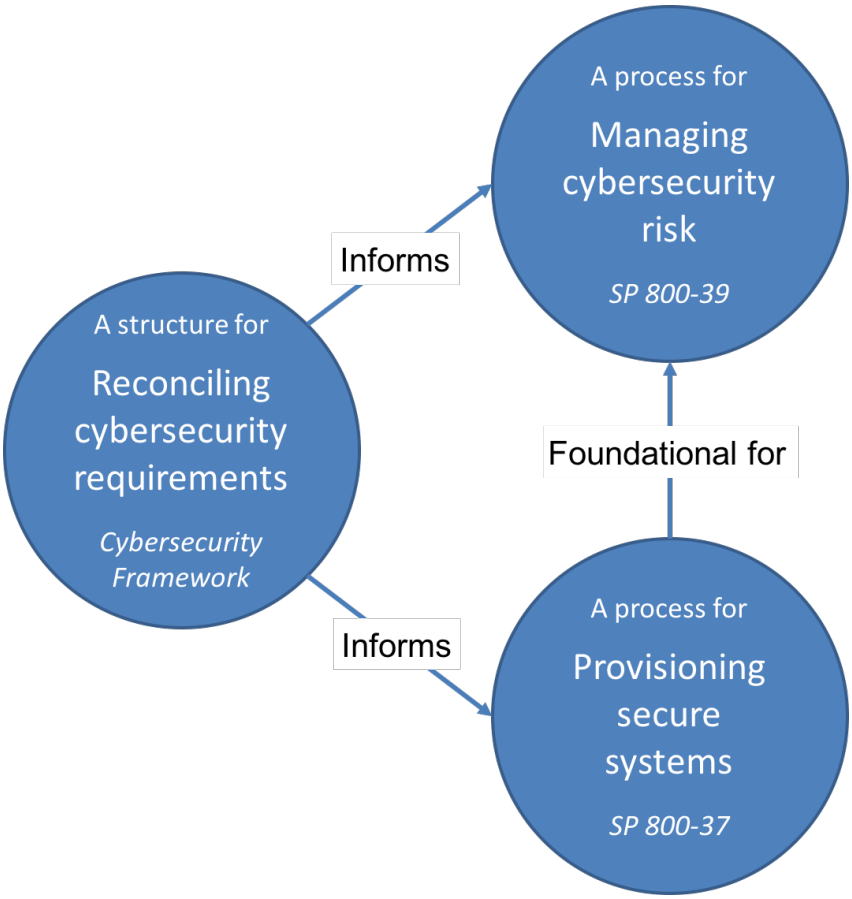

Figure 1: Relationships of Key NIST Risk Management Guidance

Basis for Document Alignment

The complex relationships among organizational missions, mission/business processes, and the systems supporting those missions/processes require an integrated view for managing risk. NIST SP 800-39 provides guidance for an integrated, organization-wide program for managing information security risk. To integrate the risk management process throughout the organization,

three levels of risk management are defined: (i) *organization*; (ii) *mission/business processes*; and (iii) *system*. Figure 2 illustrates the organization-wide multi-level risk management structure.

Figure 2: Special Publication 800-39 Multi-Level Risk Management

The three respective levels of cybersecurity risk management described in the Cybersecurity Framework and SP 800-39 are equivalent. The SP 800-39 Levels and roles are referenced throughout the SP 800-37. The equivalence of the Cybersecurity Framework and SP 800-39 organizational levels, and the current alignment of SP 800-37 with the SP 800-39 Levels, help to illustrate the alignment of organizational levels across all three RM publications.

Additionally, the SP 800-39 provides process and roles for cybersecurity risk management. The Cybersecurity Framework provides a structure for organizing cybersecurity risk management through activities like reconciling cybersecurity requirements.

NIST Risk Management Framework

The organization-wide risk management process of SP 800-39 is central to administering the RMF's six-step process in alignment with business/mission objectives and architectural considerations, as shown in Figure 3.

