Peace Corps Office of
INSPECTOR GENERAL

Special Report
Review of the Peace Corps' Information Security Program

IG-25-01-SR
October 2024

WILLIAMS ADLEY

CONTENTS

RESULTS IN BRIEF

The Peace Corps has made significant progress in enhancing its information security posture since Fiscal Year (FY) 2023 by addressing four recommendations from previous reports. Williams Adley identified improvements in various Federal Information Security Modernization Act of 2014 (FISMA) domains, such as Risk Management, Configuration Management, and Incident Response, which reflect a stronger commitment to meeting FISMA requirements. However, the Peace Corps' information security program remained at a Level 2, Defined, falling short of Level 4, the rating that the Office of Management and Budget (OMB) considers to be an effective level of security at the domain, function, and overall program level. Furthermore, Williams Adley identified nine new exceptions and issued five new recommendations.

Recommendations Closed	Exceptions Identified	Recommendations Issued
4	9	5

The FY 2024 reporting period provided an opportunity to evaluate Peace Corps against the core group of Inspector General (IG) FISMA metrics and supplemental IG FISMA metrics. The core metrics represent a combination of administration priorities and other highly valuable controls that must be evaluated annually. The supplemental metrics were last evaluated in FY 2021.

20
Core Metrics Evaluated

17
Supplemental Metrics Evaluated

Overall Maturity Rating - Level 2 (Defined)

Presented below in **Figure 1** and **Figure 2** are the results of the FY 2024 FISMA review from a core and supplemental metric perspective. Details regarding the calculation of each FISMA domain's rating are found within the body of this report.

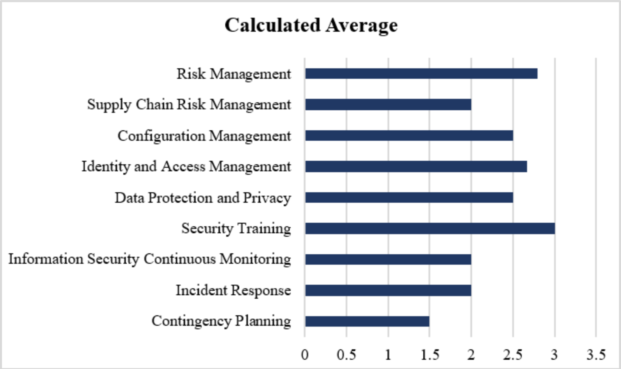


Figure 1. FY 2024 Core Maturity Ratings

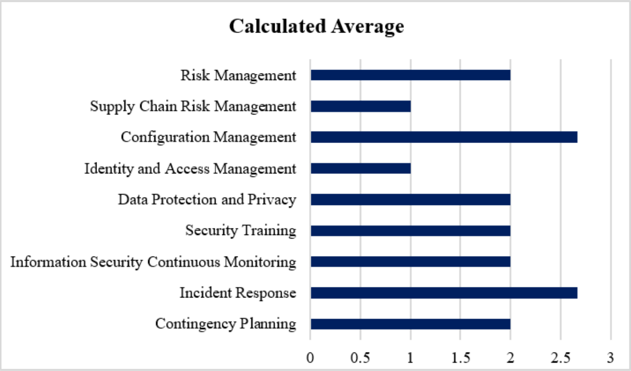


Figure 2. FY 2024 Supplemental Maturity Ratings

To supplement the content within this report, we have included a copy of the Agency's response to the results of the FY 2024 review in **Appendix C**. Please note that we did not audit the management's response and, accordingly, do not express any assurance on it.

BACKGROUND

THE PEACE CORPS

The Peace Corps is an independent Federal agency whose 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) help interested countries in meeting their need for trained people; (2) help promote a better understanding of Americans on the part of the peoples served; and (3) help promote a better understanding of other peoples 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 requires each agency's information security program to be evaluated and reported annually to OMB, Congress, and the Government Accountability Office on the effectiveness of the agency's information security policies, procedures, and practices. Each agency's Office of Inspector General (OIG) must conduct an independent annual assessment of its information security program and report the findings to OMB within the defined timelines. The Peace Corps OIG contracted with the Independent Public Accounting firm Williams Adley, & Co.-DC LLP (Williams Adley) to complete the FY 2024 IG FISMA assessment of the Peace Corps information security program. The Peace Corps OIG opted to complete the annual independent assessment in accordance with Generally Accepted Government Auditing Standards.

FISMA REPORTING METRICS

Williams Adley used the FISMA metrics published by OMB and the Department of Homeland Security (DHS), in consultation with the Council of the Inspectors General on Integrity and Efficiency, to evaluate the effectiveness of Peace Corps' information security program. The FISMA reporting metrics are organized around the five security functions—Identify, Protect, Detect, Respond, and Recover— as outlined in the National Institute of Standards and Technology (NIST)'s cybersecurity framework.

On December 4, 2023, OMB issued Memorandum M-24-04 ("Memorandum for the Heads of Executive Departments and Agencies: FY 2024 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions on how to meet the FY 2024 FISMA reporting requirements.

According to the memorandum, agency IGs, or independent assessors, are "encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency, and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls."

MATURITY MODEL AND SCORING METHODOLOGY

OMB provided guidance to agency IGs, or independent assessors, for determining the maturity of their agencies' security programs through the publication of the FY 2023 – 2024 Inspector General FISMA Reporting Metrics. According to the reporting metrics, "the OMB believes that achieving a Level 4 (Managed and Measurable) or above represents an effective level of security"; see ***Table 1*** below for a definition of each 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.
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.

Table 1 – IG Evaluation Maturity Level Descriptions

Additionally, IGs and independent auditors are instructed 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 (identify, protect, detect, respond, and recover) and the overall program".

Furthermore, IGs and independent auditors are 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 a data point to support their risk-based determination of overall program and function level effectiveness.

RESULTS OF THE FY 2024 FISMA REVIEW

I. *IDENTIFY*

The Identify function was assessed at a Level 2 maturity and is supported by the Risk Management and Supply Chain Risk Management domains.

Risk Management – Core Reporting Metrics

The OMB identified five reporting metrics as core for the development of a Risk Management program. **Table 2** presents both the previously assessed (FY 2023) maturity ratings and the FY 2024 assessed maturity ratings for the core Risk Management metrics. Notably, the maturity ratings for all five core metrics increased, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
1	Comprehensive and accurate inventory of agency information systems	Level 2	Level 3
2	An up-to-date inventory of hardware assets	Level 2	Level 3
3	An up-to-date inventory of software and associated licenses	Level 2	Level 3
5	Information system security risks are adequately managed at all organization tiers	Level 2	Level 3
10	Use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities	Level 1	Level 2

Table 2 – Ratings for Core Metric Questions within the Risk Management Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps maintains a comprehensive and accurate inventory of information systems by implementing the Cybersecurity Assessment and Management tool (Metric 1) and maintaining its hardware and software component inventories (Metrics 2 and 3).

Further, the Peace Corps defined its risk appetite and risk tolerance and is currently holding monthly Enterprise Risk Management (ERM) meetings, further maturing its ERM implementation. However, the Peace Corps has not fully incorporated cybersecurity risks into the ERM program (Metric 5).

Lastly, Williams Adley confirmed that the Peace Corps does not use technology or automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities (Metric 10).

Based on the ratings outlined in **Table 2** above, Williams Adley determined that the Risk Management core metrics have a calculated average score of 2.80, corresponding to a maturity rating of Level 3 (Consistently Implemented).[1]

Risk Management – Supplemental Reporting Metrics

OMB identified two supplemental reporting metrics to evaluate in FY 2024. **Table 3** shows the previously assessed (FY 2021) maturity ratings and the FY 2024 assessed maturity ratings for the supplemental Risk Management metrics. Notably, the maturity rating for one supplemental metric increased, as listed below:

Metric Question	Topic	FY 2021 Maturity Rating[2]	FY 2024 Maturity Rating
4	Categorized and communicated the importance/priority of information systems	Level 2	Level 2
6	Use an information security architecture to provide a disciplined and structured methodology for managing risk	Level 1	Level 2

Table 3 – Ratings for Supplemental Metric Questions within the Risk Management Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps has defined policies, procedures, and processes for categorizing, reviewing, and communicating the importance and priority of using information systems that enable its missions and business functions, including high value assets, as appropriate. However, the agency does not make decisions using risk-based allocation of resources or system categorization, including for the protection of high value assets, as appropriate, through collaboration and data-driven prioritization (Metric 4).

Additionally, since FY 2021, the Peace Corps defined an information security architecture that provides a methodology for managing risk. However, the Peace Corps has not fully implemented an information security architecture that is both integrated into and supports the agency's enterprise architecture, which should provide a disciplined and structured methodology for managing risk (Metric 6).

Based on the ratings outlined in **Table 3** above, Williams Adley determined that the Risk Management supplemental metrics have a calculated average score of 2.00, corresponding to a maturity rating of Level 2 (Defined).

[1] The FY 2024 IG FISMA Metrics state that "calculated averages will not be automatically rounded to a particular maturity level." Furthermore, it is at the discretion of the IGs, or independent assessors, to select the appropriate maturity rating based on the results of the audit procedures performed. Williams Adley believes that the current maturity of the activities associated with supplemental metrics do not significantly impact the agency's ability to manage risks within its organization.

[2] The FY 2024 supplemental FISMA reporting metrics were last evaluated during the FY 2021 reporting period.

Supply Chain Risk Management – Core Reporting Metrics

The OMB identified one reporting metric as a core for the development of a Supply Chain Risk Management program. **Table 4** presents both the previously assessed (FY 2023) maturity rating and the FY 2024 assessed maturity rating for the core Supply Chain Risk Management metric. There was no maturing since the last assessment, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
14	Products, system components, systems, and services of external providers are consistent with cybersecurity and supply chain requirements	Level 2	Level 2

Table 4 – Ratings for Core Metric Questions within the Supply Chain Risk Management Domain

The rating above is supported by the following summaries related to the metric.

Williams Adley confirmed that the Peace Corps developed Supply Chain Risk Management policy and procedures as the foundation for the strategic direction of its Supply Chain Risk Management program (Metric 14). However, as of the date of this report, the Peace Corps is still in the process of implementing its defined Supply Chain Risk Management program and was not evaluated from a Level 3 (Consistently Implemented) perspective.

Based on the rating outlined in **Table 4** above, Williams Adley determined that the Supply Chain Risk Management core metric has a calculated average score of 2.00 and a maturity rating of Level 2 (Defined).

Supply Chain Risk Management – Supplemental Reporting Metrics

OMB identified one supplemental reporting metric for evaluation in FY 2024. **Table 5** presents both the previously assessed (FY 2021) maturity rating and the FY 2024 assessed maturity rating for the supplemental Supply Chain Risk Management metric. There was no maturing since the last assessment, as listed below:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
15	Counterfeit components are detected and prevented from entering the organization’s systems	Level 1	Level 1

Table 5 – Ratings for Supplemental Metric Questions within the Supply Chain Risk Management Domain

As stated above, the Peace Corps developed Supply Chain Risk Management policy and procedures to form the foundation for the strategic direction of its Supply Chain Risk Management program. However, the Peace Corps has not defined or communicated its component authenticity policies and procedures (Metric 15).

Based on the rating outlined in **Table 5** above, Williams Adley determined that the Supply Chain Risk Management supplemental metric has a calculated average score of 1.00 and a maturity rating of Level 1 (Ad Hoc).

II. *PROTECT*

The Protect function was assessed at a Level 2 maturity and is supported by the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains.

Configuration Management – Core Reporting Metrics

The OMB identified two reporting metrics as core for the development of a Configuration Management program. **Table 6** presents both the FY 2023 maturity ratings and the FY 2024 assessed maturity ratings for the core Configuration Management metrics. Notably, the maturity rating for one core metric increased, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
20	Use of configuration settings and common secure configurations	Level 2	Level 2
21	Use of flaw remediation processes	Level 2	Level 3

Table 6 – Ratings for Core Metric Questions within the Configuration Management Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps has developed, documented, and disseminated its policies and procedures for configuration settings and common secure configurations. However, the agency has not consistently implemented, assessed, or maintained secure configuration settings for all its systems (Metric 20).

Furthermore, the Peace Corps revamped and consistently implemented its vulnerability management process and demonstrated a decrease in outstanding vulnerabilities over time. The agency also developed qualitative performance metrics to monitor the Service Level Agreements' performance in alignment with the Vulnerability Management and Patch Management program. The Peace Corps consistently implemented a Plan of Action and Milestones (POA&M) process to address outstanding critical and high vulnerabilities that are not addressed within the required timeframes (Metric 21).

Based on the ratings outlined in **Table 6** above, Williams Adley determined that the Configuration Management 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 identified three supplemental reporting metrics for evaluation in FY 2024. **Table 7** presents the previously assessed (FY 2021) maturity ratings and the FY 2024 assessed maturity ratings for the supplemental Configuration Management metrics. Importantly, the maturity rating for two supplemental metrics increased, as listed below:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
17	Roles and responsibilities of configuration management stakeholders have been defined, communicated, and implemented across the agency, and appropriately resourced	Level 2	Level 3
18	Use an enterprise-wide configuration management plan	Level 2	Level 2
23	Defined and implemented configuration change control activities	Level 2	Level 3

Table 7 – Ratings for Supplemental Metric Questions within the Configuration Management Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley confirmed that stakeholders are performing their assigned roles and responsibilities to support configuration management activities (Metric 17).

Additionally, Williams Adley confirmed that the Peace Corps has developed an enterprise-wide configuration management plan with the requirements that include the necessary components. However, the agency has not consistently implemented the activities outlined in the configuration management plan, such as developing baseline management processes (Metric 18).

Lastly, Williams Adley determined that the Peace Corps has consistently implemented its change control policies, procedures, and processes, including explicit consideration of the security impacts prior to the change's implementation (Metric 23).

Based on the ratings outlined in **Table 7** above, Williams Adley determined that the Configuration Management supplemental metrics have a calculated average score of 2.67 and a maturity rating of Level 3 (Consistently Implemented).

Identity, Credential, and Access Management – Core Reporting Metrics

OMB identified three reporting metrics as core for the development of an Identity, Credential, and Access Management (ICAM) program. **Table 8** presents both the previously assessed (FY 2023) maturity ratings and the FY 2024 assessed maturity ratings for the core ICAM metrics. Notably, the maturity ratings for all three core metrics increased, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
30	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 2	Level 3
31	Use of strong authentication mechanisms (PIV or an IAL3/ AAL3 credential for privileged users)	Level 2	Level 3
32	Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties	Level 1	Level 2

Table 8 – Ratings for Core Metric Questions within the Identity and Access Management Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that privileged and non-privileged users use PIV cards at headquarters and international posts to authenticate against Peace Corps' systems[3] (Metrics 30 and 31).

Additionally, Williams Adley found that privileged users use PIV authentication to make changes to Doman Name Services (DNS) records[4].

Lastly, Williams Adley determined that the Peace Corps has defined its processes for assigning, managing, and reviewing privileged accounts. The defined processes cover approval and tracking inventorying and validating; and logging and reviewing privileged users' accounts. However, the agency did not consistently implement its defined processes (Metric 32).

Based on the ratings outlined in **Table 8** above, Williams Adley determined that the ICAM core metrics have a calculated average score of 2.67 and a maturity rating of Level 3 (Consistently Implemented).

Identity, Credential, and Access Management – Supplemental Reporting Metrics

The OMB identified one supplemental reporting metric for evaluation in FY 2024. **Table 9** presents the previously assessed (FY 2021) maturity rating and the FY 2024 assessed maturity rating for the supplemental ICAM metric. The metric rating has decreased since the last assessment, as listed below:

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

[4] In response to attackers redirecting and intercepting web and mail traffic, DHS issued Emergency Directive 19-01 to require agency to implement Multi-Factor Authentication to DNS Accounts. This requirement is reflected in the Level 4 maturity description for Question 31.

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
28	Developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems	Level 2	Level 1

Table 9 – Ratings for Supplemental Metric Questions within the Identity, Credential, and Access Management Domain

Williams Adley determined that although the Peace Corps has reasonable processes and procedures for assigning personnel risk designations and performing personnel screenings, the Peace Corps is not in compliance with current requirements to integrate and review risks, access, and permissions as it relates to its systems and data. The Peace Corps does not have an approved ICAM strategy, as required by OMB M-19-17, which was issued in May 2019. In addition, Peace Corps has not reviewed and updated their related policies and procedures since 2019. To reach compliance as a defined program and transition to consistently implemented, the Peace Corps needs to issue an ICAM strategy and regularly review and update their policies and procedures to ensure they address current cybersecurity risks, align with relevant guidance, and are integrated with the agency's ICAM strategy (Metric 28).

Based on the rating outlined in Table 9 above, Williams Adley determined that the ICAM supplemental metric has a calculated average score of 1.00 and a maturity rating of Level 1 (Ad Hoc).

Data Protection and Privacy – Core Reporting Metrics

The OMB identified two reporting metrics as core for the development of a Data Protection and Privacy program. **Table 10** presents the previously assessed (FY 2023) maturity ratings and the FY 2024 assessed maturity ratings for the core Risk Management metrics. Notably, the maturity ratings for both core metrics increased, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
36	Use of 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.	Level 2	Level 3
37	Use of security controls to prevent data exfiltration and enhance network defenses.	Level 1	Level 2

Table 10 – Ratings for Core Metric Questions within the Data Protection and Privacy Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps implemented its data protection policies and procedures for data at rest or in transit, prevention and detection of untrusted removable media, and destruction or reuse of media containing PII or other sensitive agency data (Metric 36).

Additionally, Williams Adley determined that the Peace Corps has implemented security controls to prevent data exfiltration including, but not limited to, monitoring inbound and outbound traffic and reviewing data exfiltration traffic. The Peace Corps has implemented security controls to prevent data exfiltration including, but not limited to, monitoring inbound and outbound traffic and reviewing data exfiltration traffic. However, Data Loss Prevention (DLP) tool is not fully implemented (Metric 37).

Based on the ratings outlined in **Table 10** above, Williams Adley determined that the Data Protection and Privacy 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

The OMB identified two supplemental reporting metrics for evaluation in FY 2024. **Table 11** presents the previously assessed (FY 2021) maturity ratings and the FY 2024 assessed maturity ratings for the supplemental Data Protection and Privacy metrics. Importantly, the maturity rating for one supplemental metric increased, as listed below:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
38	Developed and implemented a Data Breach Response Plan to respond to privacy events.	Level 2	Level 2
39	Privacy awareness training is provided to all individuals, including role-based privacy training.	Level 1	Level 2

Table 11 – Ratings for Supplemental Metric Questions within the Data Protection and Privacy Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley confirmed that the Peace Corps has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notifications. Further, a breach response team that includes the appropriate agency officials has been established. However, the agency did not consistently capture and share lessons learned from previous breaches (Metric 38).

Furthermore, the Peace Corps has defined and communicated its privacy awareness training program, including requirements for role-based privacy awareness training. The training has been tailored to the agency's mission and risk environment. However, the agency did not consistently implement privacy awareness training and role-based privacy awareness training (Metric 39).

Based on the ratings outlined in **Table 11** above, Williams Adley determined that the Data Protection and Privacy supplemental metrics have a calculated average score of 2.00 and a maturity rating of Level 2 (Defined).

Security Training – Core Reporting Metrics

The OMB identified one reporting metric as core for the development of a Security Training program. **Table 12** presents the previously assessed (FY 2023) maturity rating and the FY 2024 assessed maturity rating for the core Security Training metric. Notably, the maturity rating for one core metric increased, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
42	Use of assessments of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training	Level 2	Level 3

Table 12 – Ratings for Core Metric Questions within the Security Training Domain

Williams Adley determined that the Peace Corps has assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and identified its skill gaps. Further, the agency developed and implemented POA&Ms to address the identified gaps (Metric 42).

Based on the rating outlined in **Table 12** above, Williams Adley determined that the Security Training 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 identified two supplemental reporting metrics for evaluation in FY 2024. **Table 13** presents the previously assessed (FY 2021) maturity ratings and the FY 2024 assessed maturity ratings for the supplemental Security Training metrics. There was no maturing since the last assessment, as listed below:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
44	Security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems	Level 2	Level 2
45	Specialized security training is provided to individuals with significant security responsibilities	Level 2	Level 2

Table 13 – Ratings for Supplemental Metric Questions within the Security Training Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps has defined and tailored its security awareness policies, procedures, and related material and delivery methods based on FISMA requirements, its mission, risk environment, and the types of information systems its users have access to. In addition, the agency has defined its processes for ensuring that all information system users, including contractors, are provided security awareness training. However, the agency has not defined its processes for evaluating and obtaining feedback on its security awareness and training program or using that information to make continuous improvements (Metric 44).

Additionally, Williams Adley determined that the Peace Corps has defined its security training policies, procedures, and related material based on FISMA requirements, its mission and risk environment, and the types of agency roles with significant security responsibilities. In addition, the agency has defined its processes for ensuring that personnel with assigned security roles and responsibilities are provided specialized security training. However, the agency has not defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements (Metric 45).

Based on the ratings outlined in **Table 13** above, Williams Adley determined that the Security Training supplemental metrics have a calculated average score of 2.00 and a maturity rating of Level 2 (Defined).

III. *DETECT*

The Detect function was assessed at a Level 2 maturity and is supported by the Information Security Continuous Monitoring (ISCM) domain.

ISCM – Core Reporting Metrics

OMB identified two reporting metrics as core for the development of an ISCM program. **Table 14** presents the previously assessed (FY 2023) maturity ratings and the FY 2024 assessed maturity ratings for the core ISCM metrics. Notably, maturity ratings for one core metric increased, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
47	Use of ISCM policies and an ISCM strategy that addresses the ISCM requirements and activities at each organizational tier	Level 1	Level 2
49	Performance of ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls	Level 2	Level 2

Table 14 – Ratings for Core Metric Questions within the ISCM Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps has developed, tailored, and communicated its ISCM policies and strategy. However, the Peace Corps has not consistently implemented its ISCM strategy to demonstrate how cybersecurity risks are incorporated into the agency's enterprise risk management program. Further, the Peace Corps has not yet consistently implemented its defined ISCM activities or monitoring requirements at the entity and organizational-level (Metric 47).

Williams Adley determined that the Peace Corps has developed an Ongoing Authorization Standard Operating Procedure, and successfully transitioned four FISMA systems into Ongoing Authorizations (Metric 49).

Based on the metric ratings outlined in **Table 14** above, Williams Adley determined that the ISCM core metrics have a calculated average score of 2.00 and a maturity rating of Level 2 (Defined).

ISCM – Supplemental Reporting Metrics

OMB identified one supplemental reporting metric for evaluation in FY 2024. **Table 15** presents both the previously assessed (FY 2021) maturity rating and the FY 2024 assessed maturity rating for the supplemental ISCM metric. Importantly, the maturity rating for one supplemental metric increased, as listed below:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
50	Process for collecting and analyzing ISCM performance measures and reporting findings.	Level 1	Level 2

Table 15 – Ratings for Supplemental Metric Questions within the ISCM Domain

Williams Adley determined that the Peace Corps has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, the Peace Corps has recently finalized ISCM processes and activities to address prior year recommendations and is still in the early stages of the ISCM strategy's implementation (Metric 50).

Based on the rating outlined in **Table 15** above, Williams Adley determined that the ISCM supplemental metric has a calculated average score of 2.00 and a maturity rating of Level 2 (Defined).

IV. *RESPOND*

The Respond function was assessed at a Level 2 maturity and is supported by the Incident Response domain.

Incident Response – Core Reporting Metrics

OMB identified two reporting metrics as core for the development of an Incident Response program. **Table 16** presents both the previously assessed (FY 2023) maturity ratings and the FY 2024 assessed maturity ratings for the core Incident Response metrics. Notably, maturity ratings for both core metrics increased, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
54	Processes for incident detection and analysis	Level 1	Level 2
55	Processes for incident handling	Level 1	Level 2

Table 16 – Ratings for Core Metric Questions within the Incident Response Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps has taken significant steps to enhance its incident response capabilities by revamping its incident response program and implementing the established processes, from initial detection through resolution. However, the Peace Corps did not consistently capture or share lessons learned to demonstrate the effectiveness of its incident handling activities and post-incident analysis (Metrics 54 and 55).

Based on the ratings outlined in **Table 16** above, Williams Adley determined that the Incident Response core metrics have a calculated average score of 2.00 and a maturity rating of Level 2 (Defined).

Incident Response – Supplemental Reporting Metrics

OMB identified three supplemental reporting metrics for evaluation in FY 2024. **Table 17** presents both the previously assessed (FY 2021) maturity ratings and the FY 2024 assessed maturity ratings for the supplemental Incident Response metrics. Importantly, the maturity rating for one supplemental metric increased, as listed below:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
52	Use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents	Level 2	Level 2
53	Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization	Level 2	Level 3
56	Incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner	Level 3	Level 3

Table 17 – Ratings for Supplemental Metric Questions within the Incident Response Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps has implemented its incident response plan, but the agency has not implemented lessons learned practices and does not monitor or analyze the qualitative and quantitative performance measures that have been defined in its incident response plan, to monitor and maintain the effectiveness of its overall incident response capability (Metric 52).

Additionally, Williams Adley determined that incident response stakeholders are performing their defined roles and responsibilities, and the levels of authority and dependencies are defined, communicated, and implemented (Metric 53).

Lastly, the Peace Corps collaborates with internal and external stakeholders to ensure the details regarding incidents are communicated in a timely manner. However, the Peace Corps did not capture the incident response metrics that are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders (Metric 56).

Based on the ratings outlined in **Table 17** above, Williams Adley determined that the Incident Response supplemental metrics have a calculated average score of 2.67 and a maturity rating of Level 3 (Consistently Implemented).

V. *RECOVER*

The Recover function was assessed at a Level 2 maturity and is supported by the Contingency Planning domain.

Contingency Planning – Core Reporting Metrics

OMB identified two reporting metrics as core for the development of a Contingency Planning program. **Table 18** presents both the previously assessed (FY 2023) maturity ratings and the FY 2024 assessed maturity ratings for the core Contingency Planning metrics. There was no maturing since the last assessment, as listed below:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
61	Business impact analyses (BIA) are used to guide contingency planning efforts	Level 1	Level 1
63	Performance of information system contingency plan (ISCP) tests/exercises	Level 2	Level 2

Table 18 – Ratings for Core Metric Questions within the Contingency Planning Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley determined that the Peace Corps has not fully developed an agency-level BIA and did not integrate the results into strategy or other plan development efforts (Metric 61).

Williams Adley also confirmed 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 incident response plan, the Continuity of Operations Plan, and the Business Continuity Plan (Metric 63).

Based on the ratings outlined in **Table 18** above, Williams Adley determined that the Contingency Planning core metrics have a calculated average score of 1.50 and a maturity rating of Level 2 (Defined).

Contingency Planning – Supplemental Reporting Metrics

OMB identified two supplemental reporting metrics for evaluation in FY 2024. **Table 19** presents both the previously assessed (FY 2021) maturity ratings and the FY 2024 assessed maturity ratings for the supplemental Contingency Planning metrics. There was no maturing since the last assessment, as listed below:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
62	ISCPs are developed, maintained, and integrated with other continuity plans	Level 2	Level 2
64	Perform information system backup and storage, including the use of alternate storage and processing sites	Level 2	Level 2

Table 19 – Ratings for Supplemental Metric Questions within the Contingency Planning Domain

The ratings above are supported by the following summaries related to each metric.

Firstly, Williams Adley confirmed that the Peace Corps has developed its information system contingency plans, however, they are not yet integrated with other continuity plans (Metric 62).

Furthermore, Williams Adley confirmed that the Peace Corps has defined its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and a redundant array of independent disks. The agency has considered alternative approaches when developing its backup and storage strategies, including cost, maximum downtimes, recovery priorities, and its integration with other contingency plans. However, supply chain alternatives are not incorporated into the agency's contingency planning strategy. Furthermore, the contingency plans are not integrated with continuity documents and requirements (specifically, evidence of user- and system-level backups for a defined timeframe) (Metric 64).

Based on the ratings outlined in **Table 19** above, Williams Adley determined that the Contingency Planning supplemental metrics have a calculated average score of 2.00 and a maturity rating of Level 2 (Defined).

CONCLUSION

Williams Adley concluded that the Peace Corps has continued to make significant improvements towards establishing an effective information security program through the implementation of its defined processes and addressing previously issued recommendations across multiple FISMA domains.

However, the agency's overall information security program remained at a Level 2, Defined, for the FY 2024 reporting period. OMB considers Level 4 maturity, Managed and Measurable, to be an effective level of the information security program. To further mature its information security program to the next level the Peace Corps will need to consistently implement its processes, as defined by the governing documentation (strategies, policies, and procedures) across all FISMA domains.

To assist the Peace Corps in addressing the challenges in developing a mature and effective information security program, we recommend that the Peace Corps continue to address previously identified recommendations and incorporate the following recommendations into their overall information security program:

Recommendation #	Recommendation Description
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 (ISCM) program (Metric 10).
2024-2	OIG recommends that the Peace Corps develops component authenticity policies and procedures (Metric 15).
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 ICAM strategy which includes assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (Metric 28).
2024-4	OIG recommends that the Peace Corps conducts, captures, and shares lessons learned in its implementation of the incident response program (Metric 54 and 55).
2024-5	OIG recommends that the Peace Corps conducts agency-level Business Impact Assessments (BIA) and integrates the results into information security strategies and other plan development efforts (Metric 61).

Table 20 – New Recommendations for FY 2024

APPENDIX A
OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

Williams Adley's main 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's secondary objective was to evaluate the remediation efforts taken to address previously issued conditions and recommendations.

SCOPE

The objective of this review was to perform an independent assessment of the Peace Corps' information security program, including evaluating the effectiveness of its security controls for a subset of systems, as required, for FY 2024:

- Peace Corps General Support System
- Peace Corps Medical Electronic Documentation & Inventory Control System
- Global Operations.

METHODOLOGY

Williams Adley performed the 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 audit work was performed to meet 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.

The following laws, regulations, and policies were used to evaluate the adequacy of the controls in place at the Peace Corps:

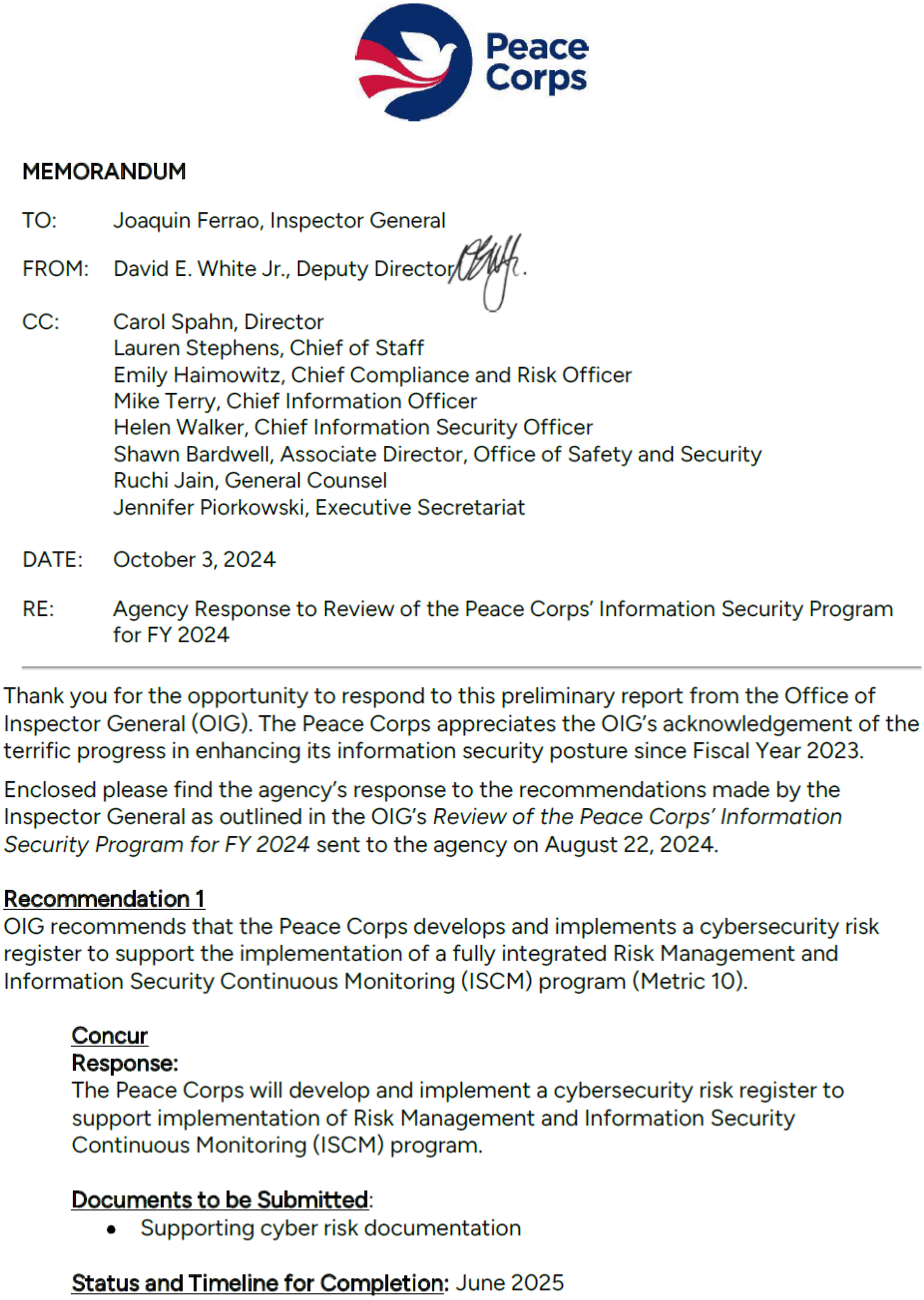
- FISMA Inspector General and CIO Metrics (FY 2023-2024)
- Public Law 113–283, FISMA
- OMB Circulars A-123, A-130
- OMB and DHS Memorandums issued annually on Reporting Instructions for FISMA and Agency Privacy Management
- OMB M-24-04, Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements
- NIST SP and NIST Federal Information Processing Standard Publications
- Peace Corps' policies and procedures relating to the FISMA domains

Williams Adley interviewed Peace Corps' management to determine the effectiveness of the Peace Corps' information security program and practices across five function areas—Identify, Protect, Detect, Respond, and Recover. In addition to interviews, we 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. We did not include the detailed Notices of Findings due to the sensitive information and because they were included in the CyberScope submission for FISMA.

APPENDIX B
STATUS OF PRIOR YEAR FISMA RECOMMENDATIONS

#	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 ERM Council, for decision-making.	Open
2	OIG recommends that the Peace Corps includes the Chief Information Security Officer at the ERM Council meetings to provide insights on cybersecurity risks.	Closed
3	OIG recommends that the Peace Corps further defines and implements the ERM program to ensure information security risks are communicated and monitored at the system, business process, and entity levels.	Open
4	OIG recommends that the Peace Corps improves its incident response process to ensure incidents are properly defined, promptly identified, and effectively remediated.	Closed
5	OIG recommends that the Peace Corps consistently improves and implements its inventory management process to ensure the information system, hardware, and software inventories are accurate, complete, and up to date.	Closed
6	OIG recommends that the Peace Corps improves its vulnerability and patch management processes by consistent and timely remediation of critical and high vulnerabilities as well as patching.	Closed
7	OIG recommends that the Peace Corps completes and fully implements an identity credential and access management program.	Open

APPENDIX C
AGENCY COMMENTS



MEMORANDUM

TO: Joaquin Ferrao, Inspector General

FROM: David E. White Jr., Deputy Director

CC: Carol Spahn, Director
Lauren Stephens, Chief of Staff
Emily Haimowitz, Chief Compliance and Risk Officer
Mike Terry, Chief Information Officer
Helen Walker, Chief Information Security Officer
Shawn Bardwell, Associate Director, Office of Safety and Security
Ruchi Jain, General Counsel
Jennifer Piorkowski, Executive Secretariat

DATE: October 3, 2024

RE: Agency Response to Review of the Peace Corps' Information Security Program for FY 2024

Thank you for the opportunity to respond to this preliminary report from the Office of Inspector General (OIG). The Peace Corps appreciates the OIG's acknowledgement of the terrific progress in enhancing its information security posture since Fiscal Year 2023.

Enclosed please find the agency's response to the recommendations made by the Inspector General as outlined in the OIG's *Review of the Peace Corps' Information Security Program for FY 2024* sent to the agency on August 22, 2024.

Recommendation 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 (ISCM) program (Metric 10).

Concur

Response:

The Peace Corps will develop and implement a cybersecurity risk register to support implementation of Risk Management and Information Security Continuous Monitoring (ISCM) program.

Documents to be Submitted:

- Supporting cyber risk documentation

Status and Timeline for Completion: June 2025

Recommendation 2

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

Concur

Response:

The Peace Corps plans to develop Supply Chain Risk Management policy and procedures to form the foundation for the strategic direction of its Supply Chain Risk Management program.

Documents to be Submitted:

- Supply Chain Risk Management policy

Status and Timeline for Completion: January 2025

Recommendation 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 ICAM strategy which includes assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (Metric 28).

Concur

Response:

The Peace Corps concurs with the recommendation to periodically evaluate, review, and update its policies and procedures to align with an issued and approved ICAM strategy. However, the organization does not concur with the report's characterization of its processes for assigning risk designations and performing appropriate screening prior to granting access to its systems as Ad Hoc. The Peace Corps has provided evidence to support its assertion that this process is both defined and consistently implemented.

Documents to be Submitted:

- Manual Section 403 Personnel Security Program policy
- Manual Section 403 Procedures

Status and Timeline for Completion: October 2025

Recommendation 4

OIG recommends that the Peace Corps conducts, captures, and shares lessons learned in its implementation of the incident response program (Metric 54 and 55).

Concur

Response:

The Peace Corps plans to conduct and capture lessons learned in its implementation of the Incident Response Program.

Documents to be Submitted:

- After Action Review documentation

Status and Timeline for Completion: January 2025

Recommendation 5

OIG recommends that the Peace Corps conducts agency-level Business Impact Assessments (BIA) and integrates the results into information security strategies and other plan development efforts (Metric 61).

Concur

Response:

The Peace Corps plans to continue coordinating its agency-level BIA development efforts with plans to publish its updated BIA.

Documents to be Submitted:

- Agency-level BIA

Status and Timeline for Completion: September 2025

APPENDIX D
OIG RESPONSE

The Agency concurred with the five recommendations and reports that it plans to implement the recommendations between January 2025 and October 2025. The FY 2025 FISMA review will validate the implementation and actions taken to address these recommendations.

We also want to recognize the improvements that the Peace Corps has made in improving many of its individual FISMA metrics from the prior year. 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, we want 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.