Peace Corps Office of
INSPECTOR GENERAL

Special Report
Review of the Peace Corps' Information Security Program

IG-26-01-SR
December 2025

WILLIAMS ADLEY

CONTENTS

Results in Brief **1**

Background **3**

The Peace Corps 3

Federal Information Security Modernization Act of 2014 (FISMA) 3

FISMA Reporting Metrics 3

Maturity Model and Scoring Methodology 5

Results of the Fiscal Year 2025 FISMA Review **7**

I. Govern 7

Cybersecurity Governance – Core Reporting Metrics 7

Cybersecurity Governance – Supplemental Reporting Metrics 7

Cybersecurity Supply Chain Risk Management – Core Reporting Metrics 8

Cybersecurity Supply Chain Risk Management – Supplemental Reporting Metrics 8

II. Identify 8

Risk and Asset Management – Core Reporting Metrics 8

Risk and Asset Management – Supplemental Reporting Metric 9

III. Protect 10

Configuration Management – Core Reporting Metrics 10

Configuration Management – Supplemental Reporting Metrics 11

Identity and Access Management – Core Reporting Metrics 11

Identity and Access Management – Supplemental Reporting Metrics 12

Data Protection and Privacy – Core Reporting Metrics 12

Data Protection and Privacy – Supplemental Reporting Metrics 12

Security Training – Core Reporting Metrics 12

Security Training – Supplemental Reporting Metrics 13

IV. Detect 13

Information Security Continuous Monitoring – Core Reporting Metrics 13

Information Security Continuous Monitoring – Supplemental Reporting Metric 14

V. Respond 14

Incident Response – Core Reporting Metrics 14

Incident Response – Supplemental Reporting Metrics 15

VI. Recover 15

Contingency Planning – Core Reporting Metrics 15

Contingency Planning – Supplemental Reporting Metrics 16

Conclusion 16

Appendix A – Objective, Scope, and Methodology **18**

Appendix B – Status of Prior Years' Recommendations **19**

Appendix C – Agency Comments **20**

Appendix D – OIG's Response **24**

RESULTS IN BRIEF

The objective of this Federal Information Security Modernization Act of 2014 (FISMA) review was to determine the effectiveness of the Peace Corps' information security program and practices based on the fiscal year (FY) 2025 Inspector General (IG) FISMA Reporting Metrics v2.0,[1] which are categorized into 6 functional areas and 10 associated domains. The review also evaluated the Peace Corps' efforts in addressing previously issued exceptions and recommendations.

Since FY 2024, the Peace Corps has continued to make progress in enhancing its information security posture and closed five recommendations from previous reports. The Peace Corps exhibited a strong commitment to meeting the FISMA requirements by improving its maturity ratings for three FISMA domains: Identity and Access Management; Information Security Continuous Monitoring; and Incident Response.

However, for FY 2025 the Peace Corps' information security program remained at Level 2 – Defined, falling short of Level 4 – Managed and Measurable, which the Office of Management and Budget (OMB) considers to be the effective level of security at the domain, function, and overall program level. Furthermore, the Peace Corps needs to address six new exceptions[2], four prior exceptions, three prior recommendations, and five new recommendations issued during this review.

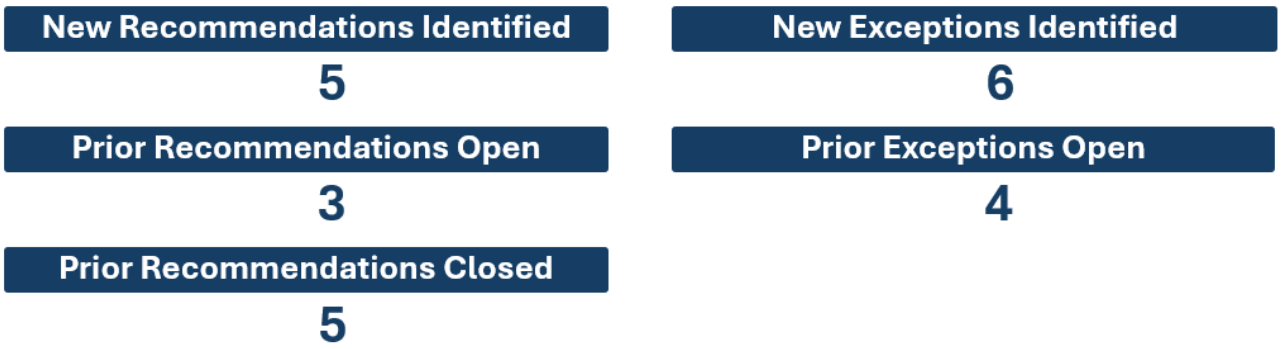

Figure 1: FY 2025 Peace Corps Information Technology Security Posture Summary
Source: as determined by Williams Adley, & Company-DC, LLP

[1] FY 2025 IG FISMA Reporting Metrics v2.0.
[2] An exception is a deviation from established policies, procedures, or control requirements identified during audit testing.

The following figures provide information on the results of the FY 2025 FISMA review. Specifically, Figure 2 provides an overview of the overall maturity ratings at both the function and domain levels.

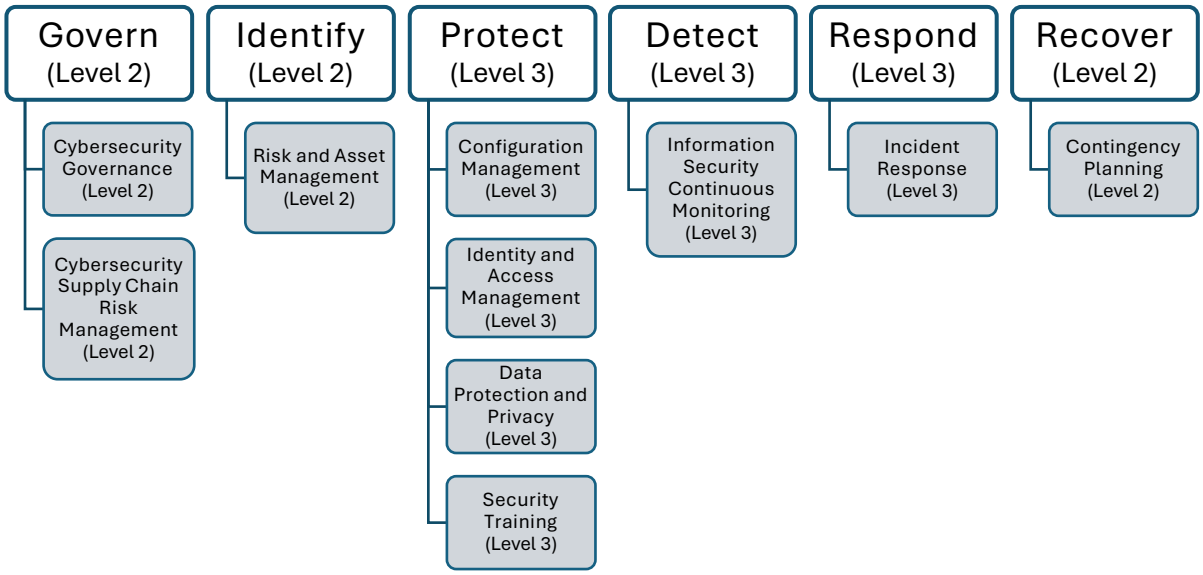

Figure 2: FY 2025 FISMA Function and Domain Maturity Ratings
SOURCE: as determined by Williams Adley, & Company-DC, LLP and documented in the FY 2025 IG FISMA Reporting Metrics

Figure 3 represents the results from a core and supplemental metric perspective. Additional details on the calculation of each domain's maturity rating are provided within the body of this report.

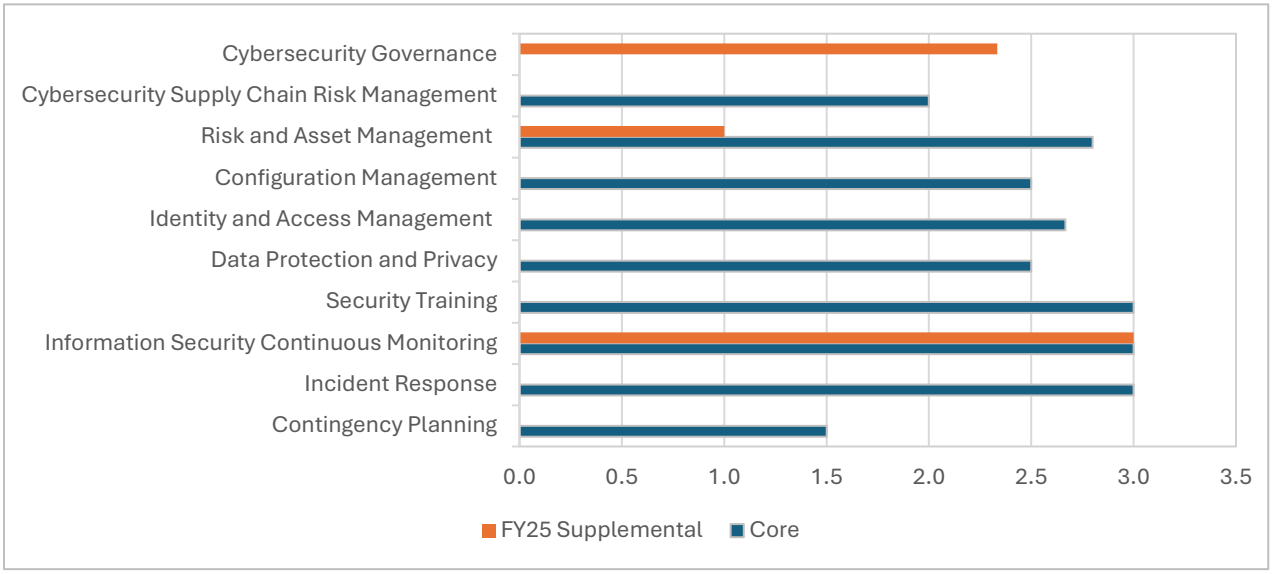

Figure 3: Calculated Average Maturity Rating of the Core and Supplemental Metrics by Domain
Source: as determined by Williams Adley, & Company-DC, LLP

A copy of the Peace Corps management's response to the results of the FY 2025 FISMA review is included in **Appendix C**.

BACKGROUND

THE PEACE CORPS

The Peace Corps is an independent Federal agency that was established in March 1961. The Peace Corps' mission is to promote world peace and friendship through community-based development and intercultural understanding. Peace Corps Volunteers and community partners advance this mission by fulfilling three goals: (1) to help people of interested countries meet their needs for trained Volunteers; (2) to promote a better understanding of Americans on the part of the people served; and (3) to promote a better understanding of other people on the part of Americans.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 (FISMA)

FISMA requires each Federal agency to protect the information and information systems that support its operations, including those provided or managed by other agencies, entities, or contractors. FISMA also established the oversight authority of the Director of OMB for agency information security policies and practices and provided the Department of Homeland Security (DHS) Secretary with the authority to administer the implementation of such policies and practices.

FISMA provides several modifications that modernize Federal security practices to address evolving security concerns. These changes have streamlined the annual compliance report, strengthened the use of continuous monitoring, placed greater responsibility on agencies for ensuring compliance, and shifted reporting to focus more on the causes and impacts of security incidents. In addition, OMB regulations require Federal agencies to ensure that the appropriate officials are assigned security responsibilities and periodically review their information systems' security controls. Specifically, the agency's Chief Information Officer (CIO) is required to designate a senior information security officer to implement an agency information security program. Each agency must establish a risk-based information security program that ensures information security is practiced throughout the life cycle of each agency's systems.

FISMA also requires each agency's information security program to be evaluated on the effectiveness of its policies, procedures, and practices, which must be annually reported to OMB, DHS, Congress, and the Government Accountability Office. Each Office of Inspector General (OIG), or independent external auditor, as determined by the IG, must also conduct an independent annual assessment of its agency's information security program and report its findings to OMB within defined timelines. The Peace Corps OIG contracted with the Independent Public Accounting firm Williams Adley, & Company-DC, LLP (Williams Adley) to complete the FY 2025 IG FISMA assessment of the Peace Corps' information security program.

FISMA REPORTING METRICS

Williams Adley used the FY 2025 IG FISMA metrics published by OMB, in consultation with the Council of the Inspectors General on Integrity and Efficiency (CIGIE), to evaluate the effectiveness of the Peace Corps' information security program. The FISMA reporting metrics are organized around six security functions: *Govern, Identify, Protect, Detect, Respond*, and *Recover*. The requirements and definitions for the six functions are outlined in the National Institute of Standards

and Technology's (NIST) Cybersecurity Framework (CSF).[3] Within the 6 functions, there are 10 associated domains. For each domain, Williams Adley reviewed a combination of entity-wide and system-specific controls, with a focus on the main information system that supports the Peace Corps' mission. Refer to Appendix A of this report for more information on the scope of the FY 2025 FISMA review of the Peace Corps.

On January 15, 2025, OMB issued the Memorandum for the Heads of Executive Departments and Agencies: FY 2025 Guidance on Federal Information Security and Privacy Management Requirements (Memorandum M-25-04) to provide instructions for meeting the FISMA reporting requirements. Additionally, the IG FISMA reporting metrics were updated to determine the agency's progress in the following areas:

- NIST CSF 2.0. NIST published CSF 2.0, which highlights the critical role that governance plays in managing cybersecurity risks and incorporates cybersecurity into an organization's broader Enterprise Risk Management (ERM) strategy. Subsequently, a new IG FISMA function (*Govern*) was created, which includes a new domain (Cybersecurity Governance). In addition, new supplemental metrics were designed to assess the maturity of an organization's:
    - Cybersecurity profiles that are used to understand, tailor, assess, prioritize, and communicate cybersecurity objectives.
    - Cybersecurity risk management strategy, which establishes an organization's priorities, constraints, risk tolerance and appetite statements, and is used to support operational risk decisions.
    - Processes and authorities to foster cybersecurity accountability, performance assessment, and continuous improvement.

  In addition, to align with CSF 2.0, the supply chain risk management (SCRM) domain moved from the *Identify* function to the *Govern* function and was renamed to Cybersecurity SCRM (C-SCRM) to better reflect the current cybersecurity environment. Furthermore, the Risk Management domain in the *Identify* security function was renamed "Risk and Asset Management" to group the metrics related to system and component inventories and data management.
- Zero Trust Architecture (ZTA) Implementation. The FY 2025 IG FISMA metrics included two new supplemental metrics that are critical for achieving the ZTA objectives. These new metrics assess the maturity of an organization's data management capabilities and its ability to monitor and measure the integrity and security posture of all owned and associated assets.[4]
- Supplemental metrics for FY 2025. The five supplemental metrics listed below were included in the FY 2025 IG FISMA review.
    - To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives?

[3] NIST.CSWP.29.pdf

[4] For the FY 2026 IG FISMA review cycle, OMB and CIGIE will consider including additional core or supplemental metrics that focus on measuring the maturity of agencies' implementation of ZTA, as necessary.

- To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?
- To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessments, and continuous improvement?
- To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate, throughout the data lifecycle?
- To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?

- Information System Level Risk Management. The core metric on information system level risk management (Metric 11; formerly Metric 5) was revised to focus on the maturity of agencies' implementation of the NIST risk management framework.

MATURITY MODEL AND SCORING METHODOLOGY

OMB published the FY 2025 IG FISMA Reporting Metrics to provide guidance to agency IGs, or independent assessors, on how to determine the maturity of their agency's information security program. According to the reporting metrics, "OMB believes that achieving a Level 4 (Managed and Measurable) or above represents an effective level of security." See Table 1 below for the definition of each maturity level.

Table 1: IG Evaluation Maturity Level Descriptions

Maturity Level		Description
Level 1	Ad-Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2	Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3	Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
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.
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.

Source: FY 2025 IG FISMA Reporting Metrics

Additionally, the guidelines instruct IGs and independent auditors to use "a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (govern, identify, protect, detect, respond, and recover) and the overall program." As part of this approach, core metrics and supplemental metrics were averaged independently to determine each domain's maturity calculation and provide data for the assessed program and function effectiveness.

IGs and independent auditors were also instructed that calculated averages will not be automatically rounded to a particular maturity level. Instead, the determination of maturity levels and the overall effectiveness of the agency's information security program should focus on the results of the core metrics and the calculated averages of the supplemental metrics as data points to support their risk-based determination of overall program and function level effectiveness.

RESULTS OF THE FISCAL YEAR 2025 FISMA REVIEW

Williams Adley assessed the effectiveness of the Peace Corps' information security program and practices on a maturity model with levels ranging from one to five. The foundational levels (Levels 1-2) ensure that policies and procedures are designed to support the requirements outlined within FISMA. The advanced levels (Levels 3-5) focus on the implementation, operational effectiveness, and continuous improvement of the defined policies and procedures. The following sections outline the results of the FY 2025 IG FISMA review for all 6 FISMA functions and their 10 corresponding domains. Metric numbers in the tables below may not be sequential in order.[5]

I. GOVERN

The *Govern* function is supported by the cybersecurity governance and the cybersecurity supply chain risk management (C-SCRM) domains. The Peace Corps' *Govern* function has an overall maturity rating of Level 2 – Defined.

Cybersecurity Governance – Core Reporting Metrics

OMB did not identify any core reporting metrics for evaluation in FY 2025.

Cybersecurity Governance – Supplemental Reporting Metrics

OMB identified three supplemental reporting metrics for evaluation in FY 2025, as outlined in Table 2 below.

Table 2: Ratings for Supplemental Metrics with the Cybersecurity Governance Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
1	Organizational context and cybersecurity profiles.	N/A	Level 1
2	Cybersecurity risk management strategy.	N/A	Level 3
3	Cybersecurity roles, responsibilities, and authorities.	N/A	Level 3

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that while the Peace Corps had visibility into the current state of its security program, it lacked a clearly defined goal for the security program and the associated steps needed to achieve it. The agency did not have formal policies or procedures for establishing or maintaining its cybersecurity profiles. The agency plans to adapt its existing cybersecurity profile to the NIST CSF 2.0 template (Metric 1). To reach compliance as a Level 2 – Defined program and transition to Level 3 – Consistently Implemented, the Peace Corps needs to develop and implement formal policies on its cybersecurity profile (Metric 1).

The Peace Corps did, however, consistently implement its risk management strategy across the organizational, mission process, and system levels. The Office of the Chief Information Officer (OCIO) held monthly check-ins with the Compliance and Risk Office, quarterly system-level risk

[5] The metric numbering in the tables may not be sequential in this report as there are metric numbers assigned to provide additional narrative information. For example, Metric 4 is to provide additional narrative information on the effectiveness of the organization's cybersecurity governance program and therefore does not have a rating.

assessments, and regular maintenance of an agency-level risk register and function-level risk registers (Metric 2).

In addition, the Peace Corps established and communicated the necessary roles, responsibilities, and authorities to support cybersecurity risk management activities across the enterprise. These defined roles and responsibilities were also incorporated into individual performance evaluations (Metric 3).

Based on the ratings outlined in Table 2 above, Williams Adley determined that the cybersecurity governance supplemental metrics have a calculated average score of 2.33 and a maturity rating of Level 2 – Defined.

Cybersecurity Supply Chain Risk Management – Core Reporting Metrics

OMB identified one core reporting metric for the development of a C-SCRM program in FY 2025, as outlined in Table 3.

Table 3: Ratings for Core Metrics within the C-SCRM Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
5	Identification, assessment, and management of cybersecurity supply chain risk.	Level 2	Level 2

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps has finalized its cybersecurity supply chain risk management strategy. However, the agency had not implemented processes to ensure that the products, system components, systems, and services obtained from external providers meet its cybersecurity and supply chain risk management requirements. The agency has been working to integrate its strategy into ongoing contract operations, in coordination with the Office of the Chief Financial Officer/Acquisitions and Contract Management (Metric 5).

Based on the ratings outlined in Table 3 above, Williams Adley determined that the C-SCRM core metric has a calculated average score of 2.00 and a maturity rating of Level 2 – Defined.

Cybersecurity Supply Chain Risk Management – Supplemental Reporting Metrics

OMB did not identify any supplemental reporting metrics for evaluation in FY 2025.

II. *IDENTIFY*

The *Identify* function is supported by the Risk and Asset Management (RAM) domain. The Peace Corps' *Identify* function has an overall maturity rating of Level 2 – Defined.

Risk and Asset Management – Core Reporting Metrics

OMB identified five core reporting metrics for the development of a RAM program in FY 2025, as outlined in Table 4.

Table 4: Ratings for Core Metrics within the RAM Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
7	Comprehensive and accurate inventory of information systems.	Level 3	Level 3
8	An up-to-date inventory of hardware assets.	Level 3	Level 3
9	An up-to-date inventory of software and associated licenses.	Level 3	Level 3
11	Information system security risks are adequately managed at all organization tiers.	Level 3	Level 3
12	Use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities.	Level 2	Level 2

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps has continued to use the Cybersecurity Assessment and Management (CSAM) tool to document and maintain its system inventory (Metric 7). The Peace Corps developed a comprehensive asset management program across the network environment by using Axonius, a system that aggregates data from multiple sources to provide visibility into all connected hardware and software assets. This integration ensures an accurate and up-to-date inventory of information system components is maintained (Metric 8 and 9). The data collected by Axonius is transferred into CSAM, which feeds into the Power Business Intelligence tool, creating both enterprise-level and system-level security risk dashboards. These dashboards are periodically presented to the CIO and authorizing official to support risk-informed decision-making and continuous monitoring. Further, the agency conducted its annual review of risk appetite and risk tolerance and continued to hold quarterly ERM meetings, further maturing its ERM implementation (Metric 11).

However, Williams Adley confirmed that the Peace Corps does not use technology or automation to provide a centralized, enterprise-wide view of cybersecurity risk management activities (Metric 12).

Based on the ratings outlined in Table 4 above, Williams Adley determined that the RAM core metrics have a calculated average score of 2.80 and a maturity rating of Level 3 – Consistently Implemented.

Risk and Asset Management – Supplemental Reporting Metric

OMB identified one supplemental reporting metric for evaluation in FY 2025, as outlined in Table 5.

Table 5: Ratings for Supplemental Metrics within the RAM Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
10	Inventories of data and metadata maintained throughout data lifecycle.	N/A	Level 1

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps had not established formal policies and procedures to develop and maintain a comprehensive inventory of its data and corresponding metadata (Metric 10). However, the agency initiated a data maturity roadmap to guide the development of a more robust data governance framework. To reach compliance as a Level 2 – Defined program and transition to Level 3 – Consistently Implemented, the Peace Corps needs to develop and implement formal policies and procedures related to maintaining a comprehensive inventory of its data and metadata (Metric 10).

Based on the ratings outlined in Table 5 above, Williams Adley determined that the RAM supplemental metric has a calculated average score of 1.00 and a maturity rating of Level 1 – Ad-Hoc.

III. PROTECT

The *Protect* function is supported by the Configuration Management (CM), Identity and Access Management (IDAM), Data Protection and Privacy (DPP), and Security Training (ST) domains. The Peace Corps' *Protect* function has an overall maturity rating of Level 3 – Consistently Implemented.

Configuration Management – Core Reporting Metrics

OMB identified two core reporting metrics for the development of a CM program in FY 2025, as outlined in Table 6.

Table 6: Ratings for Core Metrics within the CM Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
14	Use of configuration settings and common secure configurations.	Level 2	Level 2
15	Use of flaw remediation processes.	Level 3	Level 3

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps has updated its existing baseline standard operating procedures to reflect its recent process improvements. Additionally, the agency has been working on two ongoing projects that will review and update the Peace Corps General Support System (PCGSS) baseline configurations to align with the Center for Internet Security Benchmarks and Security Technical Implementation Guides. However, despite these efforts, the Peace Corps did not perform its annual review and update of the PCGSS or the Peace Corps Medical Electronic Documentation and Inventory Control System baseline configurations and associated deviations (Metric 14).

The Peace Corps continued to identify, assess, and remediate vulnerabilities across its information technology environment using automated tools. The agency has consistently implemented a Plan of Action and Milestones process to address outstanding critical and high vulnerabilities that have not been addressed within the required timeframes (Metric 15).

Based on the ratings outlined in Table 6 above, Williams Adley determined that the CM core metrics have a calculated average score of 2.50 and a maturity rating of Level 3 – Consistently Implemented.

Configuration Management – Supplemental Reporting Metrics

OMB did not identify any supplemental reporting metrics for evaluation in FY 2025.

Identity and Access Management – Core Reporting Metrics

OMB identified three core reporting metrics for the development of an IDAM program in FY 2025, as outlined in Table 7.

Table 7: Ratings for Core Metrics within the IDAM Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
17	Use of strong authentication mechanisms (Personal Identity Verification [PIV] or an Identity Assurance Level [IAL]3/Authenticator Assurance Level [AAL]3 credential) for non-privileged users.	Level 3	Level 3
18	Use of strong authentication mechanisms (PIV or an IAL3/AAL3 credential) for privileged users.	Level 3	Level 3
19	Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties.	Level 2	Level 2

SOURCE: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that privileged and non-privileged users utilized PIV cards at headquarters and international posts to authenticate against Peace Corps' systems[6] (Metrics 17 and 18). Additionally, Williams Adley found that privileged users used PIV authentication to make changes to domain name services records.[7]

Williams Adley also determined that the Peace Corps had defined processes for assigning, managing, and reviewing privileged accounts (Metric 19). The agency formalized its Identity, Credential, and Access Management (ICAM) policy in November 2024, establishing a governance framework that includes the creation of an ICAM Program Management Office, the development of ICAM architecture, and the acquisition of ICAM capabilities and services. However, the agency has not finalized an enterprise-wide strategy to guide the program's implementation. The OCIO and Office of Safety and Security plan to prioritize the completion of this strategy in FY 2026, with a focus on identifying and documenting the specific processes that bridge physical and digital security.

Based on the ratings outlined in Table 7 above, Williams Adley determined that the IDAM core metrics have a calculated average score of 2.67 and a maturity rating of Level 3 – Consistently Implemented.

[6] The PIV system is designed to meet the control and security objectives of DHS Presidential Directive-12, which require initial identity proofing, infrastructure to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials.

[7] In response to attackers redirecting and intercepting web and mail traffic, DHS issued Emergency Directive 19-01 to require agencies to implement multi-factor authentication to domain name service accounts. This requirement is reflected in the Level 4 – Managed and Measurable maturity description for Metric 18.

Identity and Access Management – Supplemental Reporting Metrics

OMB did not identify any supplemental reporting metrics for evaluation in FY 2025.

Data Protection and Privacy – Core Reporting Metrics

OMB identified two core reporting metrics for the development of a DPP program in FY 2025, as outlined in Table 8.

Table 8: Ratings for Core Metrics within the DPP Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
21	Use of security controls to protect the confidentiality, integrity, and availability of its Personal Identifiable Information and other agency sensitive data.	Level 3	Level 3
22	Use of security controls to prevent data exfiltration and enhance network defenses.	Level 2	Level 2

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps implemented its data protection controls, including safeguards for data at rest or in transit, untrusted removable media, and media reuse or destruction. The agency uses Secure Shell Layer/Transport Layer Security encryption for external communication and Advanced Encryption Standard 256-bit encryption for data storage. Additionally, CrowdStrike Falcon Complete is a tool that the agency used to detect and block suspicious or untrusted removable media (Metric 21).

Williams Adley also determined that the Peace Corps continued to leverage its Endpoint Detection and Response (EDR) tool to monitor endpoints for suspicious activities and collect behavior-based analytics that support the detection and investigation of potential security incidents. However, the agency is still in the process of procuring and implementing a Data Loss Prevention solution (Metric 22).

Based on the ratings outlined in Table 8 above, Williams Adley determined that the DPP core metrics have a calculated average score of 2.50 and a maturity rating of Level 3 – Consistently Implemented.

Data Protection and Privacy – Supplemental Reporting Metrics

OMB did not identify any supplemental reporting metrics for evaluation in FY 2025.

Security Training – Core Reporting Metrics

OMB identified one core reporting metric for the development of a ST program in FY 2025, as outlined in Table 9.

Table 9: Ratings for Core Metrics within the ST Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
24	Assessment of workforce capabilities to deliver specialized security training.	Level 3	Level 3

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps assessed the knowledge, skills, and abilities of its workforce, tailored its cybersecurity awareness and specialized training accordingly, and identified existing skill gaps. Furthermore, the agency developed and has been actively implementing Plans of Action and Milestones to remediate those gaps (Metric 24).

Based on the rating outlined in Table 9 above, Williams Adley determined that the ST core metric has a calculated average score of 3.00 and a maturity rating of Level 3 – Consistently Implemented.

Security Training – Supplemental Reporting Metrics

OMB did not identify any supplemental reporting metrics for evaluation in FY 2025.

IV. DETECT

The *Detect* function is supported by the Information Security Continuous Monitoring (ISCM) domain. The Peace Corps' *Detect* function has an overall maturity rating of Level 3 – Consistently Implemented.

Information Security Continuous Monitoring – Core Reporting Metrics

OMB identified two core reporting metrics for the development of an ISCM program in FY 2025, as outlined in Table 10.

Table 10: Ratings for Core Metrics within the ISCM Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
26	Use of ISCM policies and strategy that addresses ISCM requirements and activities at each organizational tier.	Level 2	Level 3
28	Ongoing system assessments and monitoring for continuous authorization.	Level 2	Level 3

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps implemented the ISCM policies and strategy at the organization, business process, and information system levels. This implementation highlights the agency's effort in integrating cybersecurity risks into the agency's enterprise risk management program (Metric 26).

Williams Adley determined that the Peace Corps has maintained continuous monitoring of its information systems through defined processes, including monthly risk posture briefings and annual security control assessments. The monthly briefings cover enterprise risk trends, FISMA systems assessment status, and system-specific risk posture, such as overdue vulnerabilities and delayed

Plans of Action and Milestones. Additionally, the status and trends of those Plans of Action and Milestones are tracked in both enterprise-level and system-level security risk dashboards, which are exported and incorporated into quarterly risk assessment reports to support informed, risk-based decision-making (Metric 28).

Based on the ratings outlined in Table 10 above, Williams Adley determined that the ISCM core metrics have a calculated average score of 3.00 and a maturity rating of Level 3 – Consistently Implemented.

Information Security Continuous Monitoring – Supplemental Reporting Metric

OMB identified one supplemental reporting metric for evaluation in FY 2025, as outlined in Table 11.

Table 11: Rating for Supplemental Metric within the ISMC Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
27	Monitoring and measurement of integrity and security posture of all owned and associated assets.	N/A	3

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps continuously collected asset and risk data through its technology stack, including the Security Information and Event Management (SIEM) and EDR tools. The agency implemented correlation searches, dashboards, and automated alerts to analyze security events across multiple data sources, ensuring comprehensive visibility into potentially adverse events and anomalies. When an asset shows signs of compromise, the agency leverages CrowdStrike Falcon's host management feature to block all network traffic and isolate the device (Metric 27).

Based on the ratings outlined in Table 11 above, Williams Adley determined that the ISCM supplemental metric has a calculated average score of 3.00 and a maturity rating of Level 3 – Consistently Implemented.

V. *RESPOND*

The *Respond* function is supported by the Incident Response (IR) domain. The *Respond* function has an overall maturity rating of Level 3 – Consistently Implemented.

Incident Response – Core Reporting Metrics

OMB identified two core reporting metrics for the development of an IR program in FY 2025, as outlined in Table 12.

Table 12: Ratings for Core Metrics within the IR Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
30	Processes for incident detection and analysis.	Level 2	Level 3
31	Processes for incident handling.	Level 2	Level 3

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps had made progress in strengthening its ability to detect and respond to potential threats by integrating its SIEM system with multiple security tools and applications. This integration aggregates logs from key sources – including Palo Alto firewalls, Cisco Firepower, Corelight, Windows and Linux servers, Infoblox, and various cloud service providers – to enable real-time correlation and alerts across the environment (Metrics 30 and 31). However, the agency has not yet met the event logging requirements for Event Logging Maturity Level 2 - Defined, in accordance with OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.[8]

Based on the ratings outlined in Table 12 above, Williams Adley determined that the IR core metrics have a calculated average score of 3.00 and a maturity rating of Level 3 – Consistently Implemented.

Incident Response – Supplemental Reporting Metrics

OMB did not identify any supplemental reporting metrics for evaluation in FY 2025.

VI. RECOVER

The *Recover* function is supported by the Contingency Planning (CP) domain. The Peace Corps' *Recover* function has an overall maturity rating of Level 2 – Defined.

Contingency Planning – Core Reporting Metrics

OMB identified two core reporting metrics for the development of a CP program in FY 2025, as outlined in Table 13:

Table 13: Ratings for Core Metrics within the CP Domain

Metric	Topic	FY 2024 Rating	FY 2025 Rating
33	Use of Business impact analyses (BIA) to guide contingency planning efforts.	Level 1	Level 1
34	Performance of information system contingency plan (ISCP) tests/exercises.	Level 2	Level 2

Source: as determined by Williams Adley, & Company-DC, LLP

Williams Adley determined that the Peace Corps had not fully developed an agency-level BIA and did not integrate the results into a strategy, or other plan, to enable development efforts (Metric 33). To reach compliance as a Level 2 – Defined program and transition to Level 3 – Consistently Implemented, the Peace Corps needs to conduct an agency-level BIA and integrate that information

[8] M-21-31

into security strategies, as documented in recommendation 2024-5 from the FY 2024 OIG FISMA report.

Williams Adley also determined that the Peace Corps performed its annual tabletop exercise for in-scope systems. However, the ISCP's testing and exercises were not integrated with the testing of related plans, such as an incident response plan, the Continuity of Operations Plan, and the Business Continuity Plan (Metric 34).

Based on the ratings outlined in Table 13 above, Williams Adley determined that the CP core metrics have a calculated average score of 1.50 and a maturity rating of Level 2 – Defined.

Contingency Planning – Supplemental Reporting Metrics

OMB did not identify any supplemental reporting metrics for evaluation in FY 2025.

CONCLUSION

The Peace Corps sustained progress toward establishing an effective information security program by implementing its defined processes and addressing previously issued recommendations across multiple FISMA domains. Most notably, the Information Security Continuous Monitoring and Incident Response domains advanced from Level 2 – Defined to Level 3 – Consistently Implemented, reflecting the agency's strengthened commitment to meeting FISMA requirements. Additionally, five of the eight previously issued recommendations were addressed during the FY 2025 reporting period, while three remain open at the conclusion of this review.

For the FY 2025 reporting period, the agency's overall information security program remains at Level 2 – Defined. As a result, the status of the Peace Corps' overall information security program is not effective, as it falls short of Level 4 – Managed and Measurable, which OMB has determined is necessary to have an effective information security program.

To support the Peace Corps' advancement towards a mature and effective information security program, OIG recommends that the agency continues to address previously identified recommendations and incorporates the following additional recommendations into its overall information security strategy.

Table 14: New Recommendations for FY 2025

Recommendation Number	Description
2025-1	OIG recommends that the Peace Corps develops and implements formal policies and procedures for establishing and maintaining its target cybersecurity profile(s). (Metric 1)
2025-2	OIG recommends that the Peace Corps implements formal processes to ensure externally sourced products, systems, components, and services comply with its cybersecurity and supply chain risk management requirements, including integration into procurement and vendor management activities. (Metric 5)
2025-3	OIG recommends that the Peace Corps develops and implements formal policies and procedures for maintaining a comprehensive inventory of data and corresponding metadata. (Metric 10)
2025-4	OIG recommends that the Peace Corps allocates the necessary resources to ensure that baseline configurations and associated deviations are reviewed and updated at least annually. (Metric 14)
2025-5	OIG recommends that the Peace Corps prioritize the procurement and implementation of a Data Loss Prevention solution to enhance its ability to detect and prevent unauthorized data exfiltration. (Metric 22)

Source: as determined by PC-OIG and Williams Adley, & Company-DC, LLP

APPENDIX A – OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

Williams Adley's primary objective was to determine the effectiveness of the Peace Corps' information security program and practices in accordance with FISMA requirements. Williams Adley reviewed a group of FISMA security metrics selected by OMB and submitted the assessment results through CyberScope to OMB, as required.

Williams Adley also evaluated the remediation efforts taken to address previously issued conditions and recommendations.

Scope

This review performed an independent assessment of the Peace Corps' information security program, including evaluating the effectiveness of security controls for a subset of systems, as required, for FY 2025:

- Peace Corps General Support System,
- Peace Corps Medical Electronic Documentation & Inventory Control System, and
- Peacecorps.gov.

Methodology

Williams Adley performed this review in accordance with FISMA, OMB, and NIST guidance. Williams Adley believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the review objectives. The work was performed to meet the Generally Accepted Government Auditing Standards included in Chapter 3, Ethics, Independence, and Professional Judgement; Chapter 4, Competence and Continuing Professional Education; Chapter 5, Quality Control and Peer Review; and Chapter 8, Fieldwork Standards for Performance Audits.

Williams Adley interviewed Peace Corps' management officials to determine the effectiveness of the Peace Corps' information security program and practices across six function areas — *Govern, Identify, Protect, Detect, Respond,* and *Recover*. In addition to interviews, Williams Adley also observed operations remotely via screen sharing technology, conducted sampling where applicable, inspected Peace Corps' policies and procedures, and obtained sufficient evidence to support the conclusions presented in this report. Furthermore, Williams Adley communicated identified exceptions to the agency's management using Notices of Findings and obtained management's concurrence on the findings. The detailed Notices of Findings were not included in this report due to the sensitive information and because they were included in the initial CyberScope submission for FISMA.

APPENDIX B – STATUS OF PRIOR YEARS' RECOMMENDATIONS

Recommendation Number	Description	Status
1	OIG recommends that the Peace Corps develops a strategy and structure that integrates information security into the agency's business operations. This should include an established responsibility for assessing information security risks in all agency programs and operations and providing this analysis to senior leadership, including the Enterprise Risk Management Council, for decision-making.	Closed
2	OIG recommends that the Peace Corps further defines and implements the Enterprise Risk Management program to ensure information security risks are communicated and monitored at the system, business process, and entity levels.	Closed
3	OIG recommends that the Peace Corps completes and fully implements an identity credential and access management program. (Metric 19)	Open
2024-1	OIG recommends that the Peace Corps develops and implements a cybersecurity risk register to support the implementation of a fully integrated Risk Management and Information Security Continuous Monitoring program.	Closed
2024-2	OIG recommends that the Peace Corps develops component authenticity policies and procedures. (Metric 5)	Open
2024-3	OIG recommends that the Peace Corps periodically evaluates, reviews, and updates its policies and procedures, as necessary, to align with an issued and approved Identity, Credential, and Access Management strategy which includes assigning personnel risk designations and performing appropriate screening prior to granting access to its systems.	Closed
2024-4	OIG recommends that the Peace Corps conducts, captures, and shares lessons learned in its implementation of the incident response program.	Closed
2024-5	OIG recommends that the Peace Corps conducts agency-level Business Impact Assessments and integrates the results into information security strategies and other plan development efforts. (Metric 33)	Open

APPENDIX C – AGENCY COMMENTS

MEMORANDUM

TO: Joaquin Ferrao, Inspector General

FROM: Paul Shea, Chief Executive Officer

CC: Kris Besch, Deputy Chief Executive Officer
Richard E. Swarttz, Chief of Staff
Alexis Fowler, General Counsel
Michael Terry, Chief Information Officer
Khalid Nayyar, Acting Chief Information Security Officer
Shawn Bardwell, Associate Director, Office of Safety and Security
Emily Haimowitz, Chief Compliance and Risk Officer
Jennifer Piorkowski, Director, Executive Secretariat
Julie Nelson, Compliance Officer Audit Liaison

DATE: December 12, 2025

RE: Agency Response to the *Fiscal Year (FY) 2025 Federal Information Security Modernization Act of 2014 (FISMA) Review of the Information Security Program and Practices at the Peace Corps*

Thank you for the opportunity to respond to this preliminary report from the Office of Inspector General (OIG). Enclosed please find the agency's response to the recommendations made by the Inspector General as outlined in the OIG's *Fiscal Year (FY) 2025 Federal Information Security Modernization Act of 2014 (FISMA) Review of the Information Security Program and Practices at the Peace Corps* sent to the agency on November 26, 2025.

The agency continues to prioritize recommended actions to strengthen its information security program. The proposed timelines in response to the recommendations below reflect that prioritization. Actions planned by the agency to address the recommendations are contingent on the availability and prioritization of essential resources, including the funding and acquisition of necessary technology solutions.

Recommendation 1
OIG recommends that the Peace Corps develops and implements formal policies and procedures for establishing and maintaining its target cybersecurity profile(s) (Metric 1).

Concur
Response:
The Peace Corps will adapt its existing cybersecurity profile document to the Cybersecurity Framework 2.0 template.

Documents to be Submitted:
- Cybersecurity Profile Document

Status and Timeline for Completion: March 2026

Recommendation 2
OIG recommends that the Peace Corps implements formal processes to ensure externally sourced products, systems, components, and services comply with its cybersecurity and supply chain risk management requirements, including integration into procurement and vendor management activities (Metric 5).

Concur
Response:
The Peace Corps has finalized its *Supply Chain Risk Management (SCRM) Strategy Policy* and is currently working to integrate the strategy into ongoing contract operations with the Office of the Chief Financial Officer/Acquisition and Contract Management (OCFO/ACM).

Documents to be Submitted:
- Supply Chain Risk Management policy and procedures

Status and Timeline for Completion: June 2026

Recommendation 3
OIG recommends that the Peace Corps develops and implements formal policies and procedures for maintaining a comprehensive inventory of data and corresponding metadata (Metric 10).

Concur
Response:
The Peace Corps will develop formal policies and procedures for maintaining a comprehensive inventory of data and corresponding metadata, and an implementation plan for these policies and procedures.

Documents to be Submitted:

- Data Governance policy and procedure
- Plan for implementation of policy and procedure

Status and Timeline for Completion: June 2026

Recommendation 4

OIG recommends that the Peace Corps allocates the necessary resources to ensure that baseline configurations and associated deviations are reviewed and updated at least annually (Metric 14).

Concur

Response:

The Peace Corps is committed to continuing its work to bring its configuration baselines up to date and ensuring that reviews are executed in accordance with defined procedures.

Documents to be Submitted:

- Baseline Configuration Documentation

Status and Timeline for Completion: May 2026

Recommendation 5

OIG recommends that the Peace Corps prioritizes the procurement and implementation of a Data Loss Prevention solution to enhance its ability to detect and prevent unauthorized data exfiltration (Metric 22).

Concur

Response:

The Peace Corps will work to better define its data loss prevention strategy and deploy technical controls to enforce that strategy.

Documents to be Submitted:

- *Data Loss Prevention Peace Corps Policy*

Status and Timeline for Completion: August 2026

Recommendation 6

OIG recommends that the Peace Corps completes and fully implements an identity credential and access management program (Metric 19).

Concur
Response: The Peace Corps intends to prioritize finalizing this strategy in Fiscal Year 2026, specifically identifying and documenting specific processes that bridge physical and digital security.

Documents to be Submitted:
- *Identity, Credential, and Access Management (ICAM) Policy*

Status and Timeline for Completion: March 2027

Recommendation 7
OIG recommends that the Peace Corps develops component authenticity policies and procedures (FY 2024 Metric 15).

Concur
Response:
The Peace Corps has finalized its *Supply Chain Risk Management (SCRM) Strategy Policy* and is currently working to integrate the strategy into ongoing contract operations with OCFO/ACM.

Documents to be Submitted:
- *Supply Chain Risk Management Policy*

Status and Timeline for Completion: June 2026

Recommendation 8
OIG recommends that the Peace Corps conducts agency-level Business Impact Assessments and integrates the results into information security strategies and other plan development efforts (Metric 33).

Concur
Response:
The Peace Corps intended to deliver this in early 2026, but this resource-intensive work was delayed due to resource allocation. Work continues on the Business Impact Analysis. The Peace Corps is working on new scheduling and resourcing to allow the work to be completed.

Documents to be Submitted:
- *Business Impact Analysis*

Status and Timeline for Completion: December 2026

APPENDIX D – OIG'S RESPONSE

The Agency concurred with the five new recommendations and three open prior recommendations and reports that it plans to implement the recommendations between January 2026 and March 2027. The FY 2026 FISMA review will validate the implementation and progress taken to address these recommendations.

The OIG also recognizes the progress that the Peace Corps has made toward establishing an effective information security program in implementing its defined processes and closing out prior year recommendations. The Peace Corps should continue to improve and ensure that all areas or metrics have adequate policies and procedures to ensure at least a Level 2, defined, rating and continue to work to improve the implementation to support increasing ratings to Level 3, consistently implemented, and then at a Level 4, managed and measurable, ratings.

Finally, OIG wants to stress the importance of dedicating the appropriate resources to carry out these initiatives. It is critical that corrective actions are well thought out and applied in a manner that assures the agency can make a sustainable improvement and does not put the Peace Corps' data at risk.

Help Promote the Integrity, Efficiency, and Effectiveness of the Peace Corps

Anyone knowing of wasteful practices, abuse, mismanagement, fraud, or unlawful activity involving Peace Corps programs or personnel should call or write the Office of Inspector General. Reports or complaints can also be made anonymously.

Contact OIG

Reporting Hotline:

U.S./International:	202.692.2915
Toll-Free (U.S. only):	800.233.5874
Email:	OIG@peacecorpsoig.gov
Online Reporting Tool:	Hotline | Peace Corps OIG
Mail:	Peace Corps Office of Inspector General 1275 First Street NE Washington, DC 20526

For General Information:

Main Office:	202.692.2900
Website:	peacecorpsoig.gov
:	x.com/pcoig