Figure 3: Cybersecurity Risk Management Framework described in NIST SP 800-37

The RMF provides a method of coordinating the inter-related risk management standards and guidelines described below:

- **Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems,*** is a standard for categorizing information and systems based on the potential impact to an organization and its ability to accomplish its mission, protect assets, fulfill its legal responsibilities, and maintain day-to-day functions. FIPS Publication 199 requires federal agencies to categorize their systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Federal agencies use **Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,*** to identify all information types processed, stored, or transmitted by these systems. Each identified information type has an impact value (low, moderate, or high) assigned for each of the security objectives of confidentiality, integrity, and availability.

- **FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,*** specifies (i) minimum security requirements for information and systems supporting executive agencies of the federal government and (ii) a risk-based process for selecting the security controls necessary to satisfy the minimum security

requirements. This standard promotes the development, implementation, and operation of more secure systems within the federal government by establishing minimal levels of due diligence and facilitates a more consistent, comparable, and repeatable approach for selecting and specifying security controls for systems.

- **SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,*** provides a comprehensive catalog of security and privacy controls and a process for selecting controls to protect organizational operations, assets, individuals, and other organizations from a diverse set of threats. The controls are customizable and implemented as part of an organization-wide process to manage information security and privacy risk. SP 800-53 also provides a methodology to develop specialized sets of controls, or overlays, tailored for specific types of mission/business functions, technologies, or environments of operation. **SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations***, provides a set of procedures for conducting assessments of the information security and privacy controls in SP 800-53.
- **SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,*** provides guidelines for applying the Risk Management Framework (RMF) to federal systems. The RMF promotes the concept of near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes. It provides senior leaders the information to make risk-based decisions for their systems, integrating information security into enterprise architecture and the system development lifecycle. The document describes how to apply the RMF to systems through a six-step process, including:

  (i) the categorization of information and systems;

  (ii) the selection of controls;

  (iii) the implementation of controls;

  (iv) the assessment of control effectiveness;

  (v) the authorization of the system; and

  (vi) ongoing monitoring of controls and the security state of the system.

- **SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations,*** supports the ongoing monitoring of security controls and the security state of systems. 800-137 provides guidance on developing an agency-wide information security continuous monitoring (ISCM) strategy and implementing an ISCM program. An ISCM program assists federal agencies in making informed risk management decisions by providing ongoing awareness of threats, vulnerabilities, and security control effectiveness.

- **SP 800-39, *Managing Information Security Risk*,** provides guidance for an integrated, organization-wide program for managing information security risk resulting from the operation and use of federal systems. The publication describes a multi-level approach to risk management and applying risk management concepts across an organization. The approach includes three distinct organizational levels[13]: the organization level; the mission/business process level; and the system level. The application of risk management processes among these levels is described in four key steps: "Framing Risk," "Assessing Risk," "Responding to Risk," and "Monitoring Risk." The risk management process is carried out seamlessly across the three levels, with the overall objective of continuous improvement in the organization's risk-related activities and effective communication within and across the three levels.

- **SP 800-30, *Guide for Conducting Risk Assessments*,** provides guidance for conducting risk assessments of federal systems and organizations. This document provides guidance for carrying out each of the steps in the risk assessment process and how risk assessments and other organizational risk management processes complement and inform each other. SP 800-30 also provides guidance to organizations on identifying specific risk factors to monitor on an ongoing basis. These monitoring activities enable organizations to determine whether risks have increased to unacceptable levels and to implement appropriate risk responses.

Federal agencies use the RMF to "develop, document, and implement an agency-wide program to improve the security of its information and systems that support the operations and assets of the agency.[15]"

The Cybersecurity Framework

The three primary components of the Cybersecurity Framework are the **Core**, **Implementation Tiers**, and **Profiles**.

One of the central features of the Cybersecurity Framework is its ability to translate highly technical and specialized cybersecurity language to a standardized language that experts outside of cybersecurity can understand. This allows a larger team of experts to participate in cybersecurity risk management dialogs and to incorporate considerations of cybersecurity more broadly as part of how an organization manages its risks . The **Cybersecurity Framework Core** is the structure that enables that translation. Specifically, it provides a set of specific cybersecurity outcomes and reference examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform; rather, it presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk. The Core itself is composed of four elements: Functions, Categories, Subcategories, and Informative References.

[13] SP 800-39 uses the term "Tier." To avoid confusion between the Cybersecurity Framework "Implementation Tiers" and the SP 800-39 organizational Tiers are referred to as "Levels" in this document.

The Cybersecurity Framework *Functions* – Identify, Protect, Detect, Respond, and Recover – provide a high level risk management vocabulary that is meaningful to cybersecurity experts and accessible to non-cybersecurity experts. For this reason, the Functions are applicable to both cybersecurity risk management and enterprise risk management, where cybersecurity is considered along with other organizational concerns. As illustrated in the Figure 4, the "bow tie" risk diagram,[14] the five Functions also balance prevention and reaction, including preparatory activities to enable the best possible outcome from that reaction. This balance allows Functions to act as a high level expression of risk management strategy and structure for risk assessment.

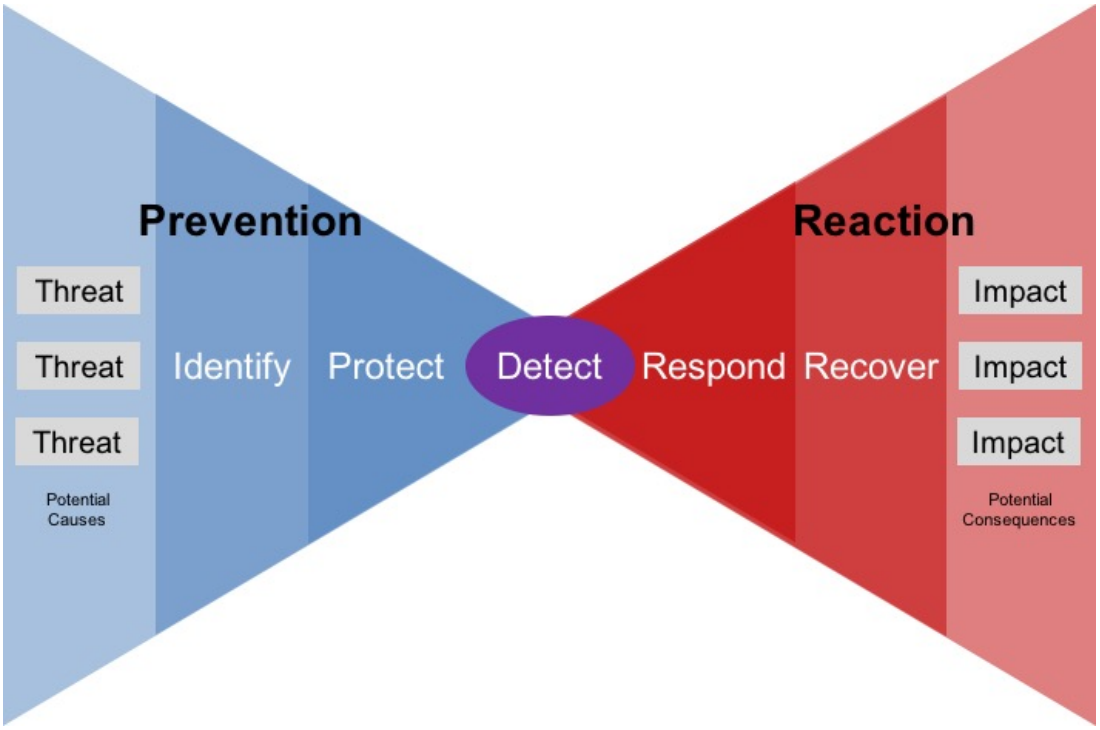

Figure 4: Balancing Organizational Focus with Cybersecurity Framework Functions

While Functions are often depicted linearly, the outcomes and dependencies associated with each Function can be iterative and often non-sequential. For example, continuous process improvements and lessons learned from the Respond and Recover Functions can inform the Protect Function. These data may be coupled with new best practices and information sharing from other organizations that also inform federal agency considerations for continuous process improvement in the Prevent Function.

