Nuclear Regulatory Commission

# Risk Management Strategy

**September 22, 2020**

| | |
|---|---|
| Revision Number: | 1.0 |
| Primary Contact: | Kathy Lyons-Burke<br>Senior Level Advisor for Information Security |
| Responsible Organization: | OCIO |
| ADAMS Accession #: | |

| | |
|---|---|
| **Effective Date:** | 9/22/2020 |
| **Approved By:** | David Nelson<br>Chief Information Officer |

David J. Nelson

Digitally signed by David J.
Nelson
Date: 2020.09.22 11:34:22
-04'00'

# Table of Contents

# Cybersecurity Risk Management Strategy

## 1 INTRODUCTION

An effective cybersecurity risk management process is an important component of a successful information security program. The principal goal of the Agency cybersecurity risk management process is to protect the organization and its ability to perform its mission while safeguarding its information assets in cyberspace. Cybersecurity risk is one of many types of risk that the Agency manages, through its information security program and through other risk management activities under the broader umbrella of enterprise risk management (ERM). Cybersecurity risk (also referred to as cyber risk) is closely related to operational risk, reputation risk, information security risk, supply chain risk, and privacy risk; however, these other types of risks can materialize without involving cyberspace. Because this strategy focuses on cybersecurity risk management, uses of the term "risk" without further qualification in this document should be assumed to refer to cybersecurity risk.

This strategy and associated policies help guide Agency processes and procedures to establish and manage an effective risk management program. This strategy reflects the elevated priority of risk management in the Agency and links cybersecurity operations and assets to the overarching Agency missions, functions, and goals.

Risk cannot be eliminated. However, the risk management process allows senior managers and IT security professionals to balance the operational costs and the protective measures required to mitigate risks and achieve gains in mission capability. By employing practices and procedures designed to foster informed risk management, the Agency helps protect its information systems and the data that support the mission.

The risk management process is guided by the Federal Information Security Modernization Act (FISMA) of 2014, which along with Executive Order 13800, empowers the Chairman with the authority and accountability for information security and cyber risk management. FISMA charges the Chief Information Officer (CIO) with developing and maintaining an Agency-wide information security program on behalf of the Chairman.

This strategy:

- Establishes the context in which the Agency views and approaches risk;
- Emphasizes the importance of including cyber risk management in the system development lifecycle (SDLC);
- Defines the boundaries for risk appetites and tolerances; and
- Explains risk management roles and responsibilities.

The federal policy and guidelines that shaped the strategy are listed in Appendix A.

This strategy is intended to be a living document that is updated as laws, regulations, industry leading practices, and Agency needs dictate.

## 1.1 Purpose

This strategy provides a comprehensive approach for framing, assessing, responding to and monitoring risks associated with Agency information systems in accordance with Federal laws, regulations, and requirements.

The mission of the Agency is to license and regulate the Nation's civilian use of radioactive materials to provide reasonable assurance of adequate protection of public health and safety and to promote the common defense and security and to protect the environment. Our data is an invaluable asset that requires an enterprise-wide strategy which reflects the importance of the mission and guides executive decisions about risk.

## 1.2 Scope

This strategy:

- Applies to all Agency offices and regions, as well as other entities (e.g., service providers, contractors) operating systems at government locations or in the Cloud or other premises on behalf of the Agency;
- Can be tailored to specific mission and business processes; and
- Is limited to cybersecurity risks in support of the overall ERM Strategy.

This strategy covers all organizational levels:

**Level 1** – Organization.[1]

**Level 2** – Mission / Business Process

**Level 3** – Information System

# 2 GOVERNANCE

Good governance ensures:

- Execution of risk management processes to frame, assess, respond to, and monitor risk to organizational operations and assets, individuals, other organizations, and the Nation;
- Strategic alignment of risk management decisions with missions and business functions consistent with organizational goals and objectives;
- Effective and efficient allocation of risk management resources;
- Performance-based outcomes by measuring, monitoring, and reporting risk management metrics to ensure that organizational goals and objectives are achieved; and
- Delivered value by optimizing risk management investments in support of organizational objectives.

[1] Note: NISTIR 8170 replaced the word “tiers” in NIST 800-39 with the word “levels”.

This strategy integrates with the Agency's ERM program at Level 1, ensuring cyber risks are represented as appropriate on the Agency's Enterprise Risk Profile.

## 2.1 Roles and Responsibilities

Numerous individuals within the cybersecurity and Agency ERM programs support the Agency's cyber risk management efforts. Table 1 identifies specific roles and responsibilities for key personnel including the Senior Accountable Official for Risk Management (SAORM) and the Chief Information Security Officer (CISO).

At the Agency, senior leadership at Level 1 establishes organizational direction, sets the prioritization of mission functions, and provides direction on risk appetite and risk tolerance (detailed information can be found in Section 3.1.3). The SAORM, guided by the NRC Chief Risk Officer (CRO), determines: (i) the types of risk management decisions that are to be reserved solely for specific senior leadership roles; (ii) the types of risk management decisions that may be delegated to other roles within the organization; and (iii) how risk management decisions is communicated to and from the CRO.

Mission owners at Level 2 are expected to make decisions within the scope of the Agency's established risk appetite and tolerance level. This includes the responsibility of managing the risk of the systems operating under them at the Information System level. Mission owners are expected to provide risk analysts with the information needed to identify, analyze, and prioritize risks at the mission level.

At Level 3, system owners and staff are expected to maintain the daily operations and functions of Agency information systems and assets within the prescribed ranges of risk appetite and risk tolerance. They are expected to provide the information needed to identify, analyze, and prioritize risks at the system level.

Table 1: Risk Management Role Responsibilities

| Role | Responsibility |
|---|---|
| Head of Agency | The head of Agency is responsible and accountable for providing information security protections commensurate with the risk to organizational operations and assets, individuals, other organizations, and the Nation—that is, risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Agency; and the information systems used or operated by an Agency or by a contractor of an Agency or other organization on behalf of an Agency. The head of Agency is also the senior official in an organization with the responsibility for ensuring that privacy interests are protected and that PII is managed responsibly within the organization. |
| Enterprise Risk Management Council | The Enterprise Risk Management Council (ERMC) consists of the CRO, the CIO, the Senior Agency Official for Supply Chain Risk Management (SAOSCRM), Chief Acquisition Officer (CAO), Chief Financial Officer (CFO), Director of the Office of Nuclear Reactor Regulation (NRR), Director of the Office of Nuclear Material Safety and Safeguards (NMSS), and the Director of Office of Nuclear Security and Incident Response (NSIR), with an Office of General Counsel (OGC) representation. The ERMC champions organization-wide efforts to manage risk and advises on the strategically aligned portfolio view of risks. The ERMC operates at the Level 1 and serves as a strategic advisor on the integration of enterprise risk management practices into the |

| Role | Responsibility |
|---|---|
| | daily business operations and decision-making. The ERMC is advised of all enterprise level risks, including cyber risk, and is supportive of the CIO and CISO in management of these cyber risks. |
| Chief Risk Officer | The CRO provides a more comprehensive, organization-wide approach to risk management. The CRO serves as the common risk management resource for senior leaders/executives, mission/business owners, chief information officers, chief information security officers, information system owners, common control providers, enterprise architects, information security architects, information systems/security engineers, information system security managers/officers, and any other stakeholders who have a vested interest in the mission/business success of organizations. |
| Senior Agency Official for Supply Chain Risk Management | The SAOSCRM is a senior executive responsible for:<br>1. Ensuring the agency effectively carries out the supply chain risk management functions and responsibilities described in law, regulation, and policy.<br>2. Serving as the primary liaison with the Federal Acquisition Security Council (FASC).<br>3. Establishing participation in an information-sharing environment, as required by the FASC, to facilitate interagency sharing of relevant supply chain risk information.<br>4. Notifying and consulting with the Office Director of National Intelligence (ODNI) on the issuance of a specific supply chain waiver request and ensuring that a waiver is not granted if ODNI has existing information suggesting that the waiver would present a material increase in risk to U.S. national security.<br>5. Leading agency information and communications technology (ICT) supply chain risk management (SCRM) efforts and ensuring development, implementation, and maintenance of a supply chain risk management strategy for the agency. |
| Chief Information Officer | The chief information officer (CIO) is a senior executive responsible for designating a senior Agency information security officer; developing and maintaining security policies, procedures, and control techniques to address security requirements; overseeing personnel with significant responsibilities for security and ensuring that the personnel are adequately trained; assisting senior organizational officials concerning their security responsibilities; and reporting to the head of the Agency on the effectiveness of the organization’s security program, including progress of remedial actions. |
| Chief Information Security Officer | The Chief Information Security Officer (CISO) is a Department official designated by the CIO under statutory authority. The role is aligned to the Department level but interfaces with all three levels. The CISO is responsible for serving as the primary liaison for the Chief Information Officer to the organization’s Authorizing Officials, Information System Owners, Common Control Providers, and Information System Security Officers for cyber risk response activities. |
| Mission or Business Owner | The mission or business owner is the senior executive within the agency with specific mission or line of business responsibilities and that has a security or privacy interest in the organizational systems supporting those missions or lines of business. Mission or business owners are key stakeholders that have a significant role in establishing organizational mission and business processes and the protection needs and security and privacy requirements |

| Role | Responsibility |
|---|---|
| | that ensure the successful conduct of the organization's missions and business operations. Mission and business owners provide essential inputs to the risk management strategy, play an active part in the SDLC, and may also serve in the role of authorizing official. |
| Authorizing Official | The authorizing official (AO) is the senior executive with the authority to formally assume responsibility and accountability for operating a system. The AO is the only organizational official who can accept the security and privacy risk to organizational operations, organizational assets, and individuals. |
| System Owner | The system owner (SO) is the senior executive with overall responsibility for the security of NRC systems owned by his or her organization or operated on behalf of his or her organization by another agency or by a contractor. |
| Information System Security Officer | The information system security officer (ISSO) is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information system owner. The information system security officer also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. |
| Control Assessor | The control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of implemented controls and control enhancements to determine the effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization). For systems, implemented system-specific controls and system-implemented parts of hybrid controls are assessed. For common controls, implemented common controls and common control implemented parts of hybrid controls are assessed. The system owner and common control provider rely on the security and privacy expertise and judgment of the assessor to assess the implemented controls using the assessment procedures specified in the security and privacy assessment plans. |
| Senior Accountable Official for Risk Management | The senior accountable official for risk management (SAORM) is the individual that leads and manages the CRO in an organization and is responsible for aligning information security and privacy risk management processes with strategic, operational, and budgetary planning processes. The senior accountable official for risk management is the head of the Agency or an individual designated by the head of the Agency. The senior accountable official for risk management determines the organizational structure and responsibilities of the CRO, and in coordination with the head of the Agency, may retain the CRO or delegate the function to another organizational official or group. The senior accountable official for risk management is an inherent U.S. Government function and is assigned to government personnel only. |
| Senior Agency Official for Privacy | The senior Agency official for privacy (SAOP) is the senior executive with Agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk. Among other things, the senior Agency official for privacy is responsible for:<br>Coordinating with the senior Agency information security officer to ensure coordination of privacy and information security activities:<br>• Reviewing and approving the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information; |

| Role | Responsibility |
|---|---|
| | • Designating which privacy controls is treated as program management, common, system-specific, and hybrid privacy controls;<br>• Identifying assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;<br>• Reviewing and approving privacy plans for information systems prior to authorization, reauthorization, or ongoing authorization;<br>• Reviewing authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information to ensure compliance with privacy requirements and manage privacy risks;<br>• Conducting and documenting the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the Agency; and<br>• Establishing and maintaining a privacy continuous monitoring program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with privacy requirements and manage privacy risks. |

# 3 RISK MANAGEMENT PROCESS[2]

This section describes how the Agency executes the fundamental risk management process in accordance with NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View.”

## 3.1 Framing Risk

The Agency risk frame describes the environment in which risk-based decisions are made. It includes the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape the Agency’s approach for managing risk and making investment and operational decisions.

The Agency frames risk within the context of mission functions. Mission functions are prioritized by their criticality to Agency operations. The prioritization of both mission functions and sensitivity of information (e.g., controlled unclassified information) is essential for consistent application of the risk management strategy.

### 3.1.1 Risk Assumptions

Enterprise-level assumptions associated with this strategy include:

- Centralized risk management and effective governance processes allow the use of a single methodology across all mission areas.
- Key risk management personnel have appropriate training and understand and execute their roles.

[2] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011.

- The five elements of NIST's Cybersecurity Framework (CSF) – Identify, Protect, Detect, Respond and Recover – have been considered as part of the risk management process.
- The Agency has identified High Value Assets (HVAs) supporting Primary Mission Essential Functions and Mission Essential Functions and uses this information to guide the prioritization of risk resolution.
- Federal Information Processing Standard (FIPS) 199 High or Moderate systems typically have a lower risk tolerance than FIPS 199 Low systems with publicly available data. Systems with personally identifiable information (PII) or other sensitive data have a lower risk tolerance than systems without such data.
- The NIST Risk Management Framework (RMF) is used to manage information security and privacy risk.
- The Agency is developing an information and communications technology (ICT) supply chain risk management plan that is used at all organizational levels.
- Systems placed into production have undergone an authorization process based upon the RMF. Any findings from the assessment and authorization (A&A) process are assessed for risk. Risk acceptances have been documented.
- Vulnerabilities are identified through Continuous Diagnostics and Mitigation (CDM) and other security tools.
- Potential threats are identified and documented including impact (the degree of harm that may occur given the potential for threats exploiting vulnerabilities), and likelihood that harm will occur.
- Appropriate processes have been developed to detect and respond to a cybersecurity incident.
- The Agency utilizes lessons learned from incident response to improve response and recovery processes and reduce risk in the future.
- The Agency fosters a climate where information security risk is considered within the context of the design of mission/business processes, the definition of enterprise architecture, and SDLC processes.

#### 3.1.1.1 Threat Sources

The Agency is subject to a broad array of internal and external threats. These include purposeful attacks, environmental disruptions, human/machine errors, and structural failures.

With respect to adversarial threats, the Agency examines threat sources and events to identify capabilities and intentions that can adversely affect organizational levels 1, 2, or 3. The Agency uses the following cyber threat modeling framework(s) or taxonomies: gov Cybersecurity Architecture Review (govCAR); NSA/CSS Technical Cyber Threat Framework, v2; and/or MITRE's ATT&CK.

The Agency utilizes multiple threat intelligence platforms including: vendor subscriptions; NIST National Checklist Program (SCAP content); NIST National Vulnerability Database (NVD) offering Common Vulnerabilities and Exposures (CVE) and Common Configuration Enumeration (CCEs); Automated Indicator Sharing (AIS) feeds; US CERT and ICS CERT alerts; and Information Sharing and Analysis Center (ISAC) reports for information on adversaries that may be targeting the Agency. These reports include tactics and techniques that adversaries may be leveraging and are intended to give the Agency advanced warning to potential attacks and the attack vectors that may be used. This gives the Agency an opportunity to be more vigilant against the attacks, and the reports are shared with other relevant parties as appropriate.

The Agency participates in the following interagency groups that discuss current threats and response strategies: Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) cybersecurity information exchanges, Trusted Internet Connection initiative information exchanges, National Cybersecurity and Communications Integration Center (NCCIC), and Networking and Information Technology Research and Development (NITRD) Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG).

The Agency has an internal threat team, whose purpose is to describe the threat landscape for the Agency and assist with co-relating evolving threats with existing vulnerabilities:

- At Level 1, these threat sources are considered in relation to their impact on regulatory efforts.
- At Level 2, special consideration is given to their impact on designated Primary and Mission Essential Functions such as event assessment, licensing inspection, enforcement, and allegations.
- At Level 3, understanding threat source tactics, techniques and procedures is essential to selecting and applying appropriate countermeasures to HVAs and other information systems.

#### 3.1.1.2 Characterization of Vulnerabilities and Sources

At Level 3, the Agency employs continuous monitoring capabilities to identify and assess the importance of system vulnerabilities in hardware, software or firmware components of information systems (or the security controls employed within those systems). The tools feed into the agency-wide cybersecurity risk dashboard to facilitate identification and handling of cybersecurity risks. The dashboard provides information on vulnerabilities at a level of detail that is meaningful and promotes consistency throughout the organization.

The Agency also conducts control assessment as part of system authorization; FISMA self-assessments and metrics analysis; and external assessments including penetration tests and audits.

At Level 2, vulnerabilities relate to the design of system-of-systems supporting mission/business processes, enterprise architectures, and enterprise IT infrastructures. Interconnected systems create process efficiencies but may increase cybersecurity risk. Vulnerabilities associated with architectural design and mission/business processes (inconsistent decisions about the relative priorities of mission/business processes, selection of incompatible implementations of security controls, outdated systems) can have great impact on the ability of the Agency to successfully carry out mission and business functions due to the potential impact across multiple information systems and mission environments.

Level 1 vulnerabilities affect the entire Agency and may be associated with facilities, intra-Agency communications, organizational governance structures and procedures (gaps in policies or training, personnel, system development lifecycle processes); or vulnerabilities associated with depending on external organizations for energy sources, supply chains, IT and telecommunications. Level 1 vulnerabilities would also include any concerns in HVAs that would impact mission achievement, including a key service to the public, economy, or Nation.

The Agency participates in CISA's Cybersecurity Coordination Assessment and Response (C-CAR) process and complies with CISA's Binding Operational Directives (BOD) and Emergency Directives (ED). The C-CAR, BOD, and ED processes mandate Agency response to vulnerabilities within a specified timeframe.

When the Agency participates in a DHS-led Risk and Vulnerability Assessment (RVA) or Security Architecture Review (SAR), the Agency remediates all major or critical weaknesses within 30 days of receipt of the assessment report.

Additionally, incidents may be reported by external or internal entities. Incident response may identify vulnerabilities that need to be assessed for risk.

#### 3.1.1.3 Consequences and Impact

The Agency applies FIPS 199 security categorizations to information types (e.g., privacy, medical, investigative) and information systems. The Agency then assesses impact using [NIST SP 800-60 provisional impact levels and adjusts based on the organization, environment, mission, use, and data sharing. The qualitative impact values (low, moderate, high) and semi-quantitative values are a preparatory step in selecting an appropriately tailored set of baseline security controls[3] to protect confidentiality, integrity and availability. The Agency uses the FIPS 199 security categorizations in conjunction with vulnerability and threat information to assess risk to organizational operations and assets, individuals, other organizations, and the Nation.

The Agency characterizes consequences in terms of their impacts on: Primary and Mission Essential Functions, other mission or business functions, High-Value Assets, privacy, sensitive information, and financial assets.

#### 3.1.1.4 Likelihood

For adversarial events, the Agency assesses the likelihood of occurrence based on (i) adversary intent; (ii) adversary capability; and (iii) adversary targeting. For other than adversarial threat events, the Agency estimates the likelihood of occurrence using historical evidence, empirical data, and expert judgement. A risk register is used for managing risk and communicating risk information.

### 3.1.2 Risk Constraints

Enterprise-wide constraints associated with the strategy include:

- Risk remediation is reliant on available resources and the effectiveness of those resources in mitigating risk.[4]
- Implementation timelines may be impacted by available funding; the complexity of the mitigation; contractual relationships; use of legacy hardware and software;

[3] See NIST SP 800-53, Rev. 5 (draft).

[4] NISTIR 8286 discusses the use of a risk reserve to avoid or mitigate an identified risk. Risk owners should discuss with acquisition or procurement teams and budget owners setting aside funding or labor hours as part of a risk reserve during project planning.

organizational governance structure; geographical location of offices; legal and regulatory requirements, workforce; organizational culture; and trust relationships.

- Maintaining an accurate inventory of physical and virtual hardware, software, and connections has become difficult with the increased number of mobile devices, the Internet of Things (IOT), and adoption of cloud-based applications and devices.
- The evolving complexity of digital assets makes risk assessment difficult.

### 3.1.3 Risk Tolerance

The Agency organizes the thresholds for acceptable risk into two constructs: risk appetite and risk tolerance. Risk appetite is the broad-based amount of qualitative risk the Agency plans to accept in pursuit of its mission and vision. It is established by the ERMC and serves as the guidepost to set strategy and select objectives.

The Agency's risk appetite is moderate about cybersecurity, information security, and privacy risk.

Risk tolerance is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level. In setting the risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite. The Agency has set cyber risk tolerance levels for each program, objective or component; and each type of loss/compromise. In setting risk tolerance levels, the Agency considered the tradeoffs between the potential cyber risk impacts and the importance of the mission and its objectives.

Risk tolerance directly impacts the risk management decisions made by senior leaders and affects the nature and extent of risk management oversight; the extent and rigor of risk assessments; and the strategies for risk response.

The Agency's cyber risk tolerance is based in part on:

- Security categorizations according to FIPS 199 levels;
- Type of data (Safeguards Information [SGI], PII, other sensitive data, publicly available data); and
- Operating environment (accessibility from the Internet, etc.).

At Level 1, cyber risk tolerance applies to organization-wide systems and business processes. The risk tolerance for cybersecurity risks at Level 1 is Moderate. All risk tolerance thresholds at Level 1 are periodically reviewed to determine whether the acceptable risk threshold benefits Agency operations and cybersecurity.

Risks due to deficiencies in cybersecurity controls implemented at Level 2 reflect the risk to the missions and business processes supported by the controls. The risk tolerance for cybersecurity risks at Level 2 is Moderate.

Risks due to deficiencies in cybersecurity controls implemented at Level 3 reflect the risk to the information system. The risk tolerance for cybersecurity risks at Level 3 is Moderate.

The Agency may change its risk tolerance based on other changes (e.g., changes in organizational or mission importance; other internal or external factors). In this case, the CISO is notified so that a review of risk assessments may occur, and risk responses updated, if necessary.

While not planned or desired, there are times when the Agency must accept risk beyond what is normally tolerable. Operating with unacceptable risk requires justification of exigent conditions. Should there be a need for acceptance of risk outside of normal tolerances, the Agency documents the acceptance by higher levels of the organization and notes the reasons and expected duration of the exception. Unacceptable risk is treated as such by establishing a list and timetable of mitigations known as a Plan of Action and Milestones (POA&M) to bring the system into a tolerable range at the earliest opportunity. Systems operating with unacceptable risk are subject to increased monitoring to rapidly detect anomalous activity and respond quickly.

### 3.1.4 Priorities and Trade-Offs

Prioritization of risk response enables a business-driven approach that maximizes the value of Agency investments. The prioritization of mission functions is established at Level 1 by the ERMC and communicated to Levels 2 and 3.

The Agency ranks threat events by the level of risk determined during the risk assessment – with the greatest attention going to high risk events impacting:

- Primary Mission Essential Functions (PMEFs): Those mission essential functions that must be performed in order to support the National Essential Functions before, during, and in the after math of an emergency.
- Mission Essential Functions (MEFs): The limited set of Agency-level government functions that must be continued throughout or resumed rapidly after a disruption of normal activities, and
- High Value Assets[5] supporting PMEFs and MEFs

The Agency has a legal responsibility to protect sensitive information residing on information systems. This includes but is not limited to PII and financial data.

The Agency must sometimes make risk trade-offs. At Level 1, it may be better to aggregate multiple risks in one broad-based response rather than individually addressing each risk. Choosing not to remediate risks on a legacy system scheduled for replacement by instead accelerating completion of the replacement is another example of a trade-off. Risk trade-off decisions are made by the SAORM in consultation with the Chief Risk Officer.

## 3.2 Assessing Risk

The Agency identifies, analyzes, and prioritizes risks to provide a foundation for risk response and risk monitoring. The Agency captures and tracks this information through a System Cybersecurity Assessment Report and using an Agency-wide Cybersecurity Risk Register. The SAORM authorizes those responsible at each Level to designate risk analysts to perform risk

[5] See Appendix D, Glossary, for the definition of an HVA.

assessments at that level and designates risk assessors to perform risk assessments for the Agency.

### 3.2.1 Risk Assessments Within the Agency

The Agency relies upon a comprehensive inventory to determine which assets within the Agency's direct control need to be assessed for cybersecurity risks. The Agency's system inventory and system component inventory provides a method for tracking the owner/manager of each asset and the asset's relative importance (or value) to mission/business processes and organizational-level risks[6].

The Agency uses risk assessments to support decision making regarding:

- Development of an information security architecture
- Definition of interconnection requirements
- Design, implementation, operation and maintenance of security solutions
- Selection of ICT SCRM controls
- Authorization, interim authorization, or denial of authorization to operate information systems,
- Modification of missions/business functions and or processes, and
- Funding of information security programs

The Agency conducts cyber hygiene/compliance assessments to support implementation of the RMF. The RMF operates primarily at level 3 with some application at levels 1 and 2 that help prepare the organization to manage risk, such as selection of common controls.

The Agency assesses risks on an ongoing basis; before re-authorization decisions; and in response to triggers discovered by risk monitoring. By conducting risk assessments during the development and implementation phases of the SDLC, the Agency can identify deficiencies early and initiate corrective action in a more cost-effective manner.

In addition to the RMF, the Agency uses a risk management methodology with an asset/impact-oriented analysis approach that provides semi-qualitative results.

The SAORM specifies the degree of autonomy subordinate organizations have in assessing, responding to, and monitoring risk. The Agency is a centralized organization with similar missions/business functions and environments of operation. The SAORM has therefore determined minimal flexibility subcomponents have in conducting specific portions of the risk management process.

Within the constraints established by the SAORM, risk assessment methodologies/tools/techniques/taxonomies (M/T/T/T) used by the Agency to evaluate risks at level 1, 2, and 3 are:

- Cyber Hygiene/Compliance Assessments (to support implementation of the RMF)

[6] A system component inventory contains information needed for accountability and monitoring of all system components, such as manufacturer, software licenses, and component owner.

- NIST 800-30
- Software dependency analysis;
- Conventional resilience analysis (e.g., mission resilience or system resilience);
- Assessment of cyber resiliency against advanced cyber adversaries (e.g., the .gov Cybersecurity Architecture Review (govCAR); NSA/CSS Technical Cyber Threat Framework, v2 [7]); MITRE ATT&CK™ for Enterprise IT[8]; and MITRE ATT&CK™ for ICS[9] )

The Agency allows the use of any M/T/T/T subject to the following considerations:

- Suitability – Whether the M/T/T/T provides the type of information the Agency seeks to develop (e.g., how to quantify risk in financial terms for risk scenarios at any organizational level)
- Maturity of the M/T/T/T - How many years has it been in use and by whom?
- Accreditation – whether or not the M/T/T/T has been accredited, authorized, approved or formally adopted by NIST, DoD, or a standards community (e.g., International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE), Open Group)
- Compatibility - How well does it work with other M/T/T/Ts? For a tool, can it exchange data with other tools (e.g., via Automated Indicator Sharing using STIX and TAXII)?
- Performance – How well does the M/T/T/T perform in practice? Does it produce its intended assessment results quickly, accurately, and with low programmatic impact?
- Scalability – Does the M/T/T/T access a single system or a system of systems?
- Evolvability - Can the M/T/T/T deal with diverse environments and needs?
- Usability - What resources (e.g., staffing, expertise, documentation, technology) are required to apply the M/T/T/T for a cyber assessment?
- Cost containment - What is the purchase cost, on-going licensing fees, maintenance fees? What are the associated labor costs - what level of effort is necessary to use the M/T/T/T, and what specialized expertise is needed?
- Evaluator Confidence - How much confidence do the evaluators have that the M/T/T/T behaves as it claims?

The Agency strives to increase the reproducibility and repeatability of risk assessments by standardizing the processes and procedures used to conduct them. This assists executives at Levels 1 and 2 with aggregating multiple risks that materialize concurrently or materialize repeatedly over a period of time.

[7] U.S. National Security Agency, Cybersecurity Report, NSA/CSS Technical Cyber Threat Framework v2, November 2018, https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf.

[8] MITRE ATT&CK® for Enterprise, https://attack.mitre.org/matrices/enterprise/.

[9] MITRE ATT&CK® for Industrial Control Systems, https://collaborate.mitre.org/attackics/index.php/Main_Page.

The Agency uses the Cybersecurity Framework's (CSF) five functions (Identify, Protect, Detect, Respond and Recover) to organize and clearly communicate cybersecurity risks. The Agency has created a current Framework profile indicating the cybersecurity outcomes that have been achieved, and a target profile indicating outcomes that will be met in the future. The gap between the current and target CSF profiles represents risks that must be managed. The Agency also uses the CSF to identify how IT investments relate to the five functions. This process of tagging risks to investments to CSF categories assists with tracking performance metrics and quarterly FISMA reporting.

### 3.2.2 Assessing Risk of External Providers

Many of the assets on which the Agency depends are not within its direct control. External providers can be public or private sector entities, domestic or international. External technical assets include cloud-based services (infrastructure, platform, software); data center operations, and telecommunication circuits. The Agency and its external providers share responsibility for supporting organizational missions and business functions.

FISMA and OMB policies require that federal agencies using external service providers assure that the providers meet the same security requirements that federal agencies are required to meet. The Agency utilizes the Federal Risk and Authorization Management Program (FedRAMP) for most of its commercial and non-commercial cloud services.

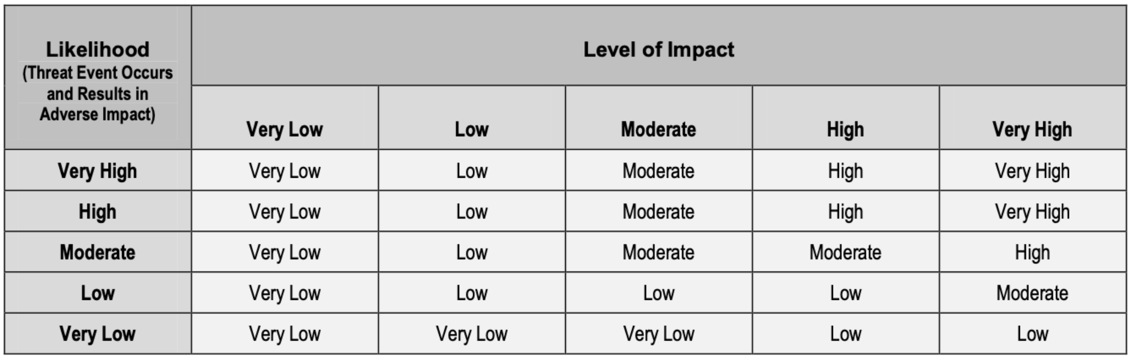
The Agency plans to use FedRAMP for all of its future commercial and non-commercial cloud services.

The Agency has incorporated the RMF into the terms and conditions of its contracts and service level agreements with FedRAMP authorized cloud service providers. The Agency requires its external providers to provide appropriate evidence to demonstrate that they have complied with the RMF in protecting federal information. This includes independent assessments conducted by third parties and continuous monitoring. The Agency maintains the responsibility for granting external service providers an authority to operate.

### 3.2.3 Risk Determination

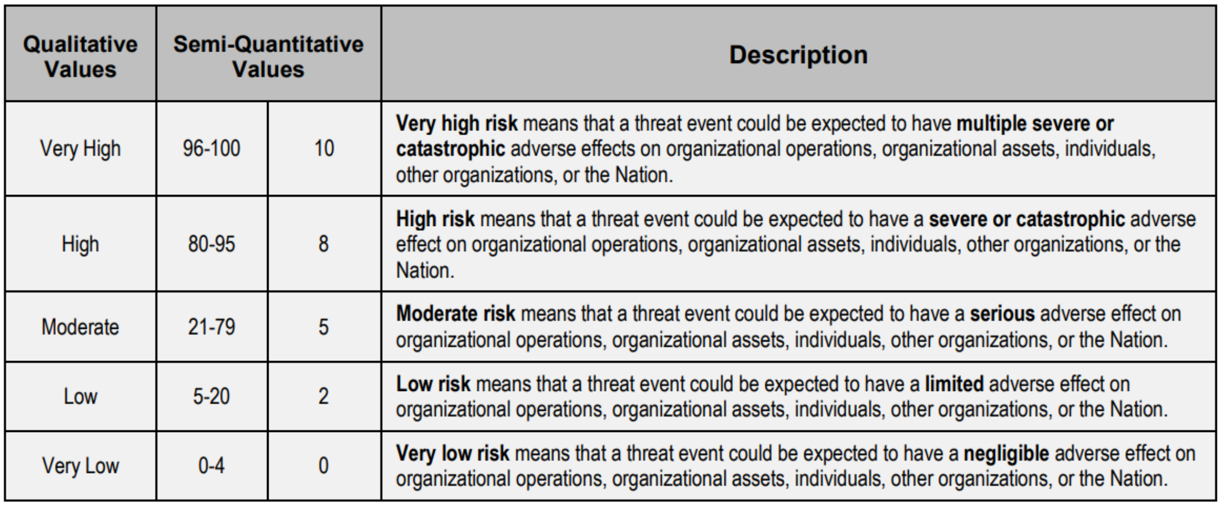
The result of a risk assessment is a determination of the risk (typically a function of the degree of harm and the likelihood of harm occurring) associated with a threat scenario, for each threat scenario identified by risk analysts subject to risk framing. The Agency uses tables from NIST 800-30 below; algorithms for combining values of factors as provided by (specific methodologies or tools); or risk score.

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)



| Likelihood (Threat Event Occurs and Results in Adverse Impact) | Level of Impact | | | | |
|---|---|---|---|---|---|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK



| Qualitative Values | Semi-Quantitative Values | | Description |
|---|---|---|---|
| Very High | 96-100 | 10 | **Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | 80-95 | 8 | **High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Moderate | 21-79 | 5 | **Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Low | 5-20 | 2 | **Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Very Low | 0-4 | 0 | **Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |

The reliability and degree of uncertainty associated with the risk determination is contingent on the accuracy of the inputs used during the assessment. Uncertainties during the risk assessment arise from sources such as missing information, subjective determinations, and assumptions made. Uncertainty is a concern when considering advanced persistent threats where analysis of interacting vulnerabilities is needed, the common body of knowledge is sparse, and past behavior may not be predictive. The Agency compiles information related to uncertainty and presents it in a manner that readily supports informed risk management decisions.

## 3.3 Responding to Risk

The Agency considers the following types of possible responses to risk when identifying, evaluating, and deciding on courses of action: risk acceptance, risk avoidance, and risk mitigation. The Agency identifies and tracks its risk responses using its Cybersecurity Risk Register and Agency-wide POA&M document.

### 3.3.1 Risk Response Identification

At each Level, alternative courses of action are identified sequentially starting with the highest risks. Alternative courses of action may include operational measures, technical changes using existing capabilities, new technical solutions, architectural changes, and changes in organizational processes or programs.

### 3.3.2 Evaluation of Alternatives

The Agency's evaluation of alternative courses of action includes (i) the expected effectiveness in achieving the desired risk response (and how effectiveness is measured and monitored); and (ii) the anticipated feasibility of implementation, including, for example, mission/business impact, political, legal, social, financial, technical, and economic considerations.

### 3.3.3 Risk Response Decision

Risk-informed decisions (e.g., risk response) enhance mission accomplishment by reducing the loss or degradation of confidentiality, integrity, or availability. The SAORM oversees all cyber risk management decisions even in cases where senior management officials are delegated authority to make risk decisions affecting mission specific systems.

#### 3.3.3.1 Risk Acceptance

The authorizing official (AO) may accept the risk and grant an authorization to operate (ATO) for systems and common controls that have exploitable deficiencies.

In keeping with the Agency's risk tolerance levels, risk acceptance is a viable response for Level 1 risks that are assessed as very low, low, or moderate.

The Agency considers risk acceptance as a viable response for Level 2 risks that are assessed as very low, low, or moderate.

The Agency considers risk acceptance as a viable response for Level 3 risks that are assessed as very low, low, or moderate.

#### 3.3.3.2 Risk Avoidance

The Agency uses risk avoidance for all technologies and external services or external service providers that have very high or high risks that cannot be mitigated in a cost-effective manner. If risk avoidance is used for any particular risk, specific actions are taken to eliminate activities or technologies that are the basis for the risk.

#### 3.3.3.3 Risk Mitigation

The Agency utilizes a consistent approach to prioritizing plans of action and milestones (POA&Ms) to mitigate risk across the organization. A POA&M, required by NIST SP 800-18, is a key part of the system authorization process and recommends remedial actions, for security controls determined to be less than effective, be completed either before or after ATO. The Agency also creates POA&Ms to reduce risk identified during continuous monitoring[10].

[10] Note POA&Ms do not inherently reduce risk, they document the deficiencies and timeline/milestones to remediate the deficiencies.

Risk mitigation is the appropriate risk response for all very high, and high risks at Levels 1, 2, and 3 that exceed the defined tolerance level, and cannot be accepted, avoided, or shared.

When risk mitigation is required, the Agency applies the following types of controls to achieve the acceptable level of risk[11]:

- Preventative: Reduce or eliminate specific instances of a vulnerability
- Deterrent: Reduce the likelihood of a threat event by dissuading a threat actor
- Detective: Provide warning of a successful or attempted threat event
- Corrective: Reduce exposure by offsetting the impact of consequences after a risk event
- Compensating: Apply one or more SP 800-53 controls to adjust for a weakness in another control

As part of risk response, residual risk is identified. If the residual risk cannot be accepted, it is managed in the same way as any other risk. All risk mitigations follow change control requirements and project management principles as appropriate.

The Agency supplements risk response at level 3 with risk mitigation strategies at Levels 1 and 2 process-level response measures, changes to the information security architecture, and modification of common controls.

Information security investments to address advanced persistent threats may require expenditures over the course of several years, as new security solutions and technologies transition from research to development to full deployment.

#### 3.3.3.4 Risk Sharing or Transfer

The Agency uses risk sharing[12] when the Agency is responsible for one piece of the hardware or software stack and another Agency is responsible for another piece of the hardware or software stack under a shared service agreement. All Agency resources that fit these criteria must have their associated risks fully documented in a formal Interconnection Security Agreement (ISA)/Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU).

### 3.3.4 Sharing Risk-Related Information

The Agency uses the following communication mechanisms to share risk-related information with key personnel within the organization: ERMC notification, notification of staff that manage the risk, and notification of any group or organization impacted by the risk. The SAORM coordinates with the Agency CIO to determine how risk to the cybersecurity program is added to the Agency Cybersecurity Risk Register. The Agency uses a Cybersecurity Risk Register to aggregate and manage the organization's highest cybersecurity risks in a consistent, repeatable manner. Inputs to the Cybersecurity Risk Register include an Agency wide POA&M, and NIST SP 800-30 Appendix J Risk Assessment Reports (RAR). See Appendix E for additional information.

The SAORM, in consultation with the CIO determines what risk information can be shared externally. The CDM and FISMA reporting processes require certain risk related information be

[11] DRAFT NISTIR 8286, Section 3.5.1: Applying Security Controls to Reduce Risk Exposure.

[12] The USG does not transfer risk. Risk transfer typically involves insurance which the USG does not use.

shared with CISA and OMB. Any risks arising from the CDM and FISMA reporting processes are communicated with the Agency EDO and Chairman by the CIO.

## 3.4 Monitoring Risk

Ongoing monitoring is a critical part of the risk management process.[13] The Agency uses risk monitoring to:

- Verify compliance with information security requirements;
- Determine the ongoing effectiveness of risk response measures; and
- Identify changes to information systems and environments of operation that may impact the risk posture.

### 3.4.1 Monitoring Compliance

Compliance monitoring ensures that cybersecurity controls at Levels 1, 2 and 3 have been implemented correctly and are operating as intended. Compliance monitoring also verifies that the information security requirements are derived from and traceable to Agency missions/business functions, federal legislation, directives, regulations, policies and standards, and guidelines.

The Agency conducts compliance/cyber hygiene assessments to support implementation of the RMF for systems in operation. The Agency's compliance monitoring solution relies on automation as much as possible and uses the agency-wide cybersecurity risk dashboard to present information from various cybersecurity monitoring tools. These control assessments are like those conducted during the initial security assessment and authorization; however, they are conducted after the completion of the authorization following the schedule defined in the Agency Information Security Continuous Monitoring (ISCM) Strategy documented separately. Compliance monitoring results aid in the creation of POA&Ms listing cybersecurity weaknesses and follow-on actions necessary to maintain acceptable levels of risk.

### 3.4.2 Monitoring Effectiveness

The Agency uses effectiveness monitoring to determine if risk response measures at Levels 1, 2 and 3 have, in fact, been effective in reducing identified risk to the desired level. Effectiveness monitoring takes into consideration the complexity of the operating environment; changes in risk factors such as threats and vulnerabilities; and changes in the system or operating environment. Agency effectiveness monitoring uses the agency-wide cybersecurity risk dashboard as a monitoring tool.

Effectiveness monitoring requires establishment of effectiveness criteria. It may be difficult to obtain criteria that are quantifiable. Based on qualitative analysis of the effectiveness of the protections and countermeasures (e.g., security controls, security services, and technologies), the Agency may modify them in order to reduce risks. Monitoring of the operational environment can reveal changes in the threat landscape that impact threat assumptions.

[13] NIST SP 800-137 defines information security continuous monitoring (ISCM) as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

### 3.4.3 Monitoring Changes

Change monitoring is a component of the change management process, which manages updates to production systems. Changes to systems are overseen through Agency change and configuration management processes. However, those changes which affect prior risk decisions (changes in the value of information, threat environment, or technology, such as an end-of-life product) can affect the security state of the system and are carefully monitored by the Agency.

The change management process considers the following types of changes to a system to be major changes that require full analysis of the change impact:

- Change in the sensitivity of information processed by the system
- Change in the criticality of the system assets with respect to the agency mission

# APPENDIX A REFERENCES

To make the CSRM Strategy more useful to its intended audience, the Agency should include a list of references. The references in Appendix B, below, provide a starting point. However, the Agency should also include references to:

- Any laws, regulations, directives, and state, local, and Tribal policies which direct or constrain how the Agency addresses concerns for cybersecurity, privacy in cyberspace, and continuity of cyberspace operations.
- Agency policies regarding data protection, privacy, information security, and continuity of operations.
- Any key publications of the information security program.

Table 2: Resources Used for Template Creation

| Document Type | Title | Description |
|---|---|---|
| Executive Order | EO 13800 "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*" | EO requiring all agencies to use NIST's Framework for Improving Critical Infrastructure Cybersecurity (The Framework) and mandating reporting by agencies to DHS and OMB on cybersecurity risk assessments. |
| Policies, Directives, and Instructions | OMB Circular A-130 (revised) "*Managing Information as a Strategic Resource*" | Circular creating generalized policy for planning and handling the infrastructure and services necessary for information management. Requires agencies to implement policy on creating information inventories, managing information, and assessing and planning for risk. |
| Policies, Directives, and Instructions | OMB Memo 17-25 "*Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*" | Memo providing a series of concrete steps pursuant to EO 13800 with mandatory completion dates for all federal agencies. |
| Policies, Directives, and Instructions | OMB Memo 16-24 "*Role and Designation of Senior Agency Officials for Privacy*" | Memo describing the Senior Agency Officials for Privacy (SAOP), including scope of role and responsibility. Mandates the creation of an Agency-wide privacy program under the direction of an SAOP. |
| Federal Standards and Guidance | FIPS 199 "*Standards for Security Categorization of Federal Information and Information Systems*" | Document outlining standard practices for categorization of information and information systems based on the level of threat and the importance of the asset. |
| Federal Standards and Guidance | NIST "*Framework for Improving Critical Infrastructure Cybersecurity*" | Framework giving a generalized and adaptable plan for incorporating cybersecurity threats into organizational risk management, with standardized activities, outcomes, and assessment criteria. |

| Document Type | Title | Description |
|---|---|---|
| Federal Standards and Guidance | NIST Special Publication 800-30 "*Guide for Conducting Risk Assessments*" | Publication on the importance of risk management for information technology, the role of risk assessments within risk management, and the proper conduct of risk assessments. |
| Federal Standards and Guidance | NIST Special Publication 800-37 Rev. 2. "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*" | Publication providing a Risk Management Framework (RMF) for securing information systems throughout their lifecycle, from acquisition and control selection through ongoing monitoring and assessment. |
| Federal Standards and Guidance | NIST Special Publication 800-39 "*Managing Information Security Risk: Organization, Mission, and Information System View*" | Publication describing and providing guidelines for a flexible risk management framework applied across three levels: organization, mission/business process, and information systems. See also NIST SP 800-037. |
| Federal Standards and Guidance | NIST Special Publication 800-137 "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*" | Document providing a more in-depth explanation of the continuous monitoring mentioned in the RMF, both in concept and in execution. |
| Federal Guidance and Standards | NIST Special Publication 800-137a "*Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*" | Publication describing an approach for the development of ISCM program assessments. |
| Federal Standards and Guidance | NIST Special Publication 800-53 "*Security and Privacy Controls for Federal Information Systems and Organizations*" | Publication providing a catalogue of available security and privacy controls, methods to select and implement those controls, and guidance on tailoring sets of controls to specific situations at both the tactical and strategic levels of risk. |
| Federal Standards and Guidance | NIST Special Publication 800-53a Rev. 4 "*Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*" | Publication providing a set of procedures for assessing controls throughout the system development lifecycle. |
| Federal Standards and Guidance | NIST Special Publication 800-60 Vol. 1 Rev. 1 "*Guide for Mapping Types of Information and Information Systems to Security Categories*" | Publication describing how various types of information map onto different security categories, in line with FISMA requirements. |
| Federal Standards and Guidance | NISTIR 8286 (Draft) "*Integrating Cybersecurity and Enterprise Risk Management (ERM)*" | Document explaining how to effectively contextualize cybersecurity risks within broader ERM through risk identification, prioritization, and monitoring. |

| Document Type | Title | Description |
|---|---|---|
| Policies, Directives, and Instructions | OMB Memo 16-17 "*OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*" | Circular outlining management responsibilities for Agency ERM.  Provides guidance on establishment of internal controls. |
| Legislation | Public Law 113-283 "*Federal Information Security Modernization Act of 2014*" | 2014 overhaul of FISMA, originally passed in 2002. Requires federal agencies to use continuous monitoring for potential threats and update or create consistent risk management plans. |

# APPENDIX B ACRONYMS

| | |
|---|---|
| AC | Access Control |
| AIS | Automated Indicator Sharing |
| AO | Authorizing Official |
| AU | Audit and Accountability |
| BOD | CISA’s Binding Operational Directives |
| C-CAR | CISA’s Cybersecurity Coordination Assessment and Response |
| CAO | Chief Acquisition Officer |
| CCE | Common Configuration Enumeration |
| CDM | Continuous Diagnostics and Mitigation |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CPO | Chief Privacy Officer |
| CRO | Chief Risk Officer |
| CSF | Cybersecurity Framework |
| CSRM | Cybersecurity Risk Management |
| CSS | Central Security Service |
| CVE | Common Vulnerabilities and Exposures |
| DHS | Department of Homeland Security |
| ERM | Enterprise Risk Management |
| ERMC | Enterprise/Risk Management Council |
| FASC | Federal Acquisition Security Council |
| FCEE | Federal Civilian Enterprise Essential |
| FedRAMP | Federal Risk and Authorization Management Program |
| FEMA | Federal Emergency Management Agency |
| FIPPs | Fair Information Practice Principles |

| | |
|---|---|
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Modernization Act |
| FOIA | Freedom of Information Act |
| HIPAA | Health Insurance Portability and Accountability Act |
| HVA | High Value Asset |
| IA | Information Assurance |
| ICT | Information and Communications Technology |
| IEEE | Institute of Electrical and Electronics Engineers |
| IOT | Internet of Things |
| ISA | Interconnection Security Agreement |
| ISAC | Information Sharing and Analysis Center |
| ISCM | Information Security Continuous Monitoring |
| ISO | International Organization for Standardization |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| JACKE | Joint Agency Cyber Knowledge Exchange |
| KRI | Key Risk Indicator |
| MEF | Mission Essential Functions |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| M/T/T/T | Risk Assessment Methodologies/Tools/Techniques/Taxonomies |
| NIST | National Institute of Standards and Technology |
| NMSS | Office of Nuclear Material Safety and Safeguards |
| NRR | Office of Nuclear Reactor Regulation |
| NSIR | Office of Nuclear Security and Incident Response |
| NSA | National Security Agency |

| | |
|---|---|
| NVD | NIST National Vulnerability Database |
| ODNI | Office Director of National Intelligence |
| OGC | Office of General Counsel |
| OMB | Office of Management and Budget |
| PCM | Privacy Continuous Monitoring |
| PDD | Presidential Policy Directive |
| PHI | Protected Health Information |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PMEF | Primary Mission Essential Functions |
| POA&M | Plan of Action and Milestones |
| PTA | Privacy Threshold Assessment |
| RAR | Risk Assessment Reports |
| RMF | Risk Management Framework |
| RVA | Risk and Vulnerability Assessment |
| SAOP | Senior Agency Official for Privacy |
| SAORM | Senior Accountable Official for Risk Management |
| SAR | Security Architecture Review |
| SCAP | Security Content Automation Protocol |
| SCRM | Supply Chain Risk Management |
| SDLC | System Development Life Cycle |
| SGI | Safeguards Information |
| SO | System Owner |
| SORN | System of Records Notice |
| SP | Special Publication |
| SPP | System Privacy Plan |

# APPENDIX C GLOSSARY

Availability

Ensuring timely and reliable access to and use of information. NIST SP 800-37, Rev. 2.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. NIST SP 800-37, Rev. 2.

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. NIST 800-37, Rev. 2.

Cybersecurity Attack

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. NIST 800-30, Rev. 1.

Cybersecurity Risk

An effect of uncertainty on or within a digital context. Cybersecurity risks arise from the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. NISTIR 8286.

Enterprise

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. NISTIR 8170.

Environment of Operation

The physical surroundings in which an information system processes, stores, and transmits information. NIST SP 800-37, Rev. 2.

Governance

The set of responsibilities and practices exercised by the Department's senior leadership with the express goal[s] of: (i) providing strategic direction; (ii) ensuring that organizational mission and business objectives are achieved; (iii) ascertaining that risks are managed appropriately; and (iv) verifying that the organization's resources are used responsibly. NIST 800-39.

High Value Asset (HVA)

An Agency may designate Federal information or a Federal information system as an HVA when it relates to one or more of the following categories:

(i) Informational Value – The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.

(ii) Mission Essential – The Agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.

(iii) Federal Civilian Enterprise Essential (FCEE) – The information or information system serves a critical function in maintaining the security and resilience of the Federal civilian enterprise.

While agencies are principally responsible for designating their HVAs, OMB and DHS may also designate HVAs at agencies based on potential impact to national security. OMB M-19-03.

Impact

With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII. NIST SP 800-37, Rev. 2.

Information Security

The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. NIST SP 800-37, Rev 2.

Information Security Continuous Monitoring (ISCM)

Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. NIST SP 800-137.

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. NIST SP 800-37, Rev. 2.

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. NIST SP 800-37, Rev. 2.

Likelihood of Occurrence

A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. NIST SP 800-30.

Mission Essential Function

The limited set of Agency-level government functions that must be continued throughout or resumed rapidly after a disruption of normal activities. FEMA.gov.

Organization

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). NISTIR 8170.

Plan of Action and Milestones (POA&M)

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. NIST SP 800-37, Rev 2.

Primary Mission Essential Function (PMEF)

Primary Mission Essential Functions (PMEFs) are those functions that need to be continuous or resumed within 12 hours after an event and maintained for up to 30 days or until normal operations can be resumed. PMEFs are validated by the Federal Emergency Management Agency (FEMA) National Community Coordinator. FEMA.gov.

Residual Risk

Residual risk is the remaining risk once a mitigation has been put into place. NISTIR 8286.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. NIST SP 800-37, Rev. 2.

Risk Appetite

The broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives. OMB A-123, Adapted.

Chief Risk Officer

An individual or group within an organization, led by the senior accountable official for risk management, that helps to ensure that: security risk considerations for individual 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 managing risk from individual systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success. NIST SP 800-37, Rev. 2.

Risk Register

A repository of risk information including the data understood about risks over time. NISTIR 8286.

Risk Tolerance

Risk tolerance is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite. OMB Circular A-123, Adapted.

SAORM (Senior Accountable Official for Risk Management)

The senior official, designated by the head of each Agency, who has vision into all areas of the organization and is responsible for alignment of information security management processes with strategic, operational, and budgetary planning processes.  NIST SP 800-37, Rev. 2.

Security Control

The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. NIST SP 800-37, Rev. 2.

System Development Life Cycle

The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. NIST SP 800-37, Rev. 2.

Threat

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.  NIST SP 800-37, Rev. 2.

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. NIST SP 800-37, Rev 2.

# APPENDIX D CYBERSECURITY RISK REGISTER

The agency is using the risk register format adapted from NIST 8286 shown in Table 3. The Agency updates the Risk Register, at a minimum, on a bi-annual basis. Elements may be added to or removed from the Register during interim periods.

Table 3: Cybersecurity Risk Register

| ID | Priority | Risk Description | Risk Category | Inherent Assessment | | | Risk Response Type | Risk Response Cost | Risk Response Description | Risk Owner | Status | Status Date |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Impact | Likelihood | Exposure Rating | | | | | | |
| YY-1 | | | | | | | | | | | | dd-Mmm-yy |
| YY-2 | | | | | | | | | | | | |
| YY-3 | | | | | | | | | | | | |
| YY-4 | | | | | | | | | | | | |
| YY-5 | | | | | | | | | | | | |

The Agency aggregates, normalizes, and prioritizes risks in the cybersecurity risk register against risks identified in other risk registers, such as program management risk, budgetary risk, and legal liability risk. The resulting document is called a risk profile. The Agency uses the risk profile to choose which enterprise risks to address and then to delegate responsibilities to appropriate risk owners.

The columns in Table 3 are defined as follows:

- **ID (Risk Identifier)**: A sequential numeric identifier for referring to a risk in the risk register (e.g., 1, 2, 3) that begins with the fiscal year.
- **Priority**: A relative indicator of the criticality of this entry in the risk register, expressed in ordinal value from 1 to 5, where 1 indicaes the highest priority.
- **Risk Description**: A brief explanation of the cybersecurity risk scenario (natural, accidental, adversarial) impacting the organization and enterprise. Risk descriptions should be written in a cause and effect format, such as “if X occurs, then Y happens.”
- **Risk Category**: An organizing construct that enables multiple risk register entries to be consolidated. This value is important for comparing across risk registers during the risk aggregation step of ERM. Examples of organizing constructs include:

  a. SP 800-53 Control Families: Access Control (AC), Audit and Accountability [AU]).

b. CSF Functions and Categories
c. Mission/business process (e.g., risks to payroll)
d. Information systems

- **Inherent Assessment—Impact**: Analysis of the potential benefits or consequences resulting from this scenario if no additional response is provided. On the first iteration of the risk cycle, this may also be considered the initial assessment.
- **Inherent Assessment— Likelihood**: An estimation of the probability using a percentage of likelihood, before any risk response, that this scenario will occur. On the first iteration of the risk cycle, this may also be considered the initial assessment.
- **Inherent Assessment— Exposure Rating**: A calculation of the likely risk exposure based on the inherent likelihood estimate and the determined benefits or consequences of the risk. Throughout this report, the combination of impact and likelihood is referred to as exposure. Other common frameworks use different terms for this combination, such as level of risk (ISO 31000, NIST SP 800-30 Rev. 1). On the first iteration of the risk cycle, this may also be considered the initial assessment.
- **Risk Response Type**: The risk response (sometimes referred to as the risk strategy or risk treatment) for handling the identified risk. Values for risk response types are provided in Table 4.

Table 4: Risk Response Types

| Type | Description |
|---|---|
| Accept | Accept cybersecurity risk within risk tolerance levels without the need for additional action. |
| Transfer | For cybersecurity risks that fall outside of tolerance levels, reduce them to an acceptable level by sharing a portion of the consequences with another party (e.g., cybersecurity insurance). While some of the financial consequences may be transferrable, there are often consequences that cannot be transferred, like loss of customer trust. |
| Mitigate | Apply actions (e.g., security controls discussed in Section 3.5.1) that reduce the threats, vulnerabilities, and impacts of a given risk to an acceptable level. Responses could include those that help prevent a loss (i.e., reducing the probability of occurrence or the likelihood that a threat event materializes/succeeds) or that help limit such a loss by decreasing the amount of damage and liability. |
| Avoid | Apply responses to ensure that the risk does not occur. Avoiding a risk may be the best option if there is not a cost-effective method for reducing the cybersecurity risk to an acceptable level. The cost of the lost opportunity associated with such a decision should be considered as well. |

- **Risk Response Cost**: The estimated cost of applying the risk response.
- **Risk Response Description**: A brief prose description of the risk response.

- **Risk Owner**: One or more parties (senior executives) that are responsible for managing and monitoring the selected risk response.
- **Status**: A field for tracking the current condition of this risk and any next steps. Valid status values are provided in Table 5.

Table 5: Risk Status Values

| Status | Description |
|---|---|
| Completed | The risk response for this risk has been implemented and is in place. |
| Not started | The risk response for this risk has not been initiated yet. |
| In process | The risk response for this risk is being implemented. |
| Delayed | The risk response for this risk has been deferred. |

- **Status Date:** The date of the status provided in the format dd-Mmm-YY.

### NRC Cybersecurity Risk Management Strategy Change History

| Date | Version | Description of Changes | Method Used to Announce & Distribute | Training |
|---|---|---|---|---|
| 22-Sep-20 | Draft | Initial document | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |