OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

MCC Implemented a Managed and Measurable Information Security Program for Fiscal Year 2022 in Support of FISMA

AUDIT REPORT A-MCC-22-006-C
September 1, 2022

Information Technology Audits Division

OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

MEMORANDUM

DATE: September 1, 2022

TO: MCC, Chief Information Officer and Chief Privacy Officer, Christopher E. Ice

FROM: Deputy Assistant Inspector General for Audit, Alvin A. Brown /s/

SUBJECT: MCC Implemented a Managed and Measurable Information Security Program for Fiscal Year 2022 in Support of FISMA (A-MCC-22-006-C)

Enclosed is the final audit report on the Millennium Challenge Corporation's (MCC) information security program for fiscal year 2022, in support of the Federal Information Security Modernization Act of 2014 (FISMA). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of RMA Associates LLC (RMA) to conduct the audit. The contract required RMA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed RMA's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on MCC's compliance with FISMA. RMA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which RMA did not comply, in all material respects, with applicable standards.

The audit objective was to determine the maturity level MCC achieved for each of its core FISMA reporting metrics.[1] Therefore, it was not designed to develop causes of, effects of, or make recommendations to improve the maturity levels.

To answer the audit objective, RMA assessed the effectiveness of MCC's implementation of the 20 core metrics. The scope of this audit was to assess whether MCC's information security program was consistent with reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security.[2] The audit included tests of management, technical, and operational controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations.* RMA reviewed four of eight judgmentally selected systems in MCC's inventory dated February 14, 2022. Audit fieldwork

[1] For this audit, "core metrics" were defined as the FY2022 inspector general FISMA reporting metrics issued by the Office of Management and Budget, Office of the Federal Chief Information Officer, "FY22 Core IG Metrics Implementation Analysis and Guidelines," April 13, 2022.
[2] "FY 2022 Core IG FISMA Metrics Evaluation Guide."

covered MCC's headquarters located in Washington, DC, from March 21, 2022, to July 11, 2022. It covered the period from March 22, 2022, through July 11, 2022.

RMA found that, for the 20 core metrics, MCC's information security program was defined for 4 metrics, consistently implemented for 2 metrics, and managed and measurable for 14 metrics. Therefore, MCC's information security program was calculated as managed and measurable.

MCC concurred with the report's conclusions and deemed it helpful in validating the agency's compliance with FISMA. The report does not include recommendations.

We appreciate the assistance provided to our staff and the audit firm's employees during the engagement.

RMA | Associates

Auditors. Consultants. Advisors.

Millennium Challenge Corporation (MCC)

Federal Information Security Modernization Act of 2014 (FISMA)

Final Report
Fiscal Year 2022

RMA | Associates
Auditors. Consultants. Advisors.

September 1, 2022

Ms. Lisa Banks
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20005-2221

Dear Ms. Banks:

RMA Associates, LLC, is pleased to present our final report on the Millennium Challenge Corporation's (MCC) compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022.

Thank you for the opportunity to serve your organization and the assistance provided by your staff and that of MCC. We will be happy to answer any questions you may have concerning the report.

Respectfully,

Reza Mahbod

Reza Mahbod, CPA, CISA, CFE, CGFM, CICA, CGMA, CDFM, CDPSE
President
RMA Associates, LLC

Table of Contents

RMA | Associates
Auditors. Consultants. Advisors.

Inspector General
United States Agency for International Development
Washington, D.C.

September 1, 2022

RMA Associates, LLC, conducted a performance audit of the Millennium Challenge Corporation's (MCC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine what maturity level did MCC achieve for each of its core FISMA reporting metrics. The scope of this audit was to assess whether MCC's information security program was consistent with reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security. The audit included tests of management, technical, and operational controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, updated December 10, 2020.

For this audit, we reviewed four of eight judgmentally selected systems in MCC's inventory as of February 14, 2022. Audit fieldwork covered MCC's headquarters located in Washington, D.C., from March 21, 2022, to July 11, 2022.

Our audit was performed in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. RMA found that, for the 20 core metrics, MCC's information security program was Defined for 4 metrics; Consistently Implemented for 2 metrics; and Managed and Measurable for 14 metrics.

Respectfully,

RMA Associates

RMA Associates, LLC
Arlington, VA

Summary of Results

Background

The United States Agency for International Development's Office of Inspector General engaged RMA Associates, LLC, (RMA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an evaluation of the Millennium Challenge Corporation's (MCC) information security program for fiscal year (FY) 2022. The objective of this performance audit was to answer the following question:

> What maturity level did MCC achieve for each of its core FISMA reporting metrics?[2]

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting federal operations and assets. FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other sources.

The statute also provides a mechanism for improved oversight of federal agency information security programs. FISMA requires agency heads to ensure (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes.

FISMA also requires the agency Inspectors General (IGs) to assess their agency's information security programs and practices and report the results of the assessments to the Office of Management and Budget (OMB).

Annually, OMB and the Department of Homeland Security (DHS) provide instructions to Federal agencies and IGs for assessing agency information security programs. On December 6, 2021, OMB issued OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements."* According to that memorandum, each year, IGs are required to complete metrics[3] to independently assess their agencies' information security programs.

The FY 2022 metrics are designed to assess the maturity of an information security program. The five maturity levels are: Level 1 – Ad hoc; Level 2 – Defined; Level 3 – Consistently Implemented; Level 4 – Managed and Measurable; and Level 5 – Optimized. (See Table 1 for definitions of each level.)

---

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] For this audit, "core metrics" are defined as the FY 2022 inspector general FISMA reporting metrics.

[3] The IG FISMA metrics will be completed as a separate deliverable.

Table 1: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description*
Level 1: Ad Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner. Achieving this maturity level is not effective.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented. Achieving this maturity level is not effective.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking. Achieving this maturity level is not effective.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes. Achieving this maturity level is effective.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs. Achieving this maturity level is effective.

* "FY 2022 Core IG FISMA Metrics" defines which maturity levels are considered to be effective.

The FY 2022 metrics are designed to assess the maturity of an information security program and align with the five functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 4.0: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 2.

Table 2: Aligning the Cybersecurity Framework Security Functions to the FY 2022 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2022 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

This audit was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions based on our audit objective.

Audit Results

RMA found that, for the 20 core metrics, MCC's information security program was:

- Defined for 4 metrics;
- Consistently Implemented for 2 metrics; and
- Managed and Measurable for 14 metrics.

Therefore, MCC's information security program was calculated by CyberScope[4] as managed and measurable. The following sections discuss the audit results in more detail. See Appendix IV for a summary of results for each core metric.

1. MCC's Implementation of Four Core Metrics Was Defined.

MCC's implementation of its supply chain risk management (metric 14), flaw remediation (metric 21), incident handling (metric 55), and contingency planning testing (metric 63) was defined (level 2). Specifically:

- Criteria for metric 14 states:

  > The organization ensures that its policies, procedures, and processes are consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component.
  >
  > In addition, the organization obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.
  >
  > Furthermore, the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers.

  MCC did not ensure that its policies, procedures, and processes were consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component.

  In addition, MCC did not provide evidence that it obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of MCC meet FISMA requirements, OMB requirements and applicable NIST guidance.

  Furthermore, MCC did not maintain visibility into its upstream suppliers and can consistently track changes in suppliers. Therefore, MCC's implementation of its supply chain risk management (metric 14) was defined (level 2).

- Criteria for metric 21 states:

  > The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days and utilizes lessons learned in implementation to make improvements to its flaw remediation policies and procedures.

[4] CyberScope is the system that agencies use to report FISMA results.

MCC did not patch critical vulnerabilities within 30 days. Therefore, MCC's implementation of its flaw remediation (metric 21) was defined (level 2).

- Criteria for metric 55 states:

  > The organization consistently implements its incident handling policies, procedures, containment strategies, and incident eradication processes. In addition, the organization consistently implements processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.

  MCC did not report incidents in a timely manner to the external parties as stated in its incident handling policies, procedures, containment strategies, and incident eradication processes. Therefore, MCC's implementation of its incident handling (metric 55) was defined (level 2).

- Criteria for metric 63 states:

  > Information system contingency plan testing and exercises are consistently implemented. ISCP [information system contingency plan] testing and exercises are integrated, to the extent practicable, with testing of related plans…

  MCC did not complete contingency planning testing for one of the four judgmentally selected systems. Therefore, MCC's implementation of its contingency planning tests (metric 63) was defined (level 2).

2. MCC's Implementation of Two Core Metrics Was Consistently Implemented.
MCC's implementation of its data exfiltration (metric 37) and workforce assessment (metric 42) was consistently implemented (level 3). Specifically:

- Criteria for metric 37 states:

  > The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware and blocks known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII [personally identifiable information]. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization utilizes email authentication technology and ensures the use of valid encryption certificates for its domains.

MCC did not complete the data exfiltration exercise during the audit period.[5] Therefore, MCC's implementation of its data exfiltration (metric 37) was consistently implemented (level 3).

- Criteria for metric 42 states:

  > The organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.

  MCC did not address the identified knowledge, skills, and abilities gaps through training or talent acquisition. Therefore, MCC's implementation of its workforce assessment (metric 42) was consistently implemented (level 3).

3. MCC's Implementation of 14 Core Metrics Was Managed and Measurable.

MCC's implementation of the following 14 metrics was managed and measurable (level 4): 1-3, 5, 10, 20, 30-32, 36, 47, 49, 54, and 61.

For example, as discussed in the following paragraphs, MCC's implementation of continuous monitoring (metric 47) and contingency planning (metric 61), was managed and measurable.

- Criteria for metric 47 states:

  > The organization's ISCM [information security continuous monitoring] policies and strategy are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs.
  >
  > The organization can demonstrate that it is using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs. MCC monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its ISCM policies and strategy and made updates as appropriate.

  MCC's ISCM policies and strategy are not fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. In addition, MCC did not demonstrate that it is using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs. Therefore, MCC's implementation of metric 47 was managed and measurable (level 4).

- Criteria for metric 61 states:

  > The organization ensures that the results of organizational and system level BIA's [business impact analysis] are integrated with enterprise risk management

[5] MCC is scheduled to complete the exercise in the fourth quarter of FY 2022.

processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets.

As appropriate, the organization utilizes the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.

MCC through its Information System Contingency Planning ensured that the results of organizational and system level BIA's are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. Therefore, MCC's implementation of metric 61 was managed and measurable (level 4), which is the highest maturity level for that metric.

Evaluation of Management Comments

In response to the draft report, MCC said it concurred with the conclusion of the report and deemed the report constructive in helping to validate the agency's compliance with FISMA. MCC's comments are included in their entirety in Appendix III.

Appendix I - Scope and Methodology

Scope

RMA conducted this performance audit in accordance with generally accepted government auditing standards as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objective. The audit was designed to determine the maturity level for the core FISMA metrics. It was not designed to develop causes of, effects of, and recommendations to improve the maturity levels.

The scope of this audit was to assess MCC's information security program consistent with FISMA and reporting instructions issued by OMB and DHS. The audit included tests of management, technical, and operational controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations.* We assessed MCC's performance and compliance with FISMA in the following areas:

- Risk Management
- Supply Chain Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Awareness Training
- Information System Continuous Monitoring
- Incident Response
- Contingency Planning

For this audit, we reviewed four of eight judgmentally selected systems in MCC's inventory as of February 14, 2022. The audit also included a follow-up on two prior audit recommendations associated with the core FISMA metrics to determine if MCC had made progress in implementing the recommended improvements concerning its information security program.[6] See Appendix II for the status of prior year recommendations.

Audit fieldwork covered MCC's headquarters located in Washington D.C., from March 21, 2022, to July 11, 2022. It covered the period from October 1, 2021, through July 11, 2022.

Methodology

To determine the MCC maturity level of the core metrics, RMA conducted interviews with MCC officials and contractors and reviewed the legal and regulatory requirements stipulated in FISMA. Additionally, RMA reviewed documentation supporting the information security program. These documents included, but were not limited to, MCC's (1) risk management policy, (2) configuration management procedures, (3) identity and access control measures, (4) security awareness training, and (5) continuous monitoring

[6] RMA only evaluated recommendation closure that pertained to the core metrics. The remaining recommendations do not affect the core metrics and will be evaluated at a later time.

controls. RMA compared documentation against requirements stipulated in NIST special publications. Also, RMA performed tests of information system controls to determine the maturity levels of those controls. Furthermore, RMA reviewed the status of FISMA audit recommendations from FY 2021.

In assessing the security controls, RMA exercised professional judgment in determining the number of items selected for testing and the method used to select them because the results did not need to be projected to the population. RMA considered the relative risk and the significance of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the proportion of deficient items found compared to the total population available for review when documenting the results of our testing. Lastly, in some instances, RMA tested samples rather than the entire audit population. In those cases, the results cannot be projected to the population as that may be misleading.

Appendix II - Status of Prior Year Findings

The following table provides the status of the FY 2021 FISMA audit recommendations.[7][8]

Table 2: FY 2021 FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2021 Audit Recommendations	MCC's Position	Auditor's Position on the Status
A-MCC-22-004-C (Rec.1)	Develop and implement processes to document and implement lessons learned related to risk management, configuration management, and identity and access management.	Closed	Agree
A-MCC-22-004-C (Rec.2)	Develop and document supply chain policies, procedures, and strategies.	Open	Agree
A-MCC-22-004-C (Rec.3)	Revise and implement MCC's Vulnerability Patch Compliance Policy to align with timeframes in the Department of Homeland Security's Fiscal Year 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.	Closed	Disagree Refer to Audit Results #1, Metric 21
A-MCC-22-004-C (Rec.4)	Develop and implement a process to conduct an independent periodic review of MCC's privacy program.	Open	Will be assessed later
A-MCC-22-004-C (Rec.5)	Fully develop and implement a security awareness training strategy.	Closed	Will be assessed later
A-MCC-22-004-C (Rec.6)	Document and implement a process to monitor and enforce MCC's procedures for security training.	Closed	Will be assessed later
A-MCC-22-004-C (Rec.7)	Document and implement a written process for obtaining and evaluating feedback on MCC's privacy and security training content, including role-based training.	Closed	Will be assessed later

[7] RMA only evaluated recommendation closure that pertained to the core metrics. The remaining recommendations that do not affect the core metrics will be evaluated in FY 2023.
[8] MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA (Audit Report A-MCC-22-004-C, December 2, 2021).

Appendix III – Management Comments

DATE: August 18, 2022

TO: Alvin Brown
Deputy Assistant Inspector General for Audit
Office of Inspector General
United States Agency for International Development
Millennium Challenge Corporation

FROM: Christopher E. Ice /s/
Chief Information Officer and Chief Privacy Officer
Department of Administration and Finance
Millennium Challenge Corporation

SUBJECT: MCC's Management Response to the Draft Report, "MCC Implemented a Managed and Measurable Information Security Program for Fiscal Year 2022 in Support of FISMA," dated August 15, 2022

The Millennium Challenge Corporation (MCC) appreciates the opportunity to review the draft report on the Office of Inspector General (OIG)'s audit, "MCC Implemented a Managed and Measurable Information Security Program for Fiscal Year 2022," dated August 15, 2022. MCC concurs with the conclusion of the report and deemed the report constructive in helping to validate the agency's compliance with FISMA.

There were no recommendations as part of this audit, and as such, MCC does not provide a corrective action plan.

If you have any questions, please contact me at 202-521-2652 or Icece@mcc.gov. Additionally, you can also contact Jude Koval, Senior Director of Internal Controls and Audit Compliance (ICAC), at 202-521-7280 or Kovaljg@mcc.gov.

CC: Lisa Banks, Director, Information Technology Audits Division, OIG, USAID
Fouad Saad, Vice President and Chief Financial Officer, A&F, MCC
Adam Bethon, Deputy Chief Financial Officer, FMD, A&F, MCC
Lori Giblin, Chief Risk Officer, ARC, A&F, MCC
Miguel Adams, Chief Information Security Officer, OCIO, A&F, MCC
Jude Koval, Senior Director, ARC, A&F, MCC

Appendix IV – Summary Results of Each Metric

Metric	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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?				☒	
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?				☒	
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?				☒	
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?				☒	
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?				☒	

Metric	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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?		☒			
20. FY22 Core Metric: To what extent does the organization utilize settings/common secure configurations for its information systems?				☒	
21. FY22 Core Metric: To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?		☒			
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 nonprivileged users to access the organization's facilities [organization defined entry/exit points], networks, and systems, including for remote access?				☒	
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?				☒	

Metric	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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?				☒	
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?				☒	
37. FY22 Core Metric: To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?			☒		
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?			☒		
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?				☒	

Metric	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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?				☒	
54. FY22 Core Metric: How mature are the organization's processes for incident detection and analysis?				☒	
55. FY22 Core Metric: How mature are the organization's processes for incident handling?		☒			
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?				☒	
63. FY22 Core Metric: To what extent does the organization perform tests/exercises of its information system contingency planning processes?		☒			
Total	**0**	**4**	**2**	**14**	**0**