The rest of the Cybersecurity Framework Core is subordinate to the Functions, and is composed of Categories, Subcategories, and Informative References. The Core hierarchy depicted in Figure 5 ensures a frame of reference. This greatly enriches the context of cybersecurity conversations or documents.

[14] Bow tie diagrams are commonly used to represent all hazards, and proactive and reactive measures to address those hazards. This type of visualization may be helpful when considering cybersecurity along side of other enterprise concerns.

Figure 5: The Cybersecurity Framework Core

Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes." *Subcategories* further divide a Category into specific outcomes of technical and/or management activities. Each subcategory is supported by one or more *Informative References*, which are specific sections of standards, guidelines, and practices that illustrate a method to achieve the outcomes described.

Using the Core taxonomy of Functions, Categories, and Subcategories, the Cybersecurity Framework fosters communication within and among the levels of an organization. The Cybersecurity Framework provides a common language among the representatives of various units of an organization and between organizations, including partners and suppliers. This helps to align a shared vision of security outcomes.

Another key feature of the Cybersecurity Framework is the qualitative measurement of organizational risk practices or behaviors. This allows organizations to identify their desirable behaviors, measure current behaviors, determine gaps, and work to improve.

The **Cybersecurity Framework Implementation Tiers** provide a method for organizations to view cybersecurity risk behaviors and the processes for managing risk. The Implementation Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They also describe the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. The Cybersecurity Framework characterizes three distinct cybersecurity risk management practices:

- *Risk Management Process* – a reflection of cybersecurity risk management within an organization.
- *Integrated Risk Management Program* – the consideration of cybersecurity alongside of other organizational concerns.
- *External Participation* – The bi-directional flow and consideration of information to better organizational Risk Management Process and Integrated Risk Management Program, as well as the Risk Management Processes and Integrated Risk Management Programs of other organizations.

While organizations identified as Implementation Tier 1 (Partial) are encouraged to consider moving toward Implementation Tier 2 or greater, *Implementation Tiers do not represent maturity levels*. Progression to higher Implementation Tiers is encouraged when the reduction in cybersecurity risk is deemed to be appropriate and cost-effective.

Cybersecurity Framework Profiles can be used to describe the current state and/or the desired target state of specific cybersecurity activities. They enable users to draw upon the Framework Core outcomes, while supporting ways to customize those outcomes to organization-specific missions, regulatory requirements, and operating environments. Profiles support business/mission requirements and aid in communicating risk within and between organizations. *Current Profiles* indicate the cybersecurity outcomes that are now being achieved. *Target Profiles* indicate the outcomes needed to achieve the desired cybersecurity risk management goals.

Comparison of Current and Target Profiles may reveal gaps and corresponding improvements needed to meet cybersecurity risk management objectives. The organization's business needs and risk management processes drive a mitigation priority for gaps. This risk-based approach enables an organization to estimate resources needed (e.g., staffing, funding) to set cybersecurity goals that can be achieved in a cost-effective, prioritized manner.

Figure 6 depicts Business/Process personnel within an organization evaluating Profile gaps, prioritizing the sequence of gap mitigation, determining mitigation resources, and coordinating mitigation with Implementation/Operations level personnel. In all instances, the central artifacts and work products are Profiles.

