NISTIR 8170

Approaches for Federal Agencies to Use the Cybersecurity Framework

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8170-upd

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

NISTIR 8170

Approaches for Federal Agencies to Use the Cybersecurity Framework

Matt Barrett*
Jeff Marron
Applied Cybersecurity Division
Information Technology Laboratory

Victoria Yan Pillitteri
Jon Boyens
Stephen Quinn
Computer Security Division
Information Technology Laboratory

Greg Witte
Larry Feldman
Huntington Ingalls Industries
Annapolis Junction, MD

**Former employee; all work for this publication was done while at NIST*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8170-upd

March 2020
INCLUDES UPDATES AS OF 08-17-2021; SEE PAGE VI

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

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

National Institute of Standards and Technology Interagency Report 8170
33 pages (March 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8170-upd

Comments on this publication may be submitted to:

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

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.

Abstract

The document highlights examples for implementing the *Framework for Improving Critical Infrastructure Cybersecurity* (known as the Cybersecurity Framework) in a manner that complements the use of other NIST security and privacy risk management standards, guidelines, and practices. These examples include support for an Enterprise Risk Management (ERM) approach in alignment with OMB and FISMA requirements that agency heads "manage risk commensurate with the magnitude of harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of a federal information system or federal information." The use of the Cybersecurity Framework's components enable discussion about the various types of risk that might occur within federal organizations and promote conversations about how to determine the likelihood and potential consequences of risk events. These activities can then be combined with those described in NIST Special Publication (SP) 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*; SP 800-39, *Managing Information Security Risk*; and other guidelines to form a comprehensive risk-based approach for security and privacy.

This risk-based approach will assist agencies in determining the risks that are relevant to its mission throughout the operational lifecycle and apply an appropriate type and degree of resources to treat those risks to an acceptable level. Examples in this publication will demonstrate the use of the Cybersecurity Framework, the NIST Risk Management Framework (RMF), and other models to evaluate and report agency goals and progress and to inform tailoring activities for managing cybersecurity risk appropriately. Use of a comprehensive cybersecurity risk-based approach, as demonstrated through these examples, supports agencies' activities to meet their concurrent obligations to comply with the requirements of FISMA and Executive Order (EO) 13800.

Keywords

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

Acknowledgments

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

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.

Document 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. The Federal Information Security Management Act of 2002 was updated through the Federal Information Security Modernization Act of 2014 [1] [2].

The term "Tiers" cited in NIST Special Publication (SP) 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. Upcoming revisions of SP 800-39 will use the term "Levels" consistently [3].

The seven steps of the RMF described in NIST SP 800-37, Revision 2—Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor—are indicated using capital letters. This convention includes many conjugations in the context of those RMF steps (e.g., Authorize, Authorizing, and Authorized all refer to the *Authorize* step of the RMF) [4].

"Cybersecurity Framework" refers to version 1.1 of the *Framework for Improving Critical Infrastructure Cybersecurity*, issued in April 2018 [5].

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

For the purposes of this document, the terms "enterprise risk management" and "organization-wide risk management" are used interchangeably. These terms and the term 'risk register' are discussed in greater detail in Draft NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, released March 19, 2020.

Executive Summary

All federal agencies are entrusted with safeguarding the information contained in their systems and ensuring that those systems operate securely and reliably. It is vital that agency personnel at all levels manage their assets wisely and address cybersecurity risks effectively. To do that, agencies need a holistic approach to their enterprises' risk management that includes timely, streamlined approaches and automated tools.

As part of its statutory responsibilities under the Federal Information Security Management Act as amended (FISMA), the National Institute of Standards and Technology (NIST) develops standards and guidelines—including minimum requirements—to provide adequate information security for federal information and information systems [1]. This suite of security and privacy risk management standards and guidelines provides guidance for an integrated, organization-wide program to manage information security risk.

NIST produced this report to assist federal agencies in strengthening their cybersecurity risk management processes by highlighting example approaches for implementing the *Framework for Improving Critical Infrastructure Cybersecurity* (known as the Cybersecurity Framework) [5]. Developed by NIST in close collaboration with private and public sectors, the Cybersecurity Framework is a risk-based approach used voluntarily by organizations across the United States. Initially developed to address cybersecurity challenges in the Nation's Critical Infrastructure (CI) sectors, the voluntary Framework is used by a variety of organizations across the world. The Cybersecurity Framework aligns with and complements NIST's suite of security and privacy risk management standards and guidelines.

