May 27, 2022

MEMORANDUM

SUBJECT: Notification of Evaluation:
EPA Compliance with the Federal Information Security Modernization Act for FY 2022
Project No. OA-FY22-0134

FROM: LaSharn Barnes, Director   *LaSharn Barnes*
Information Resources Management Directorate
Office of Audit

TO: Kimberly Patrick, Principal Deputy Assistant Administrator
Office of Mission Support

Joseph Goffman, Principal Deputy Assistant Administrator
Office of Air and Radiation

The Office of Inspector General for the U.S. Environmental Protection Agency plans to begin an evaluation of the EPA's compliance with the Federal Information Security Modernization Act of 2014. This evaluation is statutorily required. This evaluation is part of the OIG's oversight plan for fiscal year 2022. This evaluation also addresses the following fiscal year 2022 top management challenge(s) for the Agency: *Protecting information technology and systems against cyberthreats.*

Our objective is to conduct an independent evaluation of the EPA's compliance with the *U.S. Department of Homeland Security Fiscal Year 2022 Inspector General FISMA Reporting Metrics*. We plan to conduct work at the Office of Mission Support and the Office of Air and Radiation at EPA headquarters. The evaluation will be conducted using *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency. The anticipated benefit of this evaluation is to contribute to the Agency's theme of "Embracing EPA as a High-Performing Organization."

We will contact you to arrange a mutually agreeable time to discuss our objective. We would also be particularly interested in any areas of concern that you may have. We will answer any of your questions about the evaluation process, reporting procedures, methods used to gather and analyze data, and what we should expect of each other during the evaluation. Throughout the evaluation, we will provide updates on a regular basis.

We have attached our initial documentation requests which include the corresponding FISMA metric numbers and responsible offices (Attachment A). These requests relate to the Agency's information technology process and the Analytical Radiation Data System (ARadDS), the Agency's only High Value Asset categorized as a High Impact system. Additionally, the *FY22 Core IG Metrics Implementation Analysis and Guidelines* issued by OMB for FISMA this year can be found in Attachment B for your

reference. To expedite our evaluation, please be ready to provide the information listed in Attachment A at the entrance conference.

We respectfully note that the OIG is authorized by the Inspector General Act of 1978, as amended, to have timely access to personnel and all materials necessary to complete its objectives. Similarly, EPA Manual 6500, *Functions and Activities of the Office of Inspector General* (1994), requires that each EPA employee cooperate with and fully disclose information to the OIG. Also, Administrator Michael S. Regan, in an April 28, 2021 email message to EPA employees, conveyed his "expectation that EPA personnel provide OIG timely access to records or other information" and observed that "full cooperation with the OIG is in the best interest of the public we serve." We will request that you immediately resolve the situation if an Agency employee or contractor refuses to provide requested materials to the OIG or otherwise fails to cooperate with the OIG. We may report unresolved access matters to the administrator and include the incident in the *Semiannual Report to Congress*.

We will post this memorandum on our public website at www.epa.gov/oig.

cc: Janet McCabe, Deputy Administrator
 Dan Utech, Chief of Staff, Office of the Administrator
 Jon Monger, Associate Deputy Administrator
 Wesley J. Carpenter, Deputy Chief of Staff, Office of the Administrator
 Andrew Schreyer, Deputy Assistant Administrator
 Dan Coogan, Acting Director, Office of Resources and Business Operations
 Elizabeth Shaw, Deputy Assistant Administrator for Air and Radiation
 Andrew LeBlanc, Agency Follow-Up Coordinator
 José Kercado, Backup Agency Follow-Up Coordinator
 Daniela Wojtalewicz, Audit Follow-Up Coordinator, Office of Mission Support
 Michael Benton, Audit Follow-Up Coordinator, Office of the Administrator
 Marc Vincent, Audit Follow-Up Coordinator, Office of Air and Radiation
 Eunjee Koh, Audit Follow-Up Coordinator, Office of Air and Radiation
 Grant Peacock, Audit Follow-Up Coordinator, Office of Air and Radiation
 Marilyn Armstrong, Deputy Director, Office of Resource and Business Operations, Administrative
  Operations Division, Office of Mission Support
 Lindsay Hamilton, Associate Administrator for Public Affairs
 Lance McCluney, Director, Office of Administrative and Executive Services, Office of
  the Administrator
 Jeffrey Prieto, General Counsel, Office of the Administrator
 William Niebling, Associate Administrator for Congressional and Intergovernmental Relations
 Stefan Martiyan, Director, Office of Continuous Improvement, Office of the Chief Financial
  Officer
 Vaughn Noga, Deputy Assistant Administrator for Environmental Information and Chief
  Information Officer, Office of Mission Support
 Regional Audit Follow-Up Coordinators, Regions 1–10
 Elizabeth Shaw, Deputy Assistant Administrator, Office of Air and Radiation
 Andrew Schreyer, Deputy Assistant Administrator, Office of Mission Support
 Brian Epley, Director, Office of Information Technology Operations, Office of Mission Support
 David Updike, Deputy Director, Office of Information Technology Operations, Office of
  Mission Support
 Tonya J. Manning, Director, Office of Information Security and Privacy, Office of
  Mission Support

Robert Kelly, Director, Office of Information Security and Privacy, Training, Compliance, and
    Oversight, Office of Mission Support
Sean W. O'Donnell, Inspector General
Charles J. Sheehan, Deputy Inspector General
Benjamin May, Counsel to the Inspector General
Stephanie L. Wright, Assistant Inspector General for Management
Kellie J. Walker, Chief of Staff, Office of Inspector General
Katherine Trimble, Assistant Inspector General for Audit
Paul H. Bergstrand, Assistant Inspector General for Special Review and Evaluation
Marc Perez, Acting Assistant Inspector General for Investigations
Jee Kim, Deputy Assistant Inspector General for Management
Tom Collick, Deputy Counsel to the Inspector General
Laura B. Nicolosi, Principal Deputy Assistant Inspector General for Audit
Erin Barnes-Weaver, Deputy Assistant Inspector General for Evaluation
James Hatfield, Deputy Assistant Inspector General for Audit
Susan Barvenik, Associate Deputy Counsel to the Inspector General
Jennifer Kaplan, Deputy Assistant Inspector General for Congressional and Public Affairs
Jeffrey Lagda, Congressional and Media Liaison, Office of Inspector General
Lori Hoffman, Congressional and Media Liaison, Office of Inspector General

Request #	Associated FISMA Metric #	Document Request	Estimated Relevant Office	OIG POC
1		Agency hardware inventory list	OMS	Sabrena Stewart
	2	Information Component Inventory for ARadDS	OAR	Sabrena Stewart
2		ARadDS vulnerability scan reports covering system hardware for FY22's 1st, 2nd, and 3rd quarter.	OAR	Sabrena Stewart
3		Report/listing of any unauthorized hardware identified between Oct 2021 - May 2022.	OMS	Sabrena Stewart
4		Listing of ARadDS incident tickets for FY22's 2nd and 3rd quarter.	OAR	Sabrena Stewart
5		ARadDS Firewall configuration settings	OAR	Sabrena Stewart
6		Last 3 Risk Assessment Reports for ARadDS	OAR	LaVonda Harris-Claggett
7	5	Security and Privacy planning policy and procedures relevant to ARadDS	OAR	LaVonda Harris-Claggett
8		System Security Plan for ARadDS (prior to the version currently in Xacta)	OAR	LaVonda Harris-Claggett
9		Internal communications (mass emails, meeting minutes) discussing ARadDS risk management to stakeholders from Oct 2021 - May 2022	OAR	LaVonda Harris-Claggett
10	10	System level POA&Ms for ARadDS from for FY22's 2nd and 3rd quarter	OAR	LaVonda Harris-Claggett
11		Access control policy and procedures for ARadDS	OAR	LaVonda Harris-Claggett
12		Names or list of contractors associated with ARadDS operations	OAR	Alonzo Munyeneh
13	14	Associated contracts for contractors identified in request #12 above	OAR	Alonzo Munyeneh
14		RFP for ARadDS	OAR	Alonzo Munyeneh
15		Documentation of Agency review of ARadDS acquisition package (i.e. Response to RFP)	OAR	Alonzo Munyeneh
16	20	ARadDS vulnerability scan reports for FY22's 1st, 2nd, and 3rd quarter.	OAR	Alonzo Munyeneh
17	21	System generated evidence (screenshot or export) of database version for ARadDS	OAR	Alonzo Munyeneh
18	30	ARadDS operating system authentication configurations	OAR	Sabrena Stewart
19		E-Authentication Risk Assessment for ARadDS	OAR	Sabrena Stewart
20		Listing of ARadDS application's privileged user accounts by type	OAR	Sabrena Stewart
21	32	List of auditable events for ARadDS privileged users by system type	OAR	Sabrena Stewart
22		List of users by type and role for ARadDS	OAR	Sabrena Stewart
23		ARadDS's reports of SSL (Secure Socket Layer)/TLS (Transport Layer Security) across external communication boundaries for FY22's 2nd and 3rd quarter	OAR	Eric K Jackson
24	36	Supporting artifacts that captures testing of ARadDS's network access controls or other methods used to prevent and detect untrusted removable media	OAR	Eric K Jackson
25		Digital media destruction and sanitization procedures associated with ARadDS	OAR	Eric K Jackson
26		Listing of ARadDS media disposed from Oct 2021 - May 2022	OAR	Eric K Jackson
27		ARadDS's DNS records audit logs for FY22's 2nd and 3rd quarter	OAR	Eric K Jackson
28	37	ARadDS system logs that capture web content filters and reports associated with capturing monitoring of inbound and outbound network traffic for phishing, malware, and domain filtering for FY22's 2nd and 3rd quarter	OAR	Eric K Jackson
29	42	Agency Cybersecurity Workforce assessment	OMS	Sabrena Stewart
30		Action plan for the workforce assessments	OMS	Sabrena Stewart
31	47	Latest continuous monitoring report/dashboard that includes ARadDS	OAR	Alonzo Munyeneh
32		Documentation of continuos monitoring lessons learned communications for ARadDS	OAR	Alonzo Munyeneh
33		Agency ISCM policies and procedures used for ARadDS	OAR	LaVonda Harris-Claggett
34	49	Last 3 ARadDS security control assessments	OAR	LaVonda Harris-Claggett
35		Name of system used for application security testing	OAR	LaVonda Harris-Claggett
36	54	Screen Shots of ARadDS system configurations that captures the implemented security controls to prevent data exfiltration and network defenses	OAR	Eric K Jackson
37		Last recent 2 lessons learned performed on the effectiveness of ARadDS's incident detection policies and procedures.	OAR	Eric K Jackson
39	61	Last 3 ARadDS Business Impact Analysis reports	OAR	LaVonda Harris-Claggett
40		Contingency Planning policies and procedures associated with ARadDS	OAR	LaVonda Harris-Claggett
41	63	Last 3 ARadDS Information System Contingency Plan testing reports	OAR	LaVonda Harris-Claggett
42		Last 3 After action reports for ARadDS	OAR	LaVonda Harris-Claggett

OMB Office of the Federal Chief Information Officer

FY22 Core IG Metrics Implementation Analysis and Guidelines

This document outlines the Office of Management and Budget's (OMB) guidance for implementing the requirements outlined in M-22-05, accompanying the Core Inspector General (IG) Metrics for FY22 provided in Appendix A. The guidance below and related metrics are based on coordinated discussions between (and the consensus opinion of) representatives from OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch (FCEB) Chief Information Security Officers (CISOs) and their staff, and the Intelligence Community (IC). Research, interviews and IG survey data provided quantitative and qualitative information to formulate these guidelines.

Overview and Background

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency IG, or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. Accordingly, the fiscal year (FY) 2022 IG FISMA Reporting Metrics focus on key areas to ensure successful independent evaluations of agencies' information security programs.

The FY 2022 Core IG Metrics represent a continuation of work begun in FY 2016, when the IG metrics were aligned to the five function areas in the *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for assessing cybersecurity capabilities and associated risks implemented across the enterprise and enables the IGs to have a framework for the communication of capabilities and the maturity of controls that support them.

The FY22 Core IG Metrics were chosen based on alignment with Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity, including:

- Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09) – OMB and CISA solicited public feedback on strategic and technical guidance documents meant to move the U.S. government towards a zero trust architecture. The goal of OMB's Federal Zero Trust Strategy is to accelerate agencies towards a baseline of early zero trust maturity.

- Multifactor Authentication (MFA) and Encryption (EO 14028) – Per the EO, agencies were required to fully adopt MFA and encryption for data at rest and in transit by November 8, 2021. For agencies that were unable to meet these requirements within 180 days of the date of the order, the agency head was directed to provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA.

- Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31) – This memorandum provides specific requirements for log management. It includes a maturation model, prioritizing the most critical log types and requirements, to build a roadmap to success.

- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01) – On October 8, 2021, this

memorandum was issued for agencies to focus on improving early detection capabilities, creating "enterprise-level visibility" across components and sub-agencies, and requires agencies to deploy an EDR solution.

- <u>Software Supply Chain Security & Critical Software</u> – Section 4 of EO 14028 tasks OMB, NIST, and other federal entities with developing new guidelines and frameworks to improve the security and integrity of the technology supply chain. In collaboration with industry and other partners, this effort is providing frameworks and guidelines on how to assess and build secure technology, including open source software.

Additionally, OMB Memorandum M-22-05 adjusts the timeline for the Inspectors General evaluation of agency effectiveness to align the results of the evaluation with the budget submission cycle. Historically, the evaluation of agency effectiveness by Inspectors General finished in October. This timing limited agency leadership's ability to request resources in the next Budget Year submissions to provide for remediations. The expectation is this change will reduce the time between issue identification, resource request and allocation. Outlined below is implementation guidance to support IGs as they manage this adjustment.

Determining Effectiveness with Core Metrics

IGs are required to assess the effectiveness of information security programs on a maturity model spectrum. Aligning with the Carnegie Mellon Cybersecurity Maturity Model Certification (CMMI), the foundational levels require agencies to develop sound policies and procedures, while advanced levels capture the extent to which agencies institutionalize those policies and procedures.

Representatives from OMB, FCEB CISO teams, CIGIE, and IC Community agreed that these 20 Core IG Metrics should provide sufficient data to determine the effectiveness of an Agency's information security program with a high level of confidence.

As with previous guidance on the use of the five-level maturity model, a Level 4, *Managed and Measurable*, information security program is still considered operating at an effective level of security. While the determination of effectiveness can be established based on the results of the IG metrics, IGs should continue to consider their own assessment of the unique missions, resources, and challenges faced by their agency when assessing the maturity of information security programs.

To that end, IGs are encouraged to leverage supplemental reports (including past evaluations where results have had little variance year over year), and any additional evidence of information security program effectiveness to provide context within this evaluation period (or past periods, as applicable). OMB requests that IGs consider results that deterministically demonstrate outcomes of security processes through ground truth testing[1] as supportive supplemental information when evaluating for effectiveness. Finally, consideration of agency mission, resources, and challenges should also be considered in the assessment, and be documented in the agency's assessment of risk as discussed in OMB Circular A-123, the U.S. Government Accountability Office's (GAO) Green Book, and NIST SP 800-37/800-39. Collectively, this data can provide IGs alternative methods to determine agencies' overall effectiveness ratings when their offices find contextual data to support an adjustment.

---

[1] Methods that empirically validate security and find weaknesses, such as manual and automated penetration testing and red team exercises. (Source: M-22-05 FISMA Guidance)

Execution of the FY22 IG Evaluation

OMB is requesting Agency IG teams submit Core IG Metrics data from agency evaluations via Cyberscope **no later than July 30, 2022**. Understanding the unique challenges of this transition year, qualitative data and other supplemental reports can be submitted before the end of FY22.

We understand that this transition may impact both existing resources and resource planning. IG teams that utilize contract resources should prioritize their assessment for submission on July 30, 2022. For the remaining period of performance, it is recommended that resources focus on contract modifications for FY23, followed by remediation efforts and closeout activities (prioritizing areas covered by Core Metrics).

IGs should utilize Cyberscope to submit the results of the Core IG Metrics evaluation. Cyberscope will be updated to accommodate the submission of the results, and will support the data entry for Core Metrics in July. Additionally, Cyberscope will provide supplementary fields to allow the IG to provide additional comments to the Core Metrics submission. IGs may use these fields to provide additional data supporting the Core Metrics evaluation results, and will ultimately provide their determination of effectiveness within the platform.

Extension requests can be submitted to the OFCIO Mailbox (ofcio@omb.eop.gov). Extension requests will be evaluated based on unique requirements presented by the agency IG.

Core IG Metrics Working Group

A working group will be chartered by June 30, 2022 to support the future of the Core IG Metrics process. The working group will be co-led by designees identified by OMB and CIGIE respectively. Working group membership will be comprised of representatives from CIGIE, FCEB, OMB, the IC, and others deemed appropriate by OMB and CIGIE. The group will focus on evaluating the Core and supplemental metrics, providing recommendations to the IG Community that align and harmonize evaluation practices, improve reporting processes, and reduce burden where practicable and mutually beneficial. By establishing this working group, we hope to ensure that evolving cybersecurity needs and practices are reflected in future metrics. This includes evaluation of the effectiveness rating methodology, and areas of potential enhancement.[2] Additional details will be shared with the IG Community about the working group proposal as it is developed.

Summary

OMB and the IG have a unique, parallel relationship in providing oversight of agencies' cybersecurity practices—ultimately improving the efficacy of our government services. It is our strong belief that building a foundation for greater information sharing and common evaluative toolsets among our offices will have exponential benefits.

Determining effectiveness is a complex activity that involves both common data points paired with environment-specific context. Focusing on these Core Metrics, IGs will be able to coalesce the most important data points and focus on outcomes that best posture agencies for successful security programs. IG-led supplemental data and analysis helps stakeholders obtain an essential perspective on the landscape

---

[2] This action aligns with Recommendation 2 in GAO-22-104364, "OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision."

of security and provide context to these core metrics. These guidelines for the FY22 Core IG Metrics will help facilitate the transition to the vision outlined in M-22-05.

Appendix A: Core IG Metrics

The table below shows the Core IG metrics for use in the FY22 IG evaluation period. These metrics were selected from the FY 21 IG metrics for their applicability to critical efforts emanating from EO 14028 and M-22-05.

Question	Metric	Mapping
1	**FY22 Core Metric:** To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?	NIST SP 800-53, Rev. 5: CA-3 and PM-5; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3; OMB A-130, NIST SP 800-37, Rev. 2: Task P-18; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5); CISA Cybersecurity & Incident Response Playbooks
2	**FY22 Core Metric:** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting ?	NIST SP 800-53, Rev. 5: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; NIST 800-207, 7.3.2; Federal Enterprise Architecture (FEA) Framework, v2; FY 2022 CIO FISMA Metrics: 1.2-1.2.3; CSF: ID.AM-1, ID.AM-5; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 1
3	**FY22 Core Metric:** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?	NIST SP 800-53, Rev. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2
5	**FY22 Core Metric:** To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?	NIST SP 800-39; NIST SP 800-53, Rev. 5: RA-3 and PM-9; NIST IR 8286; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3
10	**FY22 Core Metric:** To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?	NIST SP 800-39; OMB A-123; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response
14	**FY22 Core Metric:** To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements ()?	The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5 and SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276, NIST 800-218, Task PO.1.3; FY 2022 CIO FISMA Metrics: 7.4.2; CIS Top 18 Security Controls v.8: Control 15

20	**FY22 Core Metric:** To what extent does the organization utilize settings/common secure configurations for its information systems?	NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5; NIST SP 800-70, Rev. 4; FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing; EO 14028, Section 4, 6, and 7; OMB M-22-09, Federal Zero Trust Strategy, Section D; OMB M-22-05; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8, Controls 4 and 7; CSF: ID.RA-1 and DE.CM-8
21	**FY22 Core Metric:** To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?	EO 14028, Sections 3 and 4; NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; NIST 800-207, section 2.1; CIS Top 18 Security Controls v.8, Controls 4 and 7; FY 2022 CIO FISMA Metrics: Section 8; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02, 19-02, and 22-01; OMB M-22-09, Federal Zero Trust Strategy, Section D; CISA Cybersecurity Incident and Vulnerability Response Playbooks
30	**FY22 Core Metric:** To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; OMB M-19-17, NIST SP 800-157; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6
31	**FY22 Core Metric:** To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17 and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; DHS ED 19-01; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6
32	**FY22 Core Metric::** To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?	EO 14028, Section 8; FY 2022 CIO FISMA Metrics: 3.1; OMB M-21-31; OMB M-19-17; NIST SP 800-53, Rev. 5: AC-1, AC-2, AC-5, AC-6, AC-17, AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4; CIS Top 18 Security Controls v.8: Controls 5, 6, and 8
36	**FY22 Core Metric:** To what extent has the organization implemented the encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?	EO 14028, Section 3(d); OMB M-22-09, Federal Zero Trust Strategy; NIST 800-207; NIST SP 800-53, Rev. 5; SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6; CIS Top 18 Security Controls v. 8: Control 3
37	**FY22 Core Metric::** To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?	FY 2022 CIO FISMA Metrics, 5.1; NIST SP 800-53, Rev. 5: SI-3, SI-7, SI-4, SC-7, and SC-18; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5, OMB M-21-07; CIS Top 18 Security Controls v.8: Controls 9 and 10
42	**FY22 Core Metric:** To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?	FY 2022 CIO FISMA Metrics, Section 6; NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS Top 18 Security Controls v.8: Control 14
47	**FY22 Core Metric::** To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?	NIST SP 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31; NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6; CIS Top 18 Security Controls v.8: Control 13

49	**FY22 Core Metric:** How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?	OMB A-130; NIST SP 800-137: Section 2.2; NIST SP 800-53, Rev. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03
54	**FY22 Core Metric::** How mature are the organization's processes for incident detection and analysis?	EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17
55	**FY22 Core Metric::** How mature are the organization's processes for incident handling?	EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2
61	**FY22 Core Metric:** To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?	FY 2022 CIO FISMA Metrics: 10.1.4; NIST SP 800-53, Rev. 5: CP-2, and RA-9; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; CSF:ID.RA-4
63	**FY22 Core Metric:** To what extent does the organization perform tests/exercises of its information system contingency planning processes?	FY 2022 CIO FISMA Metrics: 10.1; NIST SP 800-34; NIST SP 800-53, Rev. 5: CP-3 and CP-4; CSF: ID.SC-5 and CSF: PR.IP-10; CIS Top 18 Security Controls v.8: Control 11