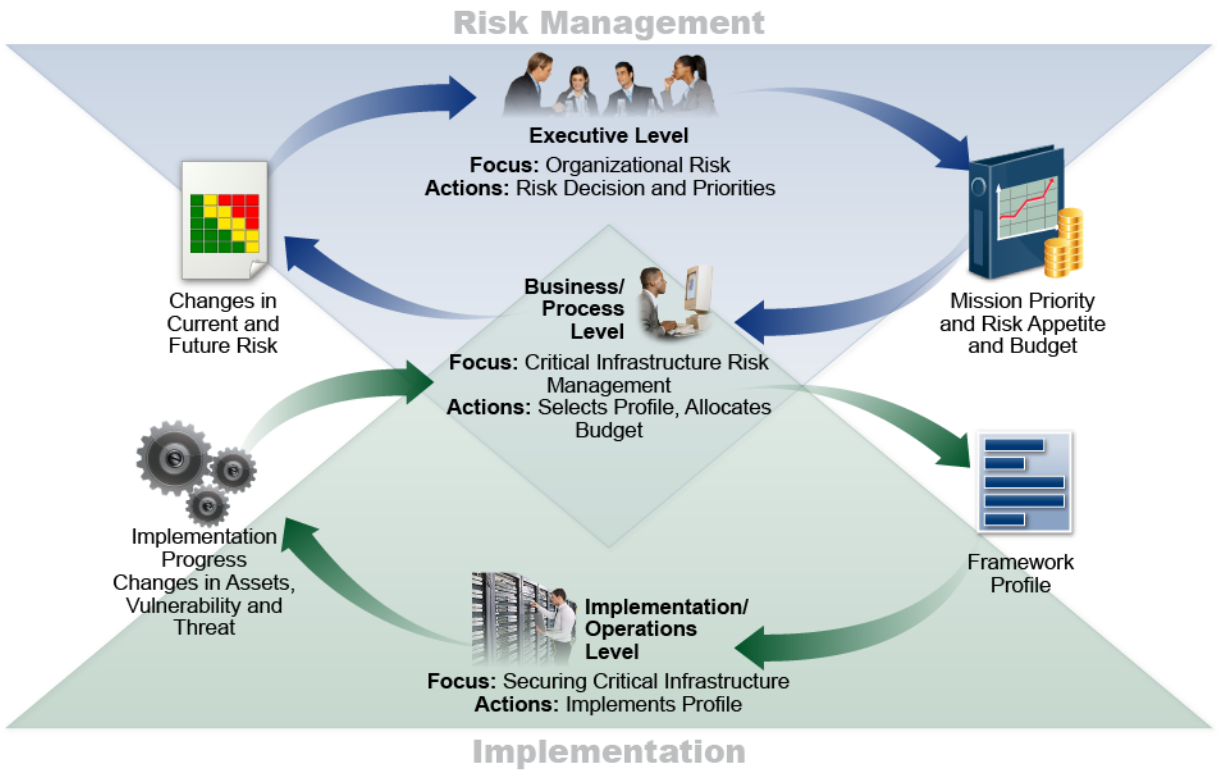

Figure 6: Notional Information and Decision Flows within an Organization

Appendix B—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

AO	Authorizing Official
CI	Critical Infrastructure
CISO	Chief Information Security Officer
EO	Executive Order
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002, as amended
HIPAA	Health Insurance Portability and Accountability Act
HVA	High Value Asset
ISCM	Information Security Continuous Monitoring
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RFC	Request for Comment
RFI	Request for Information
RMF	Risk Management Framework
SAR	Security Assessment Report
SP	Special Publication
SSP	System Security Plan

Appendix C—Glossary

Agency	See *Executive Agency*
Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Chief Information Security Officer	See *Senior Agency Information Security Officer*
Common Control [NIST SP 800-37]	A security control that is inherited by one or more organizational information systems. See *Security Control Inheritance*.
Common Control Provider [NIST SP 800-37]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).
Cybersecurity [CNSSI 4009]	The ability to protect or defend the use of cyberspace from cyber attacks.
Enterprise [CNSSI 4009]	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See *Organization*.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 United States Code (U.S.C.), Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

Federal Agency	See *Executive Agency*
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
High Value Asset [OMB M-17-09]	Those assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy – or to the public confidence, civil liberties, or public health and safety of the American people.
Hybrid Security Control [NIST SP 800-53]	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.
Information [CNSSI 4009] [FIPS 199]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. An instance of an information type.
Information Security [44 U.S.C., Sec 3541]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information System [44 U.S.C., Sec 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Security Officer	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.

Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements). See *Enterprise*.
Plan of Action and Milestones or POA&M [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Risk [CNSSI 4009]	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. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.]

Risk Executive (Function) [CNSSI 4009]	An individual or group within an organization that helps to ensure that: (i) security risk -related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management [CNSSI 4009, adapted]	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Register	A central record of current risks for a given scope or organization. Current risks are comprised of both accepted risks and risk that are have a planned mitigation path (i.e., risks to-be-eliminated as annotated in a POA&M)
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Security Control Inheritance [CNSSI 4009]	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.
Security Controls [FIPS 199, CNSSI 4009]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan.*
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.]
System	See *Information System*
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system.
Tailoring [NIST SP 800-53, CNSSI 4009]	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.
Threat [CNSSI 4009]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Appendix D—References

[1] Federal Information Security Modernization Act of 2014, Pub. L. 107-347 (Title III), 116 Stat 2946. https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

[2] Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat 2946. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[3] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication (SP) 800-39, March 2011. http://dx.doi.org/10.6028/NIST.SP.800-39

[4] Joint Task Force Transformation Initiative, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication (SP) 800-37 Revision 1, February 2010. http://dx.doi.org/10.6028/NIST.SP.800-37r1

[5] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity- framework-021214.pdf

[6] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[7] Cybersecurity Enhancement Act of 2014, Pub. L. 113-274. https://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf

[8] Office of Management and Budget (OMB), *Fiscal Year2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB Memorandum 14-04, November 18, 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

[9] The White House, Circular A-130, *Managing Federal Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revis ed.pdf

[10] U.S. Department of Commerce, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199, February 2004. http://dx.doi.org/10.6028/NIST.FIPS.199

[11] K. Stine, R. Kissel, C. Barker, J. Fahlsing, J. Gulick, *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST

Special Publication (SP) 800-60, Revision 1, August 2008. http://dx.doi.org/10.6028/NIST.SP.800-60v1r1

[12] U.S. Department of Commerce, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 200, March 2006. http://dx.doi.org/10.6028/NIST.FIPS.200

[13] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

[14] Joint Task Force Transformation Initiative, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53A Revision 4, December 2014. http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

[15] K. Dempsey, N. Chawla, A. Johnson, R. Johnston, A. Jones, A. Orebaugh, M. Scholl, K. Stine, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-137, September 2011. http://dx.doi.org/10.6028/NIST.SP.800-137

[16] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST Special Publication (SP) 800-30 Revision 1, September 2012. http://dx.doi.org/10.6028/NIST.SP.800-30r1

[17] J. Boyens, C. Paulsen, R. Moorthy, N. Bartol, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-161, April 2015. http://dx.doi.org/10.6028/NIST.SP.800-161

[18] R. Ross, P. Viscuso, G. Guissanie, K. Dempsey, M. Riddle, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST Special Publication (SP) 800-171, June 2015. http://dx.doi.org/10.6028/NIST.SP.800-171

[19] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security management systems*, ISO/IEC 27001:2013, September 2013. https://www.iso.org/standard/54534.html [accessed on 3/10/17]

[20] Information Systems Audit and Control Association (ISACA), Control Objectives for Information and Related Technology (COBIT) version 5 [Web site], https://www.isaca.org/cobit [accessed on 3/10/17].

[22] Office of Management and Budget (OMB), *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, OMB Memorandum 16-04, October 30, 2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

803