This report illustrates eight example approaches through which federal agencies can leverage the Cybersecurity Framework to address common cybersecurity-related responsibilities. By doing so, agencies can integrate the Cybersecurity Framework with key NIST cybersecurity risk management standards and guidelines that are already in wide use. These eight approaches support a mature agency-wide cybersecurity risk management program:

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 and cybersecurity approaches described in this document are intended to promote more effective risk management and to encourage dialogue within and among federal agencies.

Table of Contents

List of Appendices

Errata

This table contains changes that have been incorporated into NIST Interagency or Internal Report (NISTIR) 8170. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates for this document that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified; see the NISTIR 8170 publication details.

Date	Type	Change	Pages
08-17-2021	Substantive	Footnote 3 has been updated with the most current NIST information regarding Risk Appetite and Risk Tolerance and refers stakeholders to two relevant NISTIRs: "For a more complete discussion and guidance on Risk Appetite and Risk Tolerance, see the NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* and series documents, especially NISTIR 8286A *Identifying and Estimating Cybersecurity Risk for Enterprise Risk*."	6

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 support information security for agency operations and assets. NIST guidelines fulfill the requirements of FISMA and Office of Management and Budget (OMB) Circular A-130, and are used by agencies to develop, implement, and maintain cybersecurity and privacy programs [6]. They include Federal Information Processing Standards (FIPS), Special Publications (SPs), and NIST Interagency Reports (NISTIRs).

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. The frameworks' subsequent widespread use and adoption demonstrates their universal applicability [7]. That statute's assignments included work that NIST began in February 2013 as a result of Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity* [8], which directed the Department of Commerce to lead the development of a voluntary framework to reduce CI cybersecurity risks. Accordingly, NIST convened industry, academia, and government sectors to develop the *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 [5]. It offers a high-level vocabulary for cybersecurity risk management along with a set of cybersecurity outcomes and a methodology to assess and manage those outcomes.

The increasing frequency, creativity, and variety of cybersecurity attacks means that all organizations should place great emphasis on managing cybersecurity risk as a part of their Enterprise Risk Management (ERM) programs to fulfill their mission and business objectives. By integrating the Cybersecurity Framework with 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.[1]

1.1 Audience

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

[1] While this report is intended to help federal agencies 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.

choose to use the NIST cybersecurity risk management suite of standards and guidelines will benefit from this document.

1.2 Organization of this report

The remainder of this document is structured as follows:

- Section 2 provides guidance that includes eight approaches for 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.
- The References section provides links to external sources of additional information.
- Appendix A lists and explains acronyms that appear in the document.
- Appendix B defines key terms.

2 Example Approaches

Using eight example approaches, this section provides guidance to assist federal agencies as they develop, implement, and continuously improve their cybersecurity risk management programs. The examples are consistent with OMB Circular A-130, *Managing Information as a Strategic Resource* [6], which provides guidance regarding the heavily used NIST Risk Management Framework [4], associated documents, and the Cybersecurity Framework [5]. The examples also support OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*; use of the Cybersecurity Framework helps to identify, manage, report, and monitor the internal controls needed to properly manage potential information and technology risks to an agency [9].

OMB Guidance Regarding Enterprise Risk Management

The U.S. Office of Management and Budget (OMB) evaluates, formulates, and coordinates management procedures and program objectives within and among federal departments and agencies. In that role, OMB provides guidance in the form of memoranda to federal managers regarding the management of risks (including information and technology risks) that may impact achievement of strategic objectives and that arise from agencies' activities and operations.

Circular A-130, Appendix III
Responsibilities for Protecting Federal Information Resources, Section 4.n

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.

OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

Purpose: This Circular defines management's responsibilities for enterprise risk management (ERM) and internal control. The Circular provides updated implementation guidance to federal managers to improve accountability and effectiveness of federal programs as well as mission-support operations through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness. The Circular emphasizes the need to integrate and coordinate risk management and strong and effective internal control into existing business activities and as an integral part of managing an agency.

NIST will work with federal agencies to assess the value of these eight approaches, identify additional examples, and understand how to better illustrate applications of the Cybersecurity Framework. Feedback will inform NIST as it incorporates Cybersecurity Framework concepts into cybersecurity risk management publications.

The approaches described in this publication demonstrate how agencies can leverage both the Cybersecurity Framework and the NIST Risk Management Framework (RMF) 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.

Similarly, the RMF also demonstrates this bilateral relationship. For example, every task within the *Prepare* step of the RMF aligns with the Cybersecurity Framework Core. Specifically, the P-2 Risk Management Strategy aligns with the Cybersecurity Framework Core [Identify Function at ID.RM; ID.SC]. Other RMF examples include: Task P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles, aligns with the Cybersecurity Framework Profile construct; and Task R-5, Authorization Reporting, and Task M-5, Security and Privacy Reporting, support OMB reporting and risk management requirements organization-wide by using the Cybersecurity Framework constructs of Functions, Categories, and Subcategories.[2]

Alignment between the Cybersecurity Framework and RMF is also detailed in the following two figures. The RMF describes three levels of organizational management as illustrated in Figure 1.

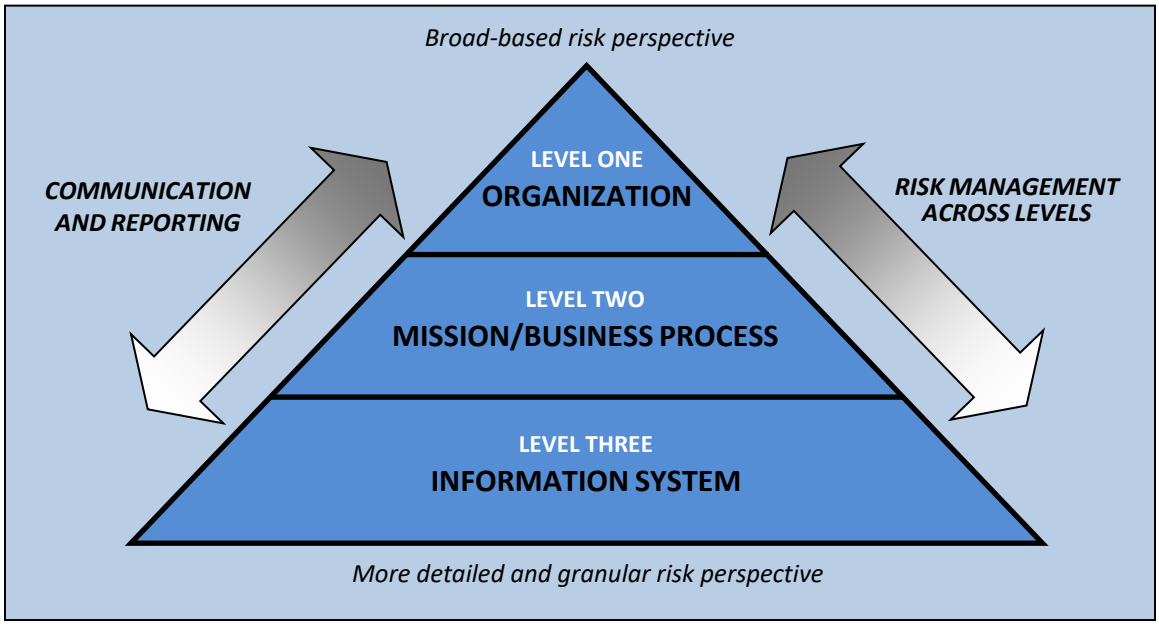

Figure 1: Organization-Wide Risk Management Approach

[2] The Subcategory mappings to the [SP 800-53] controls are available at: https://www.nist.gov/cyberframework/federal-resources.

Figure 2 depicts federal cybersecurity risk management approaches (middle column) as aligned with these three levels. Most of the approaches addressed in this publication comport with the "Mission/Business Processes" (Level 2). One approach exemplifies use of the Cybersecurity Framework at the "Organization" level (Level 1), and another addresses the "System" level (Level 3). The order of the approaches is not intended to imply criticality or priority. Agencies can prioritize implementation to best support their own cybersecurity needs.

In the right column, Figure 2 depicts the most applicable Cybersecurity Framework component—Core, Profile(s), or Implementation Tiers—for a given federal use.

Special Publication 800-37 Rev. 2 Levels				Cybersecurity Framework Components
	Level 1 Organization	**Integrate enterprise and cybersecurity risk management** by communicating with universally understood risk terms.	Core	
	Level 2 Mission/Business Processes	**Manage cybersecurity requirements** using a construct that enables integration and prioritization of requirements.	Profile(s)	
		Integrate and align cybersecurity and acquisition processes by relaying cybersecurity requirements and priorities in 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.	Profile(s)	
		Maintain a comprehensive understanding of cybersecurity risk using a standard organizing structure.	Core	
		Report cybersecurity risks using a universal and understandable structure.	Core	
	Level 3 System	**Inform the tailoring process** using a comprehensive reconciliation of cybersecurity requirements.	Profile(s)	

Figure 2: Federal Cybersecurity Approaches

Since the Cybersecurity Framework uses risk management processes to inform and prioritize organizations' cybersecurity decisions, it can be adapted to provide a flexible, risk-based implementation that can be used with a broad array of risk management processes. That includes not only SP 800-37 Rev. 2 cited above, but also SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [3] which describes the risk management process and four distinct steps – Frame, Assess, Respond, and Monitor – used by federal organizations, and optionally employed by private sector organizations.

1. Integrate Enterprise and Cybersecurity Risk Management

Organizations manage many types of risk. They develop policies to identify, assess, and mitigate adverse effects with cybersecurity dependencies across various types of enterprise risks. In addition to cybersecurity risks, other typical enterprise risks include safety, financial, program, acquisitions, supply chain, and privacy. Many of these other types of risk may also have cybersecurity risk implications or be impacted by cybersecurity. Some employ different terminologies and risk management approaches to make decisions. OMB Circular A-123 establishes an expectation for federal agencies to proactively consider and address risks through an integrated, organization-level view of events, conditions, or scenarios that impact mission achievement. Organizations may have established a unique lexicon for ERM that should be

considered when communicating risks at the organization level. This necessitates coordination with existing Enterprise Risk Management (ERM) functions on how to best incorporate and communicate cybersecurity risks at the organization and system levels.

The Cybersecurity Framework Core's five "Functions"—Identify, Protect, Detect, Respond, and Recover—offer a way to organize cybersecurity risk management activities at their highest levels that can be applied across risk management disciplines. These same five words are further classified into more specific meanings with the Cybersecurity Framework Core, enabling precise and efficient implementation of any enterprise risk decisions impacting cybersecurity. Many stakeholders from various parts of an organization can understand and may already use these five words in the context of risk decisions. Different disciplines communicate risk at differing levels of breadth and depth, so the Cybersecurity Framework outcomes help facilitate discussions.

While Chief Information Security Officers (CISOs) and other cybersecurity professionals in federal agencies are encouraged to use these five functions as a way to engage, organize, and explain cybersecurity approaches to the agency's external stakeholders, executive leadership, and employees and to integrate cybersecurity concepts into other organizational areas, traditional risk management language and concepts should likewise be communicated to the more technical ranks of the organization. The five Functions offer an organizing principle for CISOs to gather risk tolerance[3] perspectives from system owners and functional leads while preparing to engage strategies to address risk considerations at a higher level in the organization.

When representatives across an enterprise are engaged in identifying and prioritizing organizational assets and determining risk management strategies supported by a common language, they are more likely to achieve the desired outcomes.

Summary of the Approach: Integrate Enterprise and Cybersecurity Risk Management

<table>
<tr><td rowspan="2">Benefit(s):
Facilitate communication among agency stakeholders, including executive leadership.
Facilitate a common language to inform and be informed by other risk management disciplines.</td><td>Primary SP 800-37 Level:
1 - Organization</td></tr>
<tr><td>Primary Cybersecurity Framework Component:
Core</td></tr>
<tr><td colspan="2">Summary: Using the Cybersecurity Framework's Functions (Identify, Protect, Detect, Respond, and Recover) as the basis for risk management dialogues related to the cybersecurity environment, organizations can raise awareness of cybersecurity and other risks to be managed and facilitate communication among agency stakeholders, including executive leadership.[4]
This use example aggregates elements of the activities of uses 2-8.</td></tr>
<tr><td colspan="2">Typical Participants: Head of Agency (Chief Executive Officer), Risk Executive (Function), Chief Information Officer (CIO), Senior Information Security Officer/Chief Information Security Officer</td></tr>
</table>

[3] For a more complete discussion and guidance on Risk Appetite and Risk Tolerance, see the NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* and series documents, especially NISTIR 8286A *Identifying and Estimating Cybersecurity Risk for Enterprise Risk.*

[4] Source: OMB A-130

(CISO), stakeholders representing other risk management disciplines (e.g., finance, human resources, privacy, 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. These include but are not limited to laws, regulations, oversight by and reports to Congress, internal policy, and OMB policies. Using Cybersecurity Framework Profiles, Federal agencies can manage requirements by integrating and prioritizing those requirements.

Agencies can align and merge internal and external requirements 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, and their own cybersecurity policy. Applicable excerpts of these laws, guidelines, policies, and objectives can be aligned with the various Functions, Categories, and Subcategories of the Core. That can help agencies to determine where requirements overlap and/or conflict so that they can consider alternative approaches—including modifying cybersecurity requirements within that agency's control.

The NIST Online Informative Reference (OLIR) Program also can assist federal agencies in implementing cybersecurity controls derived from multiple framework and guidance document requirements.[5] The growing OLIR catalog provides a listing of cross-framework control mappings, demonstrating similarities and differences between frameworks. This can help implementers to better understand competing and unrelated requirements so that they can more accurately focus their resources.

Still, it remains challenging to ensure a specific set of system configuration baseline settings is applied while maintaining compliance with multiple requirements (e.g., FISMA, HIPAA, PCI DSS, Special Publication 800-70 Revision 4, etc.). The NIST National Checklist Program provides a catalog of automated and implementable security settings to assist with the attestation trail from the applied setting to the framework.[6]

Stakeholder discussions regarding the Core outcomes help with prioritization. For instance, certain subcategory outcomes are meaningful for multiple requirements. It may also be clear that a short list of Subcategories is essential to achieve mission objectives. Where under investing in a given area might jeopardize those mission objectives, utilizing the structure of the Core as inputs can determine priorities and drive cybersecurity investments, effort, and focus.

[5] NIST OLIR homepage: https://www.nist.gov/cyberframework/informative-references.
[6] The NIST National Checklist Program at https://checklists.nist.gov/ and supporting content in SCAP format can assist with framework to setting assurance.

Summary of the Approach: Manage Cybersecurity Requirements

<table>
<tr><td>Benefit(s):
Determine where cybersecurity requirements overlap and/or conflict to ensure compliance and improve efficiency and effectiveness.
Prioritize Subcategory outcomes based on reconciling requirements, mission priorities, and the operational environment/threat information.
Operationalize cybersecurity activities based on the Cybersecurity Framework Profile.</td><td>Primary SP 800-37 Level: 2 – Mission/Business Processes

Primary Cybersecurity Framework Components: Core, Profile(s)</td></tr>
<tr><td colspan="2">Summary: Federal agencies can use the Cybersecurity Framework Core Subcategories to align and merge cybersecurity requirements that may overlap or fall between offices in the organizational structure. This reconciliation helps to ensure compliance and prioritize 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.</td></tr>
<tr><td colspan="2">Typical Participants: Risk Executive, Chief Information Officer (CIO), Senior Information Security Officer/Chief Information Security Officer (CISO)</td></tr>
<tr><td colspan="2">Primary NIST Documents: NIST Special Publication 800-39, Cybersecurity Framework</td></tr>
</table>

3. Integrate and Align Cybersecurity and Acquisition Processes

Federal agencies and contractors each have some cybersecurity and acquisition requirements in common, while others are organizationally specific.[7] In the acquisition process, this often causes a misunderstanding of expectations between federal agencies and contractors 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 risk management practices and to support federal agencies as they interact with suppliers, including 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 its market research prior to soliciting for and selecting a vendor. Respondents can be encouraged to include their Cybersecurity Framework Profile in the reply to a request for information or a sources sought notice. A reply describing cybersecurity capabilities of a product or service that includes Cybersecurity Framework terminology would help the agency to better compare and contrast the cybersecurity capabilities of organizations, products, and services of respondents.

Cybersecurity Framework Profile can be incorporated into the acquisition process as a foundation for 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 Cybersecurity Framework Profiles allows suppliers the flexibility to select from among various standards and practices to

[7] Compare FAR § 52.204-21, *Basic Safeguarding of Covered Contractor Information System*s (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).

meet federal agency-specific requirements while communicating their cybersecurity posture in a consistent way. It also provides agencies the means to consistently and objectively assess the cybersecurity posture of potential partners.

Summary of the Approach: Integrate and Align Cybersecurity and Acquisition Processes

<table>
<tr><td rowspan="2">Benefit(s):
Delineate which cybersecurity standards and practices to incorporate into contracts.
Provide a common language to communicate requirements to offerors and awardees (agreement/contract).
Provide offerors a mechanism to express their cybersecurity posture and related standards and practices.
Support inclusion of necessary cybersecurity controls and expectations within major IT acquisitions.
Improve the cybersecurity of federal systems.</td><td>Primary SP 800-37 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, products, and services. Cybersecurity Framework Profiles can be used by federal agencies to express technical requirements, and offerors can demonstrate how they meet or exceed these requirements.</td></tr>
<tr><td colspan="2">Typical Participants: Risk Executive (Function), Chief Information Officer (CIO), Senior Information Security Officer/Chief Information Security Officer (CISO), General Counsel, Contracting Office, mission/business owners, stakeholders representing other risk management disciplines (e.g., finance, human resources, purchasing)</td></tr>
<tr><td colspan="2">Primary NIST Documents: NIST Special Publications 800-39, 800-161 [10], 800-171 [11], Cybersecurity Framework</td></tr>
</table>

4. Evaluate Organizational Cybersecurity

The Cybersecurity Framework's Implementation Tiers are designed as an overarching measurement of cybersecurity risk management behaviors within an organization. They help an organization to consider the following cybersecurity properties on a scale from 1 to 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?

Implementation Tiers are not prescriptive, and there is no set requirement for an organization and all 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 so that the agency can afford to operate at Implementation Tier 4

elsewhere. One way that federal agencies may apply these trade-offs is via FIPS-199 categorizations [12]. An agency might view FIPS-199 High Impact and High Value Asset[8] (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 target Implementation Tier as well as steps that the organization can take to progress to a desired Tier. These gaps indicate that there is a difference between current and optimal cybersecurity risk management behaviors. Agency Implementation Tier targets may be influenced by external requirements, including OMB policies and OMB cross-agency priorities.

Summary of the Approach: 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 800-37 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 with a basis for rationalizing different aspects of cybersecurity operations across an organization. These decisions are based on trade-off analyses 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>
<tr><td colspan="2">Typical Participants: Head of Agency (Chief Executive Officer), Agency Deputy (Chief Operating Officer) Risk Executive, Chief Information Officer (CIO), Senior Information Security Officer/Chief Information Security Officer (CISO), stakeholders representing other risk management disciplines (e.g., finance, human resources, acquisition)</td></tr>
<tr><td colspan="2">Primary NIST Documents: NIST Special Publication 800-39, Cybersecurity Framework</td></tr>
</table>

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 is assigned, tracked, and measured and how personnel empowerment and accountability is managed.

The Cybersecurity Framework provides a way to assign cybersecurity responsibilities to units or individuals in an organization, including external entities with risk management roles. That allows executives to specify tasks, responsibilities, and risk management strategies. It also enables executives to empower units and individuals and to reward them appropriately. If parts

[8] High Value Asset is first referenced in OMB Memorandum M-16-04 and defined in M-17-09.

of cybersecurity operations are not performing as intended, or if risk is above set threshold levels, the Cybersecurity Framework structure helps managers trace and investigate the situation and hold relevant units and individuals accountable.

Using a Cybersecurity Framework Profile also may help identify opportunities for improving management of the organization's cybersecurity workforce and how it achieves defined risk tolerance outcomes. One way to do that is by applying the NICE Workforce Framework from the National Initiative for Cybersecurity Education (NICE), documented in SP 800-181 [13]. That workforce framework serves as a fundamental reference. It offers organizations a consistent lexicon for categorizing and describing cybersecurity work by category, specialty area, and work role, as well as a superset of cybersecurity knowledge, skills, and abilities (KSAs) and tasks for each work role. These elements support consistent organizational and sector communication for cybersecurity education, training, and workforce development. While the Cybersecurity Framework and the NICE Framework were developed separately, they complement each other by describing a hierarchical approach to achieving cybersecurity goals. The NICE program is in the process of determining alignment among Cybersecurity Framework subcategory outcomes and NICE Work Roles. As this work progresses, the alignment will help agencies document current and desired outcomes (based on Framework Core Subcategories) as well as the types of personnel that might have a role in accomplishing those outcomes. Furthermore, with the knowledge of the potential NICE work roles associated with a given set of outcomes, agencies will also be able to consider the NICE Framework's definition of tasks associated with those roles and the relevant knowledge, skills, and abilities. This may help agencies to better define personnel requirements, qualifications, and evaluation criteria.

In addition to determining the applicable work roles for a set of outcomes and associated security controls, the Cybersecurity Framework provides a manageable way to apportion responsibility for cybersecurity. Since the subcategory outcomes have already been mapped to the security controls in SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, the responsibility for implementing and maintaining corresponding controls can also be assigned to these roles [14].

When analyzing the desired cybersecurity outcomes associated with the Core's Categories and Subcategories, some outcomes may be managed centrally and more cost-effectively for the entire agency rather than separately by each organizational unit. For example, an agency may determine that it is most beneficial and cost-effective for the entire agency to make Subcategory PR.AC-2 (i.e., "physical access to assets is managed and protected") the responsibility of the Physical Security unit. These determinations can assist federal agencies in identifying candidates for 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 business units within agencies have key roles in identifying high-value assets and business processes. The ensuing discussions among business unit managers, the CISO, and other stakeholders regarding how to prioritize and protect these assets will likely recognize business units with similar assets or business processes that can utilize shared services. This can lead to the subsequent identification of common controls to secure assets and business processes across business units and potentially yield cost savings.

