EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

May 19, 2017

M-17-25

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Mick Mulvaney
Director

SUBJECT: Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Overview and Purpose

On May 11, 2017, the President signed the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which outlines a number of actions to enhance cybersecurity across Federal agencies and critical infrastructure partners. Section 1 of the Executive Order reinforces the *Federal Information Security Modernization Act of 2014* (FISMA) by holding agency heads accountable for managing the cybersecurity risks to their enterprises. This Memorandum provides implementing guidance on actions required in Section 1 of the Executive Order.

Managing Agency and Government-wide Cybersecurity Risks

The Executive Order recognizes the increasing interconnectedness of Federal information and information systems and requires agency heads to ensure appropriate risk management not only for the agency's enterprise, but also for the Executive Branch as a whole. In particular, agency heads are required to 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.[1] The Executive Order directs agency heads to produce a risk management report to the Director of Office of Management and Budget (OMB)

[1] FISMA requires agencies to implement information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of "information collected or maintained by or on behalf of [an] agency" and "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency". 44 U.S.C. § 3554.

and the Secretary of the Department of Homeland Security (DHS) within 90 days of its publication.

An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public.[2] Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political, and a broad range of operational risks such as information security, human capital, business continuity, and related risks.[3] Accordingly, the Federal Government is adopting the *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework) to manage the cybersecurity component of enterprise risk as directed in the Executive Order, consistent with prior OMB memoranda and circulars.

The guidance below provides agency heads with instructions for meeting the risk management reporting requirement in the Executive Order, including the methodology for how agencies are to submit their reports, and actions agencies are required to take to implement the Framework.

I. Designating Senior Accountable Official for Risk Management

Effective management of cybersecurity risk requires that agencies align information security management processes with strategic, operational, and budgetary planning processes. To support this alignment, **on or before May 26, 2017, agencies must notify OMB of the senior accountable official (the agency head or a designated official) that will be responsible for implementing of Section 1(c) of the Executive Order**. If the agency head delegates this authority, the individual must be a direct report to the agency head, have vision into all areas of the organization, particularly those focused on risk management, possess authority for both funding and management of IT and enterprise risk, and be able to represent the challenges and opportunities across the enterprise.

Please submit the name of the senior accountable official to ombcyber@omb.eop.gov and your Resource Management Office (RMO) representative.

I. Reporting on Agency Risk Management Assessment

A critical component of implementing the Executive Order, as well as managing cybersecurity risk in general, is for agencies to understand risk in terms of agency mission and their ability to deliver necessary public services. The Executive Order directs each agency to provide a risk management report to OMB and DHS.

The FY 2017 FISMA CIO metrics provide a consistent methodology for assessing capabilities that address and/or mitigate cybersecurity risks. Accordingly, in an effort to minimize the reporting burden, **all agencies, including all small agencies, must submit responses to the FY 2017 Quarter 3 FISMA CIO metrics, through the DHS CyberScope system, on or before**

[2] See OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, for additional guidance on managing enterprise risks.
[3] See the *Enterprise Risk Management Playbook* for additional information.

July 14, 2017 in accordance with the deadline established in OMB Memorandum M-17-05 *FY 2016 -2017 Guidance on Federal Information Security and Privacy Management Requirements*. These submissions will serve as the agency risk-management report specified in Section 1(c) of the Executive Order.

Additionally, OMB and DHS will use the FISMA metrics to produce agency-specific risk assessment and will include these assessments in a report to the President in accordance with the Executive Order. OMB will provide initial assessments to agencies for review and responses no later than July 28, 2017, and **will require each agency to provide a written response to the assessment that is signed by the agency head or the agency head's designated senior accountable official and describes how the agency plans to accept, avoid, transfer, or mitigate outstanding risks by August 9, 2017**. OMB and DHS will also use the aggregate information in the report to the President, as it will serve as the basis for identifying new technology needs and areas in which government could consolidate services to improve the cybersecurity posture of the executive branch. At a minimum, the Chief Financial Officer Act agencies and small agencies will continue to conduct these risk assessments on a semiannual and annual basis, respectively, to enable tracking of agency performance and trend analysis against the Framework. OMB will provide reporting deadlines for these agencies as part of its annual FISMA guidance, in accordance with the statute. For more information on the risk assessment methodology, please refer to Appendix 1 of this memorandum.

