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

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 https://csrc.nist.gov/publications.

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

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.

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

Executive Summary .... **iv**
1 Introduction **1**
1.1 Audience 1
1.2 Organization of this report 2
2 Example Approaches **3**
1. Integrate Enterprise and Cybersecurity Risk Management 5
2. Manage Cybersecurity Requirements 7
3. Integrate and Align Cybersecurity and Acquisition Processes 8
4. Evaluate Organizational Cybersecurity 9
5. Manage the Cybersecurity Program 10
6. Maintain a Comprehensive Understanding of Cybersecurity Risk 12
7. Report Cybersecurity Risks 14
8. Inform the Tailoring Process 15
References **17**

List of Appendices

Appendix A— Acronyms **19**
Appendix B— Glossary **20**

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.