Summary of the Approach: Manage the Cybersecurity Program

<table>
<tr><td colspan="2">Benefit(s):
Provide an approach to delegate responsibility and authority for cybersecurity objectives within 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.</td><td>Primary SP 800-37 Level: 2 – Business/Mission Processes</td></tr>
<tr><td colspan="2"></td><td>Primary Cybersecurity Framework Component: Core</td></tr>
<tr><td colspan="3">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 can also assist agencies in identifying common and hybrid controls and saving resources.</td></tr>
<tr><td colspan="3">Typical Participants: Chief Information Officer (CIO), Senior Information Security Officer/Chief Information Security Officer (CISO), Common Control Provider</td></tr>
<tr><td colspan="3">Primary NIST Documents: NIST Special Publication 800-37, Cybersecurity Framework</td></tr>
</table>

6. Maintain a Comprehensive Understanding of Cybersecurity Risk

By aggregating cybersecurity findings, gaps, and vulnerabilities into a centralized record, agencies gain a combined view of cybersecurity risk and can make better informed 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 enables consistent reporting. In some organizations, this centralized record is referred to as a "risk register." OMB Circular A-11[9] describes a risk register as "a repository of risk information including the data understood about risks over time." A-11 further explains, "Typically, a risk register contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks" [15].[10]

Agencies often 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]

[9] The White House, Circular A-11, *Preparation, Submission, and Execution of the Budget*, June 2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11_web_toc.pdf

[10] The cybersecurity-based Risk Assessment Reports (RARs) described in NIST Special Publication (SP) 800-30 Rev.1 *Guide for Conducting Risk Assessments* contain supporting information about each risk identified in a cybersecurity risk register.

[11] Security Authorization artifacts and process are detailed in SP 800-37 Rev. 2, Appendix F, *System and Common Control Authorizations*.

By aggregating findings, agencies can:

- 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.

Industry users of the Cybersecurity Framework have noted that differing elements of the organization may not consistently apply risk criteria. Many organizations have risk determination models like those described in NIST Special Publication (SP) 800-30, Rev.1, *Guide for Conducting Risk Assessments* [18]. Discussions among stakeholders about risk scales and risk criteria may help the organization to improve consistency and awareness, which may in turn support improved application of the RMF tasks and related activities.

Using the Cybersecurity Framework, an organization can assemble system-level weaknesses or deficiencies into an enterprise-wide understanding of cybersecurity vulnerabilities. By discussing weaknesses or deficiencies that impact multiple systems or business units, the organization can develop consistent methods to identify, communicate, and plan mitigation activities. This information can be viewed at the Subcategory, Category, or Function level to provide agencies with additional context before making risk decisions and associated resource investments. While this integrated view may be helpful, agencies should exercise caution to prevent overextension of conclusions, especially if the impetus is to enable broad participation across the organization. The process of translating *system* risks into *organizational* risks should be thoroughly vetted by relevant cybersecurity experts to reduce distortions or oversimplifications before arriving at broader conclusions. Once the risk-rating mechanisms and processes are shown to be applied homogenously across systems, meaningful organization risks can be determined. Individual system risk ratings should first be shown to be objectively consistent and repeatable before broader implications can be considered reliable.

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 ongoing risk changes tracked through RMF Monitor activities. A cybersecurity risk register is a tool that helps the AO understand if accepting the system risk will drive overall risk beyond the organization's tolerance. Organizing a risk register using language from the Cybersecurity Framework Core enables a larger group of people to participate in and inform the authorization decision. In particular, the clear language of Functions and Categories of the Core enables broad participation.

Summary of Approach: Maintain a Comprehensive Understanding of Cybersecurity Risk

<table>
<tr><td colspan="2">Benefit(s):
Support discussions about how to consistently measure, assess, and report aspects of cybersecurity risk (e.g., evaluation of threats, likelihood, impact).
Assist federal agencies in gaining a better understanding of aggregate risk to enable RMF Authorization decisions.</td><td>Primary SP 800-37 Level: 2 – Mission/Business Processes</td></tr>
<tr><td colspan="2"></td><td>Primary Cybersecurity Framework Component: Core</td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td colspan="3">Typical Participants: Senior Information Security Officer/Chief Information Security Officer (CISO), Authorizing Official</td></tr>
<tr><td colspan="3">Primary NIST Documents: NIST Special Publication 800-37, Cybersecurity Framework</td></tr>
</table>

7. Report Cybersecurity Risks

With a cybersecurity risk register informed by the Cybersecurity Framework Core, an organization can efficiently generate risk reports. Reports often need to be distributed to a variety of audiences, including business process personnel who manage risk as 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 that reports need to be clear, understandable, and vary significantly in both transparency and detail, depending on the recipient and report requirement. Furthermore, reporting timelines need to match expectations of the receiving parties in order to minimize the time between the measurement of risk and delivery of the report. A standardized reporting format can assist agencies in meeting multiple cybersecurity reporting needs.

Today, risk reporting within federal organizations varies greatly and is performed using multiple technologies and reporting formats since different sources request information for different purposes. In part to address this variability, in recent years, the OMB has requested that annual FISMA metrics be 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.

Using standardized risk register categories such as the hierarchy of cybersecurity outcomes in the Core or the SP800-53 Control Families 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, thereby minimizing time and resources invested in generating the report.

Summary of Approach: Report Cybersecurity Risks

Benefit(s): • Provide expeditious, audience-appropriate, easy-to-understand, standardized reporting.	**Primary SP 800-37 Level:** 2 – Mission/Business Processes
	Primary Cybersecurity Framework Component: Core
Summary: The Cybersecurity Framework Core provides a reporting structure and language that aligns with SP 800-53 controls. This enables an easy roll-up of the 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 (CIO), 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 800-37, 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 as a high, moderate, or low impact (based on FIPS 199/SP 800-60), organizations leverage FIPS 200 to identify minimum security requirements associated with the system impact level [12][16][17]. 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 and supports improved reporting. (Also see Use Case 7, above.) Since Profiles can be a reconciliation of cybersecurity requirements and associated priorities from many sources, they can be used as a concise and important tool 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 can help in precisely adjusting the controls baseline in ways that best support the organizational mission.

Summary of Approach: Inform the Tailoring Process

<table>
<tr><td rowspan="2">Benefit(s):
• Provide a single document that reflects mission objectives and applicable agency cybersecurity requirements as a basis for tailoring initial system controls baselines.</td><td>Primary SP 800-37 Level:
3 – System</td></tr>
<tr><td>Primary Cybersecurity Framework Component:
Profile(s)</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td colspan="2">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)</td></tr>
<tr><td colspan="2">Primary NIST Documents: NIST Special Publication 800-53, Cybersecurity Framework</td></tr>
</table>

References

[1] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/content/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.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

[3] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[4] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

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

[6] The White House, Circular A-130, Managing Federal Information as a Strategic Resource, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[7] Cybersecurity Enhancement Act of 2014, Pub. L. 113-274, 128 Stat. 2971. https://www.govinfo.gov/content/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf

[8] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[9] The White House, Circular A-123, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[10] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[11] Ross RS, Dempsey KL, Viscuso P, Riddle M, Guissanie G (2016) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 1, Includes updates as of June 7, 2018. https://doi.org/10.6028/NIST.SP.800-171r1

[12] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

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

[14] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[15] The White House, Circular A-11, Preparation, Submission, and Execution of the Budget, June 2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11_web_toc.pdf

[16] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[17] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[18] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[19] International Organization for Standardization (ISO) (2009) Risk management – Vocabulary. ISO Guide 73:2009. https://www.iso.org/standard/44651.html

Appendix A—Acronyms

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

AO	Authorizing Official
CI	Critical Infrastructure
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
EO	Executive Order
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002, as amended, including the Federal Information Security Modernization Act
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
RAR	Risk Assessment Report
RFC	Request for Comment
RFI	Request for Information
RMF	Risk Management Framework
SAR	Security Assessment Report
SP	Special Publication
SSP	System Security Plan

Appendix B—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 Appetite	The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.

Risk Executive (Function) [NIST SP800-37]	An individual or group within an organization that helps to ensure that provides a comprehensive, organization-wide approach to risk management. The risk executive (function) serves as the common risk management resource for senior leaders, executives, and managers, mission/business owners, chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, common control providers, enterprise architects, security architects, systems security or privacy engineers, system security or privacy officers, and any other stakeholders having a vested interest in the mission/business success of organizations. The risk executive (function) is an inherent U.S. Government function and is assigned to government personnel only. (SP800-37 Revision 2)
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, and related information, 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). See OMB Circular A-11 for detailed information about risk register contents for Federal entities.
Risk Tolerance [NIST SP800-37]	Risk tolerance is the degree of risk or uncertainty that is acceptable to an organization.
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in Committee on National Security Systems (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.