II. Action Plan for Implementation of the Framework

The Executive Order requires agency heads to describe planned actions that his or her agency will undertake to align their agencies' activities with the Framework. The Framework provides a standard for managing and reducing cybersecurity risks, organizing capabilities around its five function areas: Identify, Protect, Detect, Respond, and Recover. The Framework, when used in conjunction with NIST Special Publications 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, and 800-37, *Risk Management Framework to Federal Information Systems*, as well as other associated standards and guidelines, provides agencies with a comprehensive structure for making informed, risk-based decisions and managing cybersecurity risks across their respective enterprises.

Illustrating the value of utilizing the Framework to organize cybersecurity decision making, OMB and DHS have already worked with CIOs and Inspectors General (IG) across the Executive Branch to align the FISMA metrics to the Framework's function areas. To increase consistency regarding cybersecurity capabilities and budgeting activities, OMB also aligned the Information Technology (IT) Security portion of the FY 2018 IT Budget Capital Planning Guidance with the Framework. This alignment has helped to standardize common vocabulary and the fundamental definitions used in security, mirroring the standardization that is increasingly necessary and useful with private sector suppliers, vendors, and industry partners. Eventually, this will allow greater sharing of best practices within the government and between government and industry; increase alignment of IT security requirements and capabilities across the executive branch; and, enhance efforts to improve the state of cybersecurity risk in both the public and private sectors.

In describing the agency action plan to implement the Framework, agencies must include:

- The status of planning, organizing, and submitting IT Budget materials, as directed in the FY 2018 IT Budget Capital Planning Guidance, that are aligned with the Framework;
- Proposed internal management of cybersecurity risk using the updated metrics aligned to the Framework;
- A timeline to map existing and planned capabilities with the Framework functions; and
- Proposed use of the terminology and concepts in the Framework to organize and communicate cybersecurity activities and outcomes.

All agencies, including small agencies, must submit their Framework Implementation Action Plan in .PDF format through DHS CyberScope by on or before July 14, 2017, in addition to responding to the questions in CyberScope.

NIST will provide a plan for updating its guidelines, as appropriate, to incorporate elements of the Framework.

Conclusion

As we implement the direction of the Executive Order, it is vital that you remain personally engaged in monitoring the progress of your agency. OMB and DHS will be working with your agency to improve cybersecurity risk management. Your support is critical to that improvement.

Point of Contact

Grant Schneider, Acting Federal Chief Information Security Officer, OMB - ombcyber@omb.eop.gov

This table details all actions in the Memorandum above:

Requirement	Deadline	Responsible Agencies
1. Agencies must notify OMB of the senior accountable official (whether the agency head or the agency head's designee) responsible for the implementation of Section 1(c) of the Executive Order.	May 26, 2017	All Federal Agencies
2. Agencies must submit responses to the FY 2017 Quarter 3 FISMA CIO metrics, through the DHS CyberScope system.	July 14, 2017	All Federal Agencies
3. Each agency to provide a written response to the assessment that is signed by the senior accountable official (agency head or the agency head's designee)	August 9, 2017	All Federal Agencies

and describes how the agency plans to accept, avoid, transfer, or mitigate outstanding risks.		
4. Agencies must submit their Framework Implementation Action Plan in .PDF format through DHS CyberScope.	July 14, 2017	All Federal Agencies

Appendix 1: Criteria for Assessment of Cybersecurity Risk Management

As set forward in Section 1(c) of Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, OMB will provide agencies with an assessment of agency cybersecurity risk management. The risk management assessment will rely on information submitted by agencies pursuant to FISMA and OMB Memorandum M-17-05, *FY 2016 -2017 Guidance on Federal Information Security and Privacy Management Requirements*. Specifically, the risk management assessment is a snapshot of each agency's cybersecurity risk posture based on those metrics and outcomes agencies submitted.

To produce this risk management assessment, OMB will use a combination of *FY 2016 FISMA Inspectors General (IG) metrics* and *FY 2017 FISMA Chief Information Officer (CIO) metrics*, which leverage the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework). The security-based outcomes were sorted into Security Domains, each of which has been organized under one of the five NIST Framework functions: Identify, Detect, Protect, Respond, and Recover. OMB will rate agencies under each of these Security Domains according to their current level of risk:

- **High Risk**: Key, fundamental cybersecurity policies, processes, and tools are either not in place or not sufficiently deployed, creating a high risk environment for the agency's information and systems.
- **At Risk**: Some essential policies, processes, and tools are in place to mitigate overall cybersecurity risk, but significant gaps remain that place agency information security at risk of compromise.
- **Managing Risk**: The agency has instituted required information security policies, procedures, and tools and is able to actively manage the cybersecurity risk to the enterprise.

The risk levels for each Security Domain are then used to calculate the overall risk level for the function area (e.g., Identify as at risk, and Detect as managing risk).

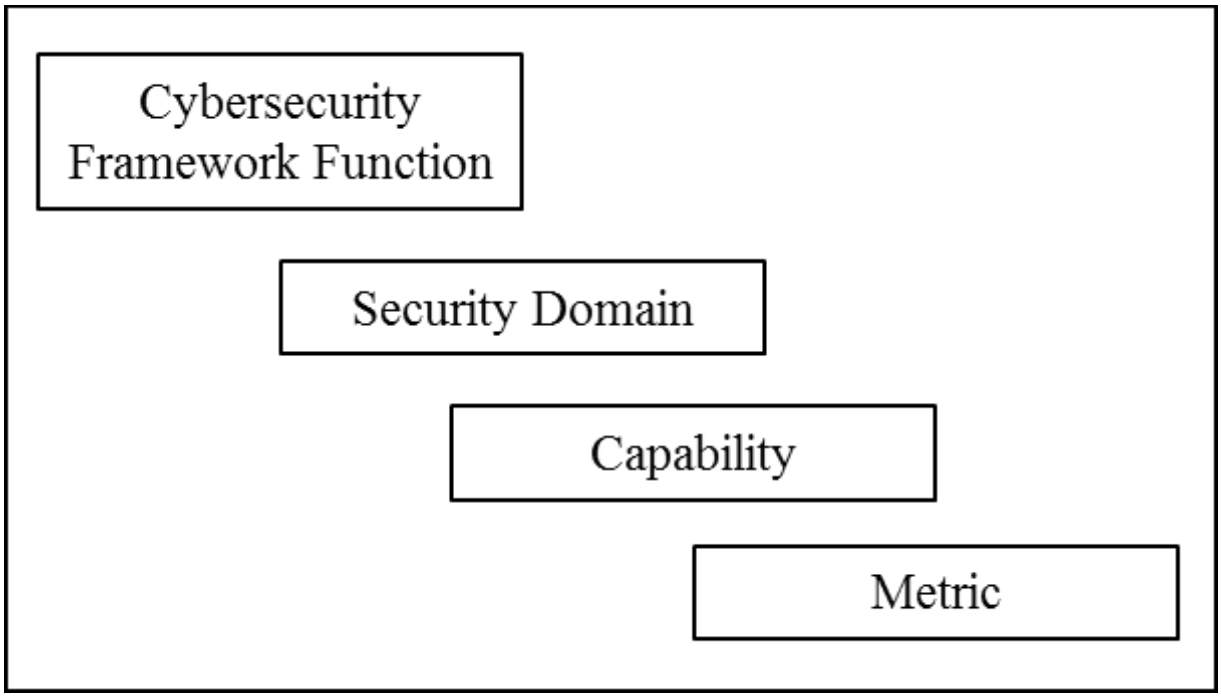
In addition to the FISMA metrics in this assessment, agencies are required to provide narrative responses regarding their risk management decision processes. OMB will use this information to gather relevant context for the agencies' risk management assessment, specifically how an agency assesses, responds to, and monitors risks. Agencies are asked to:

1. Provide a narrative assessment of the cybersecurity risks to the agency. This assessment should include risks to the agency's High Value Assets and Mission Essential Functions, as well as results of agency level and program specific security reviews.
2. Describe the strategy or approach for managing the identified risks, including decisions to accept or mitigate risks within the enterprise, including decisions to accept, transfer, or mitigate risk. Please consider specific risk factors (threats, vulnerabilities, likelihoods, and impacts) that have driven risk management decisions and include the strategic, operational, and budgetary considerations that went into the decisions, especially related to any accepted risk from unmitigated vulnerabilities.

3. Describe gaps that have been identified and the capabilities needed to resolve the highest priority risks. Additionally, provide whether the agency has aligned its efforts and resources (budget, tools, people, and processes) to provide for the capabilities needed to close these gaps.
4. What role does the agency's senior leadership play in the development and ongoing implementation of the agency's cybersecurity risk management strategy, and how does this strategy integrate with the broader enterprise risk management process required by Circular A-123? Please include a description of the processes and procedures that are in place to keep senior leadership apprised of risks within the enterprise, including the frequency of senior leadership engagement, and the impact that this senior leadership engagement has on decisions related to how resources are allocated.

Below is a description of the Framework functions, as well as the Security Domains and the capabilities that underlie them. Additionally, each capability includes a reference to the FISMA CIO or IG metric that will be used to determine whether the agency is currently engaging in the activity at the government-wide target level.

Figure 1. Levels of Risk Management Assessment



The section below details the assessment criteria in each of the Framework functions.

Identify

The capabilities in the Identify function are foundational for effective use of the Cybersecurity Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Identify includes the following Security Domains:

Asset Management and Authorization – In order to promote a robust information security posture, agencies must ensure that systems operating on their networks are appropriately authorized to operate and that, overall, they understand the assets connecting to their networks. This helps to manage the risk of threat delivery and initial system compromise.

- The organization's hardware assets are covered by an enterprise-level automatic hardware asset inventory capability. (FISMA CIO Metrics, 1.2, 1.4)
- The organization's software assets are covered by an enterprise-level automatic software asset inventory capability. (FISMA CIO Metrics, 1.2.1, 1.2.2, 1.5)
- The organization's unclassified networks possess a technology solution to detect and alert on the connection of unauthorized hardware assets. (FISMA CIO Metrics, 3.16)
- The organization's endpoints and mobile assets are covered by a capability to detect, alert, and/or block unauthorized software from executing. (FISMA CIO Metrics, 3.17)
- The organization's unclassified systems have active security ATOs. (FISMA CIO Metrics: 1.1.1, 1.1.2, 1.1.3)
- Ongoing information system authorizations are based on the risk to operations and assets, individuals, other organizations, and the Nation should a compromise occur. (FISMA IG Metrics, 1.1.11)

Comprehensive Risk Management – Information security is reliant on frequent assessments of the risks to the systems and information operated by a given organization, and the results of these assessments must be incorporated into how the agency conducts its business and operations. This helps to manage the risk of threat delivery, initial system compromise, and threat persistence.

- The organization has developed a risk management function with a comprehensive governance structure and organization-wide risk management strategy. (FISMA IG Metrics, 1.1.2)
- The organization incorporates mission and business process-related risks into risk-based decisions at the organizational perspective. (FISMA IG Metrics, 1.1.3)
- Information system-level risk assessments integrate risk decisions from the organizational and mission/business process perspectives. (FISMA IG Metrics, 1.1.4)
- The organization provides timely communication of specific risks at the information system, mission/business, and organization-level. (FISMA IG Metrics, 1.1.5)
- The organization performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FISMA IG Metrics, 1.1.6)
- The organization implements appropriate baseline security controls based on mission/business requirements and policies. (FISMA IG Metrics, 1.1.8)

- Officials at the program- and executive-levels are actively involved in the ongoing management of information-system-related security risks. (FISMA IG Metrics, 1.1.15)

Protect

The Protect function seeks to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services and supports the ability to limit or contain the impact of a potential cybersecurity event. Protect includes the following Security Classes:

Remote Access Protection – In an ever more interconnected world, it is vital to promote the security of remote connections to Federal IT resources and information in order to defend against the delivery of potential threats, initial system compromise, unauthorized credential access, cyber defense evasion, and the lateral movement of adversaries.

- Remote connections utilize FIPS 140-2 validated cryptographic modules. (FISMA CIO Metrics, 2.20.1)
- Remote connections timeout after 30 minutes of inactivity. (FISMA CIO Metrics, 2.20.2)
- Remote connections prohibit the use of split tunneling and/or dual-connected remote hosts. (FISMA CIO Metrics, 2.20.3)

Credentialing and Authorization – Federal agencies must have an understanding as to who is on their networks, what their privileges are, and how often those privileges are reviewed in accordance with the principle of least privilege. Such knowledge and control can reduce the risks posed by initial threat delivery, threat persistence, privilege escalation, cyber defense evasion, unauthorized credential access, internal reconnaissance, lateral movement, system observation, and information exfiltration.

- Unprivileged network users are technologically required to log onto the network with a two-factor PIV card or other NIST LOA 4 credential. (machine-based enforcement) (FISMA CIO Metrics, 2.4, 2.4.1)
- Privileged network users are technologically required to log onto the network with a two-factor PIV card or other NIST LOA 4 credential (machine-based enforcement). (FISMA CIO Metrics, 2.5, 2.5.1)
- Users with privileged local system accounts are technologically required to log onto the network with a two-factor PIV card or other NIST LOA 4 credential (machine-based enforcement). (FISMA CIO Metrics, 2.11, 2.12)
- The organization's physical access control systems electronically accept and authenticate PIV credentials for access. (FISMA CIO Metrics, 2.17)
- The organization ensures all users are only granted access base on the principles of least privilege and separation of duties. (FISMA IG Metrics, 2.2.2)
- The organization tracks and controls the use of administrative privileges and ensures privileges are periodically reviewed and adjusted in accordance with policy. (FISMA IG Metrics, 2.2.7)
- The organization identifies, limits, and controls the use of shared accounts. (FISMA IG Metrics, 2.2.9)

Network Protection – The threats posed to Federal networks are diverse, and agencies must have robust policies and procedures in place to defend against the potential dangers they pose. Such

measures help to defend against threat delivery, initial system compromise, command and control threats, lateral threat movement, threat persistence, and cyber defense evasion.

- The organization's unclassified networks are assessed for vulnerabilities using Security Content Automation Protocol (SCAP) validated products. (FISMA CIO Metrics, 2.2)
- The organization's assets are covered by auditing for compliance with the appropriate security configuration baseline. (FISMA CIO Metrics, 2.31, 2.3.2, 2.3.3)
- The organization's unclassified networks are covered by a capability that blocks unauthorized devices from connecting. (FISMA CIO Metrics, 2.1)
- Government furnished endpoints and mobile assets encrypt data at rest. (FISMA CIO Metrics, 1.2.1, 1.2.2, and 2.19)
- Organization possesses an Insider Threat program deemed by the National Insider Threat Task Force to be at Full Operating Capability. (FISMA CIO Metrics, 2.35)
- An enterprise-level policy is in place that covers the destruction of media containing sensitive information. (FISMA CIO Metrics, 2.36)

Detect

The Detect function necessitates the ability to identify the occurrence of a cybersecurity and enables timely discovery of cybersecurity events. Detect includes the following Security Classes.

Anti-Phishing Capabilities – One of the most persistent and pervasive threats to Federal networks is the social engineering attack known as phishing, which attempts to obtain information from individuals through the use of legitimate-seeming identities to distribute infected file attachments and websites. Anti-phishing technologies help to defend against the delivery of potential threats as well initial system compromise.

- The organization's users demonstrate understanding of phishing threats by passing associated tests. (FISMA CIO Metrics, 2.3, 2.3.1)
- Incoming email traffic passes through anti-phishing and anti-spam filters at the outermost border mail agent or server. (FISMA CIO Metrics, 3.1)
- Incoming email traffic is analyzed using sender authentication protocols. (FISMA CIO Metrics, 3.2)
- Incoming email traffic is analyzed using a reputation filter. (FISMA CIO Metrics, 3.3)
- Incoming email traffic is analyzed to detect for clickable URLs, embedded content, and attachments. (FISMA CIO Metrics, 3.4)
- Incoming email traffic is analyzed for suspicious or potentially nefarious attachments and opened in a sandboxed environment or detonation chamber. (FISMA CIO Metrics, 3.5)
- Outgoing email traffic enables recipients to verify the originator using sender authentication protocols. (FISMA CIO Metrics, 3.6)

Malware Defense Capabilities – Often a component of phishing attacks, malware is the larger category of malicious software designed to infect and compromise information systems and data. Defending against malware incidents is important in order to defend against the delivery of potential threats, initial system compromise, and cyber defense evasion.

- Endpoints are covered by an intrusion detection system. (FISMA CIO Metrics, 3.7)
- Endpoints are covered by an antivirus solution using file reputation services based on continuously updated malware information. (FISMA CIO Metrics, 3.8)

- Government furnished endpoints are covered by an anti-exploitation tool. (FISMA CIO Metrics, 3.9)
- Government furnished endpoints are protected by a browser-based or enterprise-based tool that blocks known phishing websites and IP addresses. (FISMA CIO Metrics, 3.10)
- The organization's assets are scanned for malware prior to an authorized remote access connection to the unclassified network. (FISMA CIO Metrics, 3.11, 3.11.1)

Exfiltration and Other Defense Capabilities – Phishing and malware are only two of the many threats facing Federal networks, which is why it is important for agencies to have robust defense beyond those targeting these two categories of threats. This is particularly true with regards to detecting and responding to the potential external transfer of Federal information. These controls provide a bulwark against not only threat delivery and initial system compromise, but also internal reconnaissance and data exfiltration.

- Users with privileged network accounts have a technical control limiting access to only trusted sites (FISMA CIO Metrics, 3.12)
- Inbound network traffic passes through a web content filter, which provides anti-phishing, anti-malware, and blocking of malicious websites (FISMA CIO Metrics, 3.13)
- Outbound communications traffic is checked to detect encrypted exfiltration of information (FISMA CIO Metrics, 3.14)
- Emails are processed by systems that quarantine or otherwise block suspected malicious traffic (FISMA CIO Metrics, 3.15)
- The organization has the ability to detect attempts to access large volumes of data and investigates such instances (FISMA CIO Metrics, 3.19)
- The organization conducts exfiltration tests at least annually (FISMA CIO Metrics, 3.18)
- EINSTEIN tools are fully implemented (Department of Homeland Security)

Respond

The Respond function seeks to develop and implement the appropriate activities to take action regarding a detected cybersecurity event and supports the ability to contain the impact of a potential cybersecurity event. Respond includes the following Security Classes.

Planning and Processes – An essential component of strong incident response activities is having plans and procedures in place should a vulnerability be uncovered or an incident occur and regularly testing those capabilities to ensure they operate effectively. Such planning and processes can prevent the initial compromise of systems, privilege escalation, and lateral threat movement, as well as mitigate the potential impact of incidents.

- The organization mitigates all significant vulnerabilities within 30 days of notification (DHS NCATS Vulnerability Scans)
- The organization has an enterprise-level incident response plan that is tested at least twice annually (FISMA CIO Metrics, 4.1, 4.6)
- Incident commanders are empowered to direct and manage cybersecurity incidents (FISMA CIO Metrics, 1.6)
- Incident response roles have been validated during or prior to incident response testing (FISMA CIO Metrics, 4.5)
- Incident response processes are consistently implemented across the organization (FISMA IG Metrics, 4.3.1.5)

- The organization has processes in place to collaborate with DHS, and other parties as appropriate, to quickly acquire incident response resources and assistance (FISMA IG Metrics, 4.3.1.6.)

Evaluation and Improvement – In order to ensure incident response activities function as intended, it is vital that agencies utilize metrics and evaluation criteria to assess their programs as part of an effort to continually improve response performance. These efforts can help to improve the efficacy with which the agency is able to lessen the impact of incidents.

- Qualitative and quantitative data is utilized to determine the effectiveness of the organization's incident response processes (FISMA IG Metrics, 4.4.1.4)
- The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices (FISMA IG Metrics, 4.5.1.2)
- The rigor, intensity, scope, and results of incident response activities are comparable and predictable across the organization (FISMA IG Metrics, 4.3.1.9)
- Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format (FISMA IG Metrics, 4.4.1.5)
- Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities (FISMA IG Metrics, 4.4.1.7)

Recover

The Recover function seeks to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event and supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Recover includes the following Security Classes.

Planning and Testing – As in the case of incident response, a strong incident recovery program requires advanced planning of activities as well as testing of those plans to ensure they execute properly. This enhances agencies' ability to restore capabilities and/or services following an incident or disaster.

- The organization has a business continuity plan at the enterprise-level that is tested annually (FISMA CIO Metrics, 5.5)
- The organization has incident recovery plan at the enterprise-level and it is tested annually (FISMA CIO Metrics, 5.6)
- The organization has a disaster recovery plan at the enterprise-level and it is tested annually (FISMA CIO Metrics, 5.7)
- The organization has developed and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels (FISMA IG Metrics, 5.1.3)
- The organization develops and facilitates recovery testing, training, and exercise (TT&E) programs (FISMA IG Metrics, 5.1.1)
- The organization incorporates Business Impact Analysis and Business Process Analysis into analysis and strategy toward the development of continuity and recovery plans (FISMA IG Metrics, 5.1.2)

Personal Impact Processes – For those cases in which personally identifiable information (PII) has been, or potentially could have been, compromised, it is imperative that organizations have in place capabilities to notify affected persons and provide them with necessary identification protection tools and/or services. This ensures that agencies are providing potentially affected persons with timely information and identity protections tools, which helps to preserve public confidence in the government.

- The organization has a policy in place that establishes a timeline for public and internal notifications following the detection or discovery of a compromise of PII. (FISMA CIO Metrics, 5.8)
- The organization has established metrics for tracking compliance with the timelines set forth in applicable policy and fully adheres to its policy. (FISMA CIO Metrics, 5.9, 5.3)
- The organization has either contracted credit monitoring services in the case of a breach of PII or produced cost projections based on potential scenarios. (FISMA CIO Metrics, 5.11)
- The organization has either contracted credit repair services in the case of a breach of PII or produced cost projections based on potential scenarios. (FISMA CIO Metrics, 5.10, 5.11)

Back-Up Capacity – If an organization loses the capacity to execute upon its mission, whether due to an incident or a disaster, it is important that back-up facilities and capabilities have been designated and are prepared to come online. Such capabilities enhance organizational resilience and aid in the restoration of agency capabilities and services.

- The Organization has identified, through risk assessments, alternate processing and storage sites that are not subject to the same physical and/or cybersecurity risks as the primary sites. (FISMA IG Metrics, 5.1.8)
- Backups of information are conducted at the user- and system-levels that protect the confidentiality, integrity, and availability of backup information at storage sites. (FISMA IG Metrics, 5.1.9)

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu