# OIG HIGHLIGHTS

View Report AUD-IT-16-16.

November 2015
OFFICE OF AUDITS
Information Technology Division

## Audit of the Department of State Information Security Program

### What Was Audited

**(U)** Acting on OIG's behalf, Williams, Adley & Company-DC, LLP (Williams, Adley), an independent public accounting firm, conducted this audit to assess the effectiveness of the Department's information security program and to determine whether security practices in FY 2015 complied with applicable Federal laws, regulations, and information security standards.

### What OIG Recommends

**(U)** OIG made four recommendations to improve the Department's information security program. Specifically, OIG is recommending that the Department (1) amend the [Redacted] (b) (5) [redacted] (2) review the organizational placement of the Chief Information Officer (CIO) and make a determination as to whether the CIO should be realigned within the Department's organizational structure; (3) implement an [Redacted] (b) (5) [redacted]

**(U)** Based on the Department's responses to a draft report of this report, OIG considers all four recommendations resolved, pending further action.

### What Was Found

~~(SBU)~~ Williams, Adley identified control weaknesses that significantly impacted the Department's information security program. While the Department had taken some action to improve its information security program since our last assessment in FY 2014, Williams, Adley continued to find that the Department was not in compliance with Federal laws, regulations, and information security standards. Specifically, although the Department had documented and approved an ISRMS, [Redacted] (b) (5) [redacted] According to Department officials, this occurred because the Department was waiting for the Department of Homeland Security to implement the Continuous Diagnostics and Mitigation solution, which the Department intends to inherit.

**(U)** In addition, although the Department documented and approved an ISCM strategy, the strategy was not fully implemented. Williams, Adley found that the Department had not established and implemented an [Redacted] (b) (5) [redacted]

**(U)** Overall, Williams, Adley identified control deficiencies in [redacted] [Redacted] (b) (5) [redacted] Without an effective information security program, the Department is vulnerable to attacks and threats.

OIG
Office of Inspector General
U.S. Department of State • Broadcasting Board of Governors

AUD-IT-16-16 | Office of Audits | November 2015

# (U) Audit of the Department of State Information Security Program

## INFORMATION TECHNOLOGY DIVISION

WILLIAMS ADLEY

Audit of the Department of State's Information Security Program

November 11, 2015

Office of Inspector General
U.S. Department of State and the Broadcasting Board of Governors
Washington, DC

Williams, Adley & Company-DC, LLP has performed an audit of the Department of State's (Department) information security program. We audited the Department's compliance with the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014; Office of Management and Budget requirements; and National Institute of Standards and Technology standards. We performed this audit under Contract No. SAQMMA15F0980. The audit was designed to meet the objectives described in the report.

We conducted this performance audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We communicated the results of our audit and the related findings and recommendations to the U.S. Department of State and the Broadcasting Board of Governors Office of Inspector General.

We appreciate the cooperation provided by the Department's personnel during the audit.

Williams, Adley & Company-DC, LLP

WILLIAMS, ADLEY & COMPANY-DC, LLP
*Certified Public Accountants / Management Consultants*
1030 15th Street, NW, Suite 300W • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

# (U) CONTENTS

# (U) OBJECTIVE

(U) The objectives of this audit were to assess the effectiveness of the Department of State's (Department) information security program and to determine whether security practices in FY 2015 complied with applicable laws, regulations, and information security standards established by the Federal Information Security Management Act of 2002 (FISMA),[1] as amended by the Federal Information Security Modernization Act of 2014;[2] the Office of Management and Budget (OMB); and the National Institute of Standards and Technology (NIST). Specifically, the audit assessed the Department's information security program and related practices for risk management and continuous monitoring, which would include configuration management, identity and access management, incident response and reporting, security training, plans of action and milestones (POA&M), remote access management, contingency planning, and contractor systems.[3]

# (U) BACKGROUND

(U) The Department is the U.S. Government's principal agency for advancing freedom for the benefit of the American people and the international community by helping to build and sustain a more democratic, secure, and prosperous world composed of well-governed states that respond to the needs of their people, reduce widespread poverty, and act responsibly within the international system. The Department's mission is carried out by geographic and functional bureaus that provide policy guidance, program management, administrative support, and in-depth expertise. The Department has an extensive overseas presence, with over 275 missions worldwide. Further, domestically the Department operates in numerous locations across the country.

(U) The Department, as well as its contractors, depends on information systems and electronic data to carry out essential mission-related functions. The security of these systems and networks is vital to protecting national and economic security, public health and safety, and the flow of commerce. As such, these information systems are subject to serious threats that can have adverse effects on organizational operations (that is, missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or the availability of information being processed, stored, and transmitted by those systems.

[1] (U) Public Law No. 107-347, Title III, Federal Information Security Management Act of 2002 (Dec. 2002).
[2] (U) Public Law No. 113-283, Federal Information Security Modernization Act of 2014 (Dec. 2014).
[3] (U) [redacted]

## (U) Risk Management

(U) Because of the risk posed to information systems, it is crucial that organizations take appropriate steps to secure information and information systems. To effectively manage risk to information, senior executives must be committed to making risk management a fundamental business requirement. This top-level executive commitment ensures that sufficient resources are available to develop and implement an effective organization-wide risk management program. In addition, senior executives must recognize that explicit, well-informed risk-based decisions are crucial in order to balance the benefits of using information systems against the risk of those same information systems being the channels through which attacks, environmental disruptions, or human errors cause business failures.

(U) To assist in making those explicit, well-informed risk-based decisions, a comprehensive process must be in place that requires the organization to do the following:

(U) (1) *Frame risk (that is, establish the context for risk-based decisions)*—The purpose of framing risk is to produce a risk management strategy that addresses how the organization intends to assess risk, respond to risk, and monitor risk. The frame establishes a foundation for managing risk and defines the boundaries for risk-based decisions within the organization. In addition, the risk-framing component and the associated risk management strategy also include any strategic-level decisions on how risk is to be managed by senior executives.

(U) (2) *Assess risk*—The purpose of assessing risk is to identify threats to the organization, vulnerabilities, the harm that may occur given the potential exploitation of those vulnerabilities, and the likelihood that consequences will occur. The end result is a determination of risk—that is, the degree of impact and likelihood of that impact occurring.

(U) (3) *Respond to risk*—The purpose of risk response is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by developing alternative courses of action, evaluating the alternative courses of action, determining appropriate courses of action consistent with organizational risk tolerance, and implementing risk responses based on selected courses of action.

(U) (4) *Monitor risk on an ongoing basis*—The purpose of risk monitoring is to verify that planned risk response measures are implemented and information security requirements derived from organizational business functions are satisfied, to determine the ongoing effectiveness of risk response measures after they have been implemented, and to identify risk-impacting changes to organizational information systems and the environments in which those systems operate. This monitoring leverages Information Security Continuous Monitoring (ISCM) activities, which provide awareness of threats, vulnerabilities, and the effectiveness of deployed security controls, to assist in making risk-based decisions.

(U) Based on these objectives, information security risk management must be a holistic activity that involves the entire organization. With all individuals directly influenced by the risk frame that is established by senior executives, organizational culture becomes a key factor in determining how risk is managed within an organization.

(U) Organizational culture refers to the values, beliefs, and norms that influence the behaviors and actions of the senior executives and individual members of organizations. As such, cultural influences and impacts affect all levels of the organization. Senior executives, both directly and indirectly, set the stage for how the organization responds to various approaches to managing risk. Senior executives establish the risk tolerance for organizations both formally (for example, through publication of strategy and guidance documents) and informally (for example, through actions that get rewarded and penalized, the degree of consistency in actions, and the degree of accountability enforced). The direction set by senior executives and the understanding of existing organizational values and priorities are major factors that determine how risk is managed within the organization.

## (U) Continuous Monitoring Program

(U) To assist in securing systems, federal agencies leverage ISCM activities, which provide awareness of threats, vulnerabilities, and the effectiveness of deployed security controls, to assist in making risk-based decisions from the organization and information systems perspectives. ISCM is intertwined with risk management at every level of the organization. Specifically, ISCM gives agency officials access to security-related information on demand and enables timely management, assessment, and response to security issues as part of an agency's information security risk management framework.

[Redacted] (b) (5)

To assist in achieving these objectives, security controls must be implemented consistently, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time at the information systems level so that they support the monitoring requirements at the organization and bureau levels. These information security controls at the information systems level are implemented through the following eight key FISMA reportable information security process areas:

- (U) Configuration Management—The purpose of configuration management is to manage the effects of changes or differences in configurations on an information system or network. Configuration management is an essential component of monitoring the status of security controls and identifying potential security-related problems in information systems. This information can help security managers understand and monitor the evolving nature of vulnerabilities as they appear in a

system under their responsibility, thus enabling managers to direct appropriate changes as required. The goal of configuration management is to make assets harder to exploit through better configuration.

- (U) Identity and Access Management—Users and devices must be authenticated to ensure that they are who or what they identify themselves to be. The purpose of identity and access management is to ensure that users and devices are properly authorized to access information and information systems.

- (U) Incident Response and Reporting—The purpose of incident response and reporting is to determine the kinds of attacks that have been successful and position the organization to make a risk-based decision about where it is most cost effective to focus its security resources. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations quickly.

- (U) Security Training—Establishing and maintaining a robust and relevant information security training process as part of the overall information security program is the primary conduit for providing a workforce with the information and tools needed to protect an agency's vital information resources. This will ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information and resources entrusted to them. Organizations that continually train their workforce in organizational security policy and role-based security responsibilities will have a higher rate of success in protecting information.

- (U) POA&Ms—The purpose of POA&Ms is to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. POA&Ms track the measures implemented to correct deficiencies and to reduce or eliminate known vulnerabilities. POA&Ms can also assist in identifying performance gaps, in evaluating an organization's security performance and efficiency, and in conducting oversight. POA&Ms are essential parts of the risk management process to track problems and to decide which issues to address, and they show an organization's efforts to address corrective action with a standard and centralized approach.

- (U) Remote Access Management—The purpose of remote access management is to help deter, detect, and defend against unauthorized network connections and/or access to internal and external networks. Secure remote access is essential to an organization's operations because the proliferation of system access through telework, mobile devices, and information sharing means that information security is no longer confined within system perimeters. According to the Office of Management and Budget's Annual Report to Congress, "Organizations also rely on

remote access as a critical component of contingency planning and disaster recovery."[4]

- (U) Contingency Planning—Contingency planning involves the actions required to plan for, respond to, and mitigate damaging events. As such, the primary purpose of contingency planning is to give attention to rare events that have the potential for significant consequences and promoting first priority risk.

- (U) Contractor Systems—The purpose of contractor systems is to ensure that information systems operated by contractors and other external entities on behalf of the Federal Government meet all applicable security requirements.

## (U) Federal Information Security Management Act

(U) FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that support Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

(U) FISMA assigns specific responsibilities to NIST, OMB, and the Department of Homeland Security (DHS)[5] for the purpose of strengthening information system security throughout the Federal Government. In particular, FISMA requires the head of each agency to implement policies and procedures to cost effectively reduce IT security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, chief information officers (CIO), chief information security officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to DHS.

(U) In an effort to improve Federal cybersecurity, the Federal Information Security Modernization Act of 2014, which amended FISMA, was enacted on December 18, 2014. The act served to clarify and strengthen information security roles and responsibilities for OMB and DHS, placed an emphasis on assessing effectiveness, and reiterated the requirement for Federal agencies to develop, document, and implement an organization-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor.

---

[4] (U) OMB, "Annual Report to Congress: Federal Information Security Management Act," <https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf>, accessed on September 16, 2015.

[5] (U) OMB Memorandum M-10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland," https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf >, accessed on September 23, 2015.

**(U)** To assist agencies in implementing the requirements of FISMA, OMB and DHS annually issue metrics[6] providing guidance to agencies and OIG on how to meet FISMA evaluation and reporting requirements. Appendix F presents the 10 FISMA reportable areas for FY 2015.

### (U) *Continuous Monitoring Maturity Model*

**(U)** As part of the updated FY 2015 DHS FISMA reporting metrics, dated June 19, 2015, the Council of the Inspectors General on Integrity and Efficiency, DHS, OMB, NIST, and other stakeholders developed a maturity model for the continuous monitoring domain to provide perspective on the overall status of information security within an agency. The purposes of the Council of Inspectors General on Integrity and Efficiency maturity model, shown in Appendix D, are the following:

- **(U)** To summarize the status of agencies' information security programs and their maturity on a 5-level scale.
- **(U)** To provide transparency to agency CIOs, top management officials, and other interested readers of OIG FISMA reports about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level.
- **(U)** To help ensure consistency across the OIGs in their annual FISMA review.

## (U) AUDIT RESULTS

~~(SBU)~~ Overall, Williams, Adley & Company-DC, LLP (Williams, Adley), identified [redacted] While the Department had taken some action[8] to improve its information security program, Williams, Adley continued to find that the Department was not in compliance with FISMA, OMB, and NIST requirements. Specifically, Williams, Adley found that the Department had [redacted] as defined by [Redacted] (b) (5)

[6] **(U)** DHS, FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics, June 2015.
[7] **(U)** Williams, Adley [redacted]
[8] **(U)** Examples include that the Department took actions to implement products and tools designed to control administrator privileges, improving current software, and initiating Information Systems Security Officer and system owner role-based training courses.
[9] **(U)** OMB Memorandum M-14-04, "FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf>, accessed on October 20, 2015.

## (U) Finding A: [Redacted] (b) (5)

~~(SBU)~~ Williams, Adley found that the Department had [Redacted] (b) (5) [redacted]. In addition, the CIO is not properly positioned within the organization to ensure that the Department's information security program is effective. For example, the Bureau of Diplomatic Security (DS) and other bureaus and offices are not required to communicate information security risks to the CIO. [redacted]

**(U)** According to NIST Special Publication (SP) 800-39,[11] effectively managing information security risk organization-wide requires the following key elements:

- **(U)** Assignment of risk management responsibilities to senior leaders/executives.
- **(U)** Ongoing recognition and understanding by senior leaders/executives of the information security risks to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.
- **(U)** Establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization including guidance on how risk tolerance impacts ongoing decision-making activities.
- **(U)** [Establishing] accountability by senior leaders/executives for their risk management decisions and for the implementation of effective, organization-wide risk management programs.

**(U)** NIST SP 800-39 goes on to say that managing information security risk requires the involvement of the entire organization defined in three tiers, from senior leaders providing the strategic vision and top-level goals and objectives for the organization; to bureau leaders planning, executing, and managing projects; to system owners operating the information systems supporting the organization's business functions.

~~(SBU)~~ Using the approach described in the Federal Information Security Modernization Act of 2014, Williams, Adley assessed whether the Department established and implemented an

[10] **(U)** According to DHS, Continuous Diagnostics and Mitigation provides Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the Continuous Diagnostics and Mitigation program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. Site <www.dhs.gov/cdm>, accessed on September 29, 2015.
[11] **(U)** NIST SP 800-39.

effective organization-wide risk management program at all levels of the organization (that is organization level, bureau level, and information systems level). At the organizational level, the Department had documented and approved an Information Security Risk Management Strategy[12] (ISRMS) in May 2014; however, [redacted]

[Redacted] (b) (5)

~~(SBU)~~ Williams, Adley also found that although the ISRMS[14] states that "Office of Management Policy, Rightsizing and Innovation is leading efforts in establishing an enterprise risk management program in which IT system risk is an input," these roles and responsibilities are not clearly documented in the Foreign Affairs Manual (FAM).[15]

**(U)** In addition, at the information systems level, Williams, Adley found that the Department had not effectively managed risk for all phases of the system development lifecycle, which Williams, Adley has reported annually since FY 2010. For example, the Department had [redacted]

[12] **(U)** IRM ISRMS, May 2014.
[13] **(U)** Ibid.
[14] **(U)** Ibid.
[15] **(U)** 1 FAM 040, "The Under Secretaries of State," June 2011.

officials to incorporate into the risk-based decisionmaking process in support of the business mission. Specifically, the Department's [Redacted] (b) (5) comprises the following:

[Redacted] (b) (5)

**(U)** The FAM[16] states, "All systems (including applicable contractor systems) and applications associated with any projects must be registered in the Information Technology Applications Baseline."[17] However, Williams, Adley found that the Department's [Redacted] (b) (5) Therefore, Williams, Adley could not assess the ATO status of all the Department's information systems as a key [Redacted] (b) (5) Specifically, Williams, Adley found the following:

- ~~(SBU)~~ For FISMA reportable systems that received an ATO in FY 2015, the Department provided two different system inventory lists from two separate dates. One list, provided on April 17, 2015, [Redacted] (b) (5) However, the other list, provided on April 22, 2015, The Department also [Redacted] (b) (5) in accordance with 5 FAM 1110.[18]
- ~~(SBU)~~ Although the Department acquired the [Redacted] (b) (5) for performing discovery scans,[19] the Department [Redacted] (b) (5)

[16] **(U)** 5 FAM 600, "Information Technology Systems," June 2009.
[17] **(U)** Information Technology Applications Baseline is now referred to as iMATRIX.
[18] **(U)** 5 FAM 1110, "Cloud Computing," September 2013.
[19] **(U)** Per NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," September 2008, network discovery uses a number of methods to identify active and responding hosts on a network, identify weaknesses, and learn how the network operates.

[redacted] System owners can add and remove devices from the network without communicating the information to IRM, which is responsible for managing [Redacted] (b) (5) [redacted]

- ~~(SBU)~~ The Department [redacted] in accordance with [Redacted] (b) (5)
- **(U)** The Department did not have Standard Operating Procedures documenting the processes and procedures for managing [redacted]
- ~~(SBU)~~ [Redacted] (b) (5) [redacted] FISMA reportable systems and [Redacted] (b) (5) [redacted] classification FISMA reportable systems, demonstrating that systems may have operated [Redacted] (b) (5) during FY 2015. [redacted]
- **(U)** Although the Department's Cyber Security Assessment tool [redacted] was tested and deemed functional on June 9, 2015, [Redacted] (b) (5) [redacted]. Since the tool had not been fully implemented, the Department was still following the old POA&M processes with many of the same deficiencies.

**(U)** One overall cause of the weaknesses Williams, Adley identified is that the CIO is not properly positioned within the organization to ensure that the Department's information security program is effective. OMB's 25 Point Implementation Plan to Reform Federal IT

---

[20] **(U)** NIST Interagency Report 7298, rev. 2, "Glossary of Key Information Security Terms," May 2013, states that a [redacted] [Redacted] (b) (5) [redacted]

[21] **(U)** Per NIST SP 800-44, rev. 2, "Guidelines on Securing Public Web Servers," September 2007, [Redacted] (b) (5) [redacted]

[22] **(U)** Per Techopedia, a [Redacted] (b) (5) [redacted] accessed on October 1, 2015.

[23] **(U)** 5 FAM 600.

[24] **(U)** [redacted]

[25] **(U)** 5 FAM 600.

[26] **(U)** Federal Information Processing Standard Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004, states that [Redacted] (b) (5) [redacted]

[27] **(U)** [Redacted] (b) (5) will be used to document and track artifacts related to the A&A process.

Management[28] states that the CIO must be positioned with certain responsibilities and authorities to effectively manage IT programs throughout the Department. The IT Reform Plan clarifies the primary areas of responsibility for agency CIOs to have a lead role in, in addition to their statutory responsibilities through the Clinger-Cohen Act.[29] Specifically, the IT Reform Plan states that the CIO should have lead roles in information security and governance.

**(U)** Under the Department's current organizational reporting structure, the CIO of the Department, who is the head of IRM, reports to the Under Secretary for Management. In addition, DS reports separately to the Under Secretary for Management. However, according to Department guidance,[30] IRM and DS both have statutory responsibilities for information security. Furthermore, under this reporting structure, DS and any other bureaus or offices reporting to the Under Secretary for Management are not required to communicate information security risks to IRM. To enhance the CIO's position in relation to information security, OMB Memorandum M-11-29 states that CIOs or senior agency officials reporting to the CIO should have the authority and primary responsibility to implement an agency-wide information security program.

**(U)** To achieve its core missions, Department personnel must be able to access information systems at any time and from any location—domestic and abroad. The Department's information systems and sensitive information rely on the confidentiality, integrity, and availability of its comprehensive and interconnected systems utilizing various technologies around the globe. Managing information security risk effectively throughout the organization is critical to achieving this mission successfully. However, without a centralized approach to communicating information security risks, the Department cannot have an effective risk management program, and the consequence of that ineffectiveness can impact all levels of the organization. For example, at the organizational level, the Department is vulnerable to attacks and threats.

**(U)** Further, bureaus could potentially miscommunicate information security risks to leadership, which could increase the likelihood and impact of potential attacks. In addition, without centralized guidance, each bureau could have a different perspective on what constitutes risk and how to manage risk. This directly obstructs an understanding of how bureau-level information security risks contribute to Department-wide risk. Furthermore, bureaus may accept risks associated with one mission or business function without understanding the potential effect on other mission and/or business functions. [redacted] in the February report from the National Security Agency's (NSA) Department of State Mitigations Analysis,[31] which stated that

[28] **(U)** OMB Memorandum M-11-29, "Chief Information Officer Authorities," <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf>, accessed on September 15, 2015.
[29] **(U)** Public Law No. 104-106, Division E, Clinger-Cohen Act of 1996 (February 1996).
[30] **(U)** IRM and DS Cyber Security Roles, October 2003.
[31] **(U)** NSA, Department of State Mitigations Analysis, February 2015.

[redacted]

**(U)** In addition, without a sufficient risk management program, system owners cannot appropriately prioritize resources to manage information security risks to protect information systems and sensitive data from attacks and threats. For example, new vulnerabilities discovered in an information system may have systemic implications that extend Department-wide. Those same vulnerabilities may trigger changes to the organizational information security architecture or may require an adjustment to the organizational risk tolerance.

**~~(SBU)~~** The lack of a [redacted] For example, as reported in the media in August 2015, a hacked Department email account led to months-long attacks against the White House and the Department.[33] Further, as [redacted].

**Recommendation 1: (U)** OIG recommends that the Chief Information Officer amend the [redacted] in accordance with National Institute of Standards and Technology Special Publication 800-39.

**(U) Management Response:** IRM concurred with this recommendation. IRM stated that it has developed and shared the Information Security Risk Management Strategy with OIG and plans to use the feedback provided to amend the strategy as appropriate (see Appendix G).

**(U) OIG Reply:** OIG considers this recommendation resolved because IRM agreed to implement it. This recommendation will be closed when [redacted] in accordance with NIST SP 800-39.

**Recommendation 2: (U)** OIG recommends that the Deputy Secretary of State for Management and Resources review the organizational placement of the Chief Information

[32] **(U)** U.S. Department of State Cybersecurity Strategy, August 2015.
[33] **(U)** Nextgov, <http://www.nextgov.com/cybersecurity/2015/08/common-malware-jimmied-open-white-house-and-anthem-systems-say-researchers/119085/?oref=dropdown#> accessed on August 17, 2015.
[34] **(U)** *Audit of the Department of State Information Security Program* report, AUD-IT-15-17, November 2014.

Officer (CIO), with respect to the Clinger-Cohen Act and Office of Management and Budget Memorandum M-11-29 and make a determination as to whether the CIO should be realigned within the Department of State's (Department) organizational structure to carry out the CIO's lead role in managing information security for the Department.

**(U) Management Response:** The Deputy Secretary for Management and Resources concurred with this recommendation (see Appendix H).

**(U) OIG Reply:** OIG considers the recommendation resolved because the Deputy Secretary agreed to review the organizational placement of the CIO and make a determination as to whether the CIO should be realigned within the Department's organizational structure to carry out the CIO's lead role in managing information security for the Department. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the Deputy Secretary of State for Management and Resources has made a determination regarding the organizational placement of the CIO in consideration of the Clinger-Cohen Act and OMB Memorandum M-11-29.

## ~~(SBU)~~ Finding B: The Department [Redacted] (b) (5)

~~(SBU)~~ Williams, Adley found that the Department did not have an [redacted] Specifically, Williams, Adley identified deficiencies in [redacted] Without an [Redacted] (b) (5), the Department cannot fully and effectively execute its overall organization-wide information security program [Redacted] (b) (5)

**(U)** Using the approach described in the Federal Information Security Modernization Act of 2014, Williams, Adley assessed whether the Department established and implemented an [redacted] At the organizational level, the Department documented and approved [redacted] in May 2014; however, [Redacted] (b) (5) [redacted]. Overall, Williams, Adley found that the Department had [Redacted] (b) (5) [redacted]

[Redacted] (b) (5) [redacted]

[Redacted] (b) (5) Specifically, at the organization and bureau levels, the Department did not do the following:

[redacted]

**(U)** The Department, in coordination with NSA, took actions such as implementing products and tools designed to control administrator privileges, improving current software, segregating the network,[40] and performing network discovery scans to address deficiencies. The Department has also taken actions to improve its security training process by initiating Information Systems Security Officer and system owner role-based training courses. In addition, the Department has improved its remote access management process, and Williams, Adley did not find any deficiencies within that process during the FY 2015 audit. However, during this audit, Williams,

[36] **(U)** Per 5 FAM 100 "Information Technology (IT) Management," July 2013, [redacted]

[37] **(U)** Per 5 FAM 870, "Networks," September 2014, [redacted]

[38] **(U)** OMB Circular A-130, "Management of Federal Information Resources," [redacted]

[39] [redacted].

[40] **(U)** Per NSA, "Segregating the Network," properly segregated networks contain completely separate infrastructure for each functional area within an organization. This includes providing separate servers, storage devices, routers, and switches for different areas of varying sensitivity and access. Site <https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_SegregatingNetworksAndFunctions_Web.pdf > accessed on September 28, 2015.

Adley continued to find security control deficiencies at the information systems level. Since FY 2010, Williams, Adley has cumulatively tested [Redacted] (b) (5) systems (see Appendix C for systems tested since 2010) and identified similar control deficiencies throughout our audits, which Williams, Adley believes is indicative of a systemic problem within the Department. In FY 2015, Williams, Adley identified the deficiencies described. :

## (U) Configuration Management

~~(SBU)~~ The Department had not implemented [redacted] for all of its systems. Williams, Adley found that the CIO had not finalized and [redacted] for all systems and applications. Furthermore, Williams, Adley identified the following:

- ~~(SBU)~~ The CIO, in coordination with DS's Security Infrastructure Directorate, Office of Computer Security, [redacted] the following components for compliance and vulnerabilities:

[redacted]

[41] **(U)** Per Investopedia, [redacted]

[42] **(U)** Per NIST SP 800-115, [redacted]

[43] **(U)** Per TechTarget, a [redacted]

[44] **(U)** Per NIST SP 800-115, [redacted]

[45] **(U)** NIST SP 800-115 [Redacted] (b) (5)

- ~~(SBU)~~ Although the Department [redacted] to identify and monitor vulnerabilities, of [redacted] systems[47] tested, Williams, Adley found the Department had not remediated [redacted] high-risk vulnerabilities and [redacted] medium-risk vulnerabilities. [redacted]
- (U) Of 22 deviations[50] tested, system owners had not followed the appropriate risk acceptance process for [redacted] (77 percent) deviations, in accordance with [redacted] Specifically, system owners had not done the following:
  - (U) Acknowledged and returned risk acceptance documentation within the allotted time (30 days) for [redacted] (76 percent) deviations.
  - (U) Documented an official memorandum accepting the associated risks for [redacted] (24 percent) deviations.

## (U) Identity and Access Management

- ~~(SBU)~~ Of [redacted] administrator accounts[52] sampled [redacted] system owners did not provide elevated access request forms[54] for [redacted] (23 percent) administrative users [redacted] as required by 12 FAM 620.[55]

[redacted]

[48] (U) Per TechNet, vulnerability ratings range from low to critical. A critical vulnerability is defined as a vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (for example, network worms) or unavoidable common use scenarios where code execution occurs without warnings or prompts. Microsoft recommends that customers apply critical updates immediately. Site <https://technet.microsoft.com/en-us/security/gg309177.aspx> accessed on October 1, 2015.

[49] (U) Williams, Adley notified DS of the identified vulnerabilities on June 30, 2015.

[50] (U) Product Lifecycle Management states that a deviation is a specific written authorization to depart from a particular requirement of an item's current approved configuration documentation for a specific number of units or a specified period of time. Site <http://www.product-lifecycle-management.com/mil-hdbk-61a-6-3.htm> accessed on October 1, 2015.

[51] (U) 5 FAM 1060.

[52] (U) Per NIST Interagency Report 7298, rev. 2, an administrative account is a user account with full privileges on a computer.

[53] (U) Per 5 FAM 870, [redacted]

[54] (U) Elevated access request forms are required prior to creating administrator accounts.

[55] (U) 12 FAM 620, "Unclassified Automated Information Systems," August 2008.

- **(U)** System owners had not provisioned[56] user accounts consistently for [redacted] accounts.[58] Specifically,
  - ~~(SBU)~~ Of [redacted] separated user accounts tested, [redacted] (18 percent) were enabled after the termination of the employee. Of the [redacted] user accounts that were enabled after user separation,[59] [redacted] (50 percent) were accessed after the separation date.[60]
  - **(U)** Of [redacted] new user accounts tested [Redacted] (b) (5) the Department was unable to provide new user account request forms for 7 (32 percent) accounts.
  - **(U)** Of [redacted] mailbox accounts tested, [redacted] (9 percent) mailbox accounts had not been assigned a primary user account to manage them as required.[61]
- **(U)** For systems that reside on [redacted], system owners had not done the following:
  - ~~(SBU)~~ Changed passwords [Redacted] (b) (5) for [redacted] of [redacted] accounts[63] (3 percent), as required by 12 FAM 620.
  - ~~(SBU)~~ Disabled accounts after 90 days of inactivity for [redacted] of [Redacted] (b) (5) accounts (7 percent), as required by the Foreign Affairs Handbook.[65]
  - ~~(SBU)~~ Configured accounts to require passwords for [redacted] of [redacted] accounts (less than one percent).
  - ~~(SBU)~~ Set passwords to expire for [Redacted] (b) (5) [redacted] accounts (less than 1 percent).

---

[56] **(U)** Per NIST Interagency Report 7657, "A Report on the Privilege (Access) Management Workshop," March 2010, provisioning refers to defining the attributes and policies, including semantics and representations, and instantiating them.

[57] **(U)** Per TechNet, [redacted]

[58] **(U)** Williams, Adley sampled three different populations of accounts: separated users (that is, transferring or terminated users), new users, and mailbox accounts. Per the Department of State Global Address List (GAL) and AD Standardization, in AD, it is necessary to have an individual account assigned to mailbox accounts, September 2014.

[59] **(U)** An IRM official stated that the list of separated users provided by the Bureau of Human Resources did not distinguish between users who were transferring and users who were terminated from employment. Accounts are deleted for users who are terminated; however, based on the Department's policy, since these users are on the Bureau of Human Resources separated users list, all separated users (terminated or transferred) should be disabled.

[60] **(U)** [redacted]

[61] **(U)** GAL guidelines aid account administration across the enterprise.

[62] **(U)** This number reflects enabled accounts as of May 20, 2015, when Williams, Adley received the [redacted] listing.

[63] **(U)** [redacted] accounts consist of user accounts, mailbox accounts, and service accounts. The GAL states that mailbox accounts are certain business units in the Department that are monitored and managed by multiple primary user accounts. These accounts are delegated certain access to the shared mailbox. Further, a service account is usually a Windows account that the operating system process uses when it hosts a service, and is configured by an administrative account holder.

[64] **(U)** This number reflects enabled accounts as of May 20, 2015, when Williams, Adley received the AD listing.

[65] **(U)** 12 Foreign Affairs Handbook-10 H-100, "Unclassified/SBU Information System Security Technical Controls," Sept.2014.

- **(U)** For systems that reside on [redacted] system owners had not done the following:
  - ~~(SBU)~~ Disabled accounts after 90 days of inactivity for [redacted] accounts (5 percent), as required by 12 FAM 630.[67]
  - ~~(SBU)~~ Configured accounts to require passwords for [redacted] accounts (less than one percent).

## (U) Incident Response and Reporting

**(U)** Williams, Adley performed a separate effort focused on the operating effectiveness of the Department's incident response and reporting process area. While this effort will be reported separately, Williams, Adley [redacted] In addition, although the Department established required cyber security incident response and reporting policies and procedures, it did not consistently comply with prescribed categorization guidelines, reporting requirements, and remediation timelines.

## (U) Security Training

**(U)** Although the Department took actions to address previously identified security training weaknesses by initiating Information Systems Security Officer and system owner role-based training courses in FY 2015, the Department had not implemented an effective security training process, as demonstrated in the following information:

- **(U)** For [redacted] tested users with significant security responsibilities for the Department, [redacted] (77 percent) had not taken specialized role-based security training.
- **(U)** DS had not fully implemented a tracking mechanism for employees who had taken the required role-based training.
- **(U)** Users with only [redacted] access, who do not have [redacted] access, were not required to take the security training course.[68]
- **(U)** For [redacted] new [redacted] and [redacted] user accounts tested, [redacted] (43 percent) new users did not complete the required training within 10 days, as required by the Cybersecurity Awareness and Training Program.[69]
- **(U)** For [redacted] existing [redacted] and [redacted] user accounts tested, [redacted] (41 percent) users did not complete the training annually as required by the Program.[70]

[66] **(U)** This number reflects enabled accounts as of May 20, 2015, when Williams, Adley received the AD listing.
[67] **(U)** 12 FAM 630, "Classified Automated Information Systems," April 2014.
[68] **(U)** Users did not have an [redacted] account; however, users still had access to classified information through [redacted] thereby increasing the risk of a loss of information, the compromise of personally identifiable information, and the introduction of vulnerabilities to systems.
[69] **(U)** Cybersecurity Awareness and Training Program, October 2014.
[70] **(U)** Ibid.

## (U) POA&Ms

~~(SBU)~~ For each year from FY 2010 to FY 2015, the Department had not consistently identified, assessed, prioritized, and monitored the progress of corrective actions for identified security deficiencies. In addition, management of the POA&Ms process continues to be ineffective and does not capture necessary elements for remediation. System owners have also failed to follow the Department's policy for completing all necessary elements of a POA&M (see Table 5 in Appendix E). For systems that reside on [redacted], Williams, Adley found the following:

- **(U)** System owners and IRM's Office of Information Assurance were unable to provide evidence of remediation efforts for [redacted] (14 percent) of [redacted] POA&Ms closed in FY 2015.
- **(U)** System owners did not adhere to established completion dates for POA&Ms. Specifically, of [redacted] POA&Ms closed in FY 2015, [redacted][71] (45 percent) exceeded the scheduled completion date by 90 or more days.
- **(U)** Of [redacted] POA&Ms closed in FY 2015, [redacted] (5 percent) did not have a scheduled completion date.[72]
- **(U)** System owners had not consistently updated all POA&Ms fields. Specifically,
  - **(U)** Of [redacted] POA&Ms closed in FY 2015, [redacted] (44 percent) did not have budgeted resources identified.
    - **(U)** Of [redacted] POA&Ms closed in FY 2015, [redacted] (20 percent) had not recorded Unique Investment Identifiers (UII).[73] Specifically,
      - **(U)** [redacted] actions (9 percent) had been reported as "No Major Investment."[74]
      - **(U)** [redacted] (2 percent) had been reported as "Not Provided."[75]
      - **(U)** [redacted] (10 percent) had not populated UII fields (fields were left blank).
- **(U)** Quarterly POA&M reports to the CIO were not produced during Quarter 1 and Quarter 2 of FY 2015.
- ~~(SBU)~~ IRM's Office of Information Assurance, in conjunction with system owners, had not recorded and tracked all identified security deficiencies. Specifically,

---

[71] **(U)** The delays ranged from 105 to 1,128 days.

[72] **(U)** The Department's POA&M Toolkit states that it is necessary to have a scheduled completion date field for POA&Ms so that system owners may update the field to reflect estimations for POA&M completion. POA&M Toolkit site at <http://irm.m.state.sbu/sites/ia/SiteDirectory/poams/Pages/default.aspx>, accessed on Sept. 28, 2015.

[73] **(U)** Per OMB's "Guidance on Exhibits 53 and 300 – Information Technology and E-Government," a UII refers to a persistent numeric code applied to an investment that allows the identification and tracking of an investment across multiple fiscal years of an agency's investment portfolio. Site https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy14_guidance_on_exhibits_53_and_300.pdf, accessed on September 23, 2015.

[74] **(U)** In the POA&M database, the Department filled these 35 UII fields with this particular wording instead of a required UII.

[75] **(U)** In the POA&M database, the Department filled these eight UII fields with this particular wording instead of a required UII.

- (U) Although the Department was tracking findings identified in the FY 2014 report *Audit of the Department of State Information Security Program* [76] within its corrective action plan,[77] the Department did not incorporate any of the findings in the POA&M database.
- (U) The POA&M database excluded findings from DS's vulnerability assessments. An IRM official stated that the Department uses iPost to track vulnerability assessment results instead of incorporating any outstanding vulnerabilities into the master POA&M database.

## (U) Remote Access Management

(U) Williams, Adley performed testing on the Department's remote access management process to determine whether users with active remote access tokens were enrolled in the required Mobile Computing Management System[78] prior to gaining access to [Redacted] (b) (5).[79] Williams, Adley selected a sample of [Redacted] (b) (5) remote users and did not identify any deficiencies in the Mobile Computing Management System enrollment process for those [redacted] sampled users.

## (U) Contingency Planning

(U) The Department had not fully documented and implemented its information system contingency plans in accordance with the FAM. Additionally, system owners, in coordination with IRM's Office of Information Assurance, did not develop information system contingency plans in accordance with the FAM,[80] NIST SP 800-34, rev. 1,[81] and NIST SP 800-53, rev 4.[82] Specifically, Williams, Adley found that the Department had not done the following:

- (U) Included [Redacted] (b) (5) procedures[83] in the contingency plan testing for [Redacted] (b) (5) (13 percent) systems sampled.
- (U) Provided approval by system owners for information system contingency plans for [Redacted] (b) (5) [Redacted] (b) (5) (75 percent) systems tested.

[76] (U) AUD-IT-15-17, November 2014.
[77] (U) Department of State IT Security Corrective Action Plan for FY 2015, August 2015.
[78] (U) Per,12 FAM 680, "Remote Access and Mobile Computing Technology," November 2014, the Mobile Computing Management System is the [Redacted] (b) (5) enrollment system.
[79] (U) [redacted] is the Department's approved remote access system.
[80] (U) 6 FAM 400, "General Services and Domestic Emergency Management," June 2012.
[81] (U) NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information System," May 2010.
[82] (U) NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organization," January 2014.
[83] (U) NIST SP 800-53, rev. 4, states that [redacted]

- **(U)** Documented contingency plans that established alternate storage sites, alternate processing sites, or alternate telecommunication sites for [redacted] (13 percent) systems tested.
- **(U)** Performed business impact analyses for [redacted] (38 percent) systems tested.
- **(U)** Consistently conducted weekly backups for [redacted] (50 percent) systems tested.
- **(U)** Provided approval by the Bureau's Assistant Secretary, or equivalent, for [redacted] (67 percent) Bureau Emergency Action Plans tested, as required by 6 FAM 400.[84]

## (U) Contractor Systems

**(U)** Again in FY 2015, Williams, Adley found that the Department had not followed policies and procedures for managing its Government and contractor extensions.[85] Specifically,

- ~~**(SBU)**~~ Of [redacted] Government and contractor extensions, [redacted] (36 percent) were not documented [redacted], which is the Department's official system of record for documenting extensions. In addition, all cloud services were not contained within [redacted] and were operating without being validated for Federal Risk and Authorization Management Program[87] certification.[88]
- **(U)** Of [redacted] extensions sampled [redacted] (60 percent) did not have a physical inspection by the annual inspection date, as required by 5 FAM 1060.[89]
- **(U)** Of the [redacted] Government extensions sampled, [redacted] (34 percent) Government extension did not have a completed Memorandum of Agreement, as required by 5 FAM 1060.[90]

**(U)** [redacted] Based on NIST SP 800-137 guidance, an effective risk management framework, in support of its core mission and business processes, must establish how ISCM activities[91] are incorporated into the risk-based decisions made throughout an organization. However, the Department had not fully established and [redacted] To establish how ISCM activities

[84] **(U)** 6 FAM 400.
[85] **(U)** Contractor and Government extensions, including third-party vendors, are Department [redacted] systems located at the contractor or Government facility.
[86] ~~**(SBU)**~~ [redacted]
[87] **(U)** The U.S. General Service Administration' website states that FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Site <http://www.gsa.gov/portal/category/102371> accessed on Sept. 28, 2015.
[88] **(U)** Williams, Adley was provided with a preliminary inventory of cloud systems on May 11, 2015, that, according to an IRM official, had not been validated for FedRAMP.
[89] **(U)** 5 FAM 1060.
[90] **(U)** Ibid.
[91] **(U)** Per NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organization," September 2011, ISCM activities include security controls, security status, and other metrics defined and monitored by Department leadership.

are incorporated into risk-based decisions made throughout an organization, criteria for those activities must be established. NIST SP 800-137states, "The criteria for ISCM are defined by the organization's risk management strategy, including how the organization plans to assess, respond to, and monitor risk, and the oversight required to ensure that the risk management strategy is effective." Furthermore, "Security controls, security status, and other metrics defined and monitored by officials at this tier are designed to deliver information necessary to make risk management decisions in support of governance." However, the Department did [redacted]

**(U)** Leveraging [redacted] activities effectively to make risk-based decisions throughout the organization is critical to achieving the Department's core missions. [Redacted] (b) (5) [redacted]

**(U)** The Council of the Inspectors General on Integrity and Efficiency ISCM Maturity Model for FY 2015 Federal Information Security Management Act[93] states that an established and implemented ISCM program defines how ISCM information will be shared with senior officials. [redacted]

[92] **(U)** Per NIST SP 800-137, [redacted]

[93] **(U)** DHS, FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics, June 2015.

[94] **(U)** U.S. Department of State Cybersecurity Strategy, August 2015.

[Redacted] (b) (5)

(U) Further, the [Redacted] (b) (5) are evident from the continued identification of many of the same control deficiencies in key information security process areas[Redacted] (b) (5) Specifically, Williams, Adley continued to find the same systemic and pervasive information security weaknesses across its IT security posture since FY 2010. These key information security process areas have a direct impact on an effective [Redacted] (b) (5) For example,

[Redacted] (b) (5)

- (U) Without appropriate training and tracking of all personnel with access to Department systems, including IT personnel with specific security responsibilities, users could compromise the security of the network, resulting in a loss of information; compromise of Personally Identifiable Information; and the introduction of vulnerabilities to systems.
- (U) Without adequate identification, assessment, prioritization, and monitoring of corrective actions on an enterprise basis, the most important actions (highest security risks) affecting the Department may not be fully funded, resolved within a timely manner, or communicated to senior management, thus exposing the Department's sensitive data, systems, and hardware to unauthorized access and potentially malicious attacks.
- ~~(SBU)~~

[95] (U) Nextgov,

[96] (U) AUD-IT-15-17, November 2014.

[redacted]

- (U) By not following Department policies for Government and contractor extensions, the Department has minimal assurance that the [redacted] In addition, there is an increased risk that the Department's data that is collected and processed may be exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

**Recommendation 3:** (U) OIG recommends that the Chief Information Officer, with input from the Information Security Steering Committee, [redacted]

**(U) Management Response:** IRM concurred with this recommendation. IRM stated that the overall risk management plan is being addressed by the Office of Management Policy, Rightsizing, and Innovation. IRM plans to continue to support the Office of Management Policy, Rightsizing, and Innovation in this effort and will work to further develop and refine its risk management approach for the Department's bureau-owned information systems.

**(U) OIG Reply:** OIG considers the recommendation resolved because IRM agreed to implement it. This recommendation will be closed when OIG [redacted]

**Recommendation 4:** (U) OIG recommends that the Chief Information Officer define and implement th [redacted]

**(U) Management Response:** IRM concurred with this recommendation. IRM stated that the Department is in the implementation stage of its multi-year collaboration with DHS to expand its implementation of continuous monitoring. The kickoff meeting with DHS and their contractor was held in October 2015.

**(U) OIG Reply:** OIG considers this recommendation resolved because IRM agreed to implement it. This recommendation will be closed when OIG [Redacted] (b) (5) [redacted]

# (U) RECOMMENDATIONS

**Recommendation 1: (U)** OIG recommends that the Chief Information Officer amend the [redacted] in accordance with National Institute of Standards and Technology Special Publication 800-39.

**Recommendation 2: (U)** OIG recommends that the Deputy Secretary of State for Management and Resources review the organizational placement of the Chief Information Officer (CIO), with respect to the Clinger-Cohen Act and Office of Management and Budget Memorandum M-11-29 and make a determination as to whether the CIO should be realigned within the Department of State's (Department) organizational structure to carry out the CIO's lead role in managing information security for the Department.

**Recommendation 3: (U)** OIG recommends that the Chief Information Officer, with input from the Information Security Steering Committee, [redacted]

**Recommendation 4: (U)** OIG recommends that the Chief Information Officer define and implement the [redacted]

# (U) APPENDIX A: SCOPE AND METHODOLOGY

**(U)** In order to fulfill its responsibilities related to the Federal Information Security Management Act of 2002 (FISMA),[1] the OIG, Office of Audits, contracted with Williams, Adley & Company-DC, LLP (Williams, Adley), an independent public accountant, to assess the effectiveness of the Department's information security program and to determine whether security practices in FY 2015 complied with applicable laws, regulations, and information security standards established by FISMA,[2] as amended by the Federal Information Security Modernization Act of 2014;[3] the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). Specifically, the audit assessed the Department's information security program and related practices for risk management and continuous monitoring, which would include configuration management, identity and access management, incident response and reporting, security training, plans of action and milestones , remote access management, contingency planning, and contractor systems.[4]

**(U)** FISMA, as amended by the Federal Information Security Modernization Act of 2014, requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or another source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency's inspector general or an independent external auditor to perform annual reviews of the information security program and to report those results to OMB and the Department of Homeland Security. The FY 2015 FISMA guidance from Department of Homeland Security is intended to assist OIGs in reporting FISMA performance metrics. The updated FY 2015 Department of Homeland Security FISMA reporting metrics, dated June 19, 2015,[5] include the Council of Inspectors General on Integrity and Efficiency maturity model (see Appendix D) for the continuous monitoring domain to provide perspective on the summary of the status of the agencies information security continuous monitoring program on a five-level scale.

**(U)** Williams, Adley performed this audit from April through August 2015. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that Williams, Adley plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Williams, Adley believes that the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objective.

---

[1] **(U)** Public Law L. No. 107-347, Title III, Federal Information Security Management Act of 2002 (December 2002).
[2] **(U)** Ibid.
[3] **(U)** Pub. Law No. 113-283, Federal Information Security Modernization Act of 2014 (December 2014).
[4] **(U)** Although risk management is a part of continuous monitoring, because of the nature of the risk management deficiency, we have made the deficiency a separate finding for risk management.
[5] **(U)** Department of Homeland Security, FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics, June 2015.

**(U)** To perform this audit, Williams, Adley interviewed Department senior management, employees, and contractors to evaluate managerial effectiveness and operational controls in accordance with NIST and OMB guidance. Williams, Adley observed daily operations, obtained evidence to support its conclusions and recommendations, tested the effectiveness of established controls, sampled where applicable, and collected written documents to supplement observations and interviews. In addition, Williams, Adley reviewed system-generated outputs where possible to support our conclusions.

**~~(SBU)~~** In prior years, OIG made recommendations to the Department for each key FISMA reportable information security process area separately. Each recommendation was provided to address individual control deficiencies that were identified for the applicable key information security process areas. For example, OIG made 33 recommendations in FY 2014.[6] Since the Department's corrective actions toward addressing prior year recommendations have not resolved all of these deficiencies, OIG is no longer making recommendations to address individual control deficiencies identified within the key FISMA reportable information security process areas. Instead, OIG is focusing its recommendations on addressing the underlying causes for all control deficiencies. The intent of these recommendations is to provide guidance on the first steps the Department needs to take in the development and implementation of an effective information security program, which would include identifying, assessing, responding to, and monitoring information security weaknesses using risk-based decision making at all levels of the organization. We have separately notified the Bureau of Information Resource Management[7] and the Bureau of Diplomatic Security[8] of all control deficiencies identified during the FY 2015 audit period. In addition, we have included the status of all prior year recommendations from the FY 2014 FISMA report in Appendix B.

## (U) Prior OIG Reports

**(U)** Williams, Adley has conducted annual FISMA audits of the information security program for the Department since FY 2010. In the FY 2014 FISMA report *Audit of the Department of State Information Security Program*,[9] OIG made 33 recommendations to improve the Department's information security program. In 2015, the Department closed 6 of the 33 recommendations from the FY 2014 report (the status of prior year findings is in Appendix B).

[6] **(U)** OIG, *Audit of the Department of State Information Security Program* (AUD-IT-15-17, November 2014).
[7] **(U)** Williams, Adley notified IRM of the control deficiencies in the following process areas: identity and access management (July 27, 2015), risk management (August 5, 2015), POA&Ms (July 29, 2015), and contingency planning (July 31, 2015).
[8] **(U)** Williams, Adley notified DS of the control deficiencies in the following process areas: configuration management (June 24, 2015), incident response and reporting (September 15, 2015), security training (June 24, 2015), and contractor systems (June 24, 2015).
[9] **(U)** AUD-IT-15-17, November 2014.

## (U) Work Related to Internal Controls

(U) Williams, Adley reviewed the Department's internal controls to determine whether the Department had taken the following actions:

- (U) Established an enterprise-wide information security continuous monitoring program that is institutionalized, repeatable, self-regulating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.
- (U) Established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) Established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that identifies users and network devices.
- (U) Established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) Established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) Established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) Established a plan of action and milestones program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that it tracked and monitored known information security weaknesses.
- (U) The Department has established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) Established an enterprise-wide business continuity disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) Established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in a cloud external to the organization.

(U) Deficiencies identified with the Department's internal controls are presented in the "Audit Results" section of this report.

## (U) Use of Computer-Processed Data

~~(SBU)~~ During the audit, Williams, Adley utilized computer-processed data to obtain samples and information regarding the existence of information security controls. Specifically, Williams, Adley obtained data extracted from Microsoft's Windows Active Directory and the Department's human resources system to test user account management controls. Williams, Adley assessed the reliability of computer-generated data primarily by comparing selected data with source documents. Williams, Adley determined that the information was sufficiently reliable for assessing the adequacy of related information security controls [Redacted] (b) (5) [redacted] For FISMA reportable systems that received an

authority to operate in FY 2015, the Department provided two different system inventory lists from two separate dates. [redacted] Williams, Adley took a conservative approach and used the system inventory list provided by the Bureau of Information Resource Management on April 22, 2015 (Williams, Adley used a sample of systems based on this inventory list for testing of the configuration management and contingency planning process areas).

## (U) Detailed Sampling Methodology

**(U)** For all samples selected during the audit, Williams, Adley used non-statistical audit sampling techniques where applicable and appropriate. As guidance, Williams, Adley used the American Institute of Certified Public Accountants Audit Guide Audit Sampling. This guidance assists in applying audit sampling in accordance with auditing standards. The audit strategy for the FY 2015 FISMA review uses a risk-based approach.

**(U)** With respect to the sampling methodology employed, the Government Accountability Office's *Government Auditing Standards* indicates that either a statistical or a judgment sample can yield sufficient and appropriate audit evidence. A statistical sample is generally preferable, although it may not always be practicable. By definition, a statistical sample requires that each sampling unit in the population be selected via a random process and have a known, non-zero chance of selection. These requirements often have posed a problem when conducting audits of the Department. All information systems, irrespective of size or importance, must have a chance to be randomly selected. Therefore, the exclusion of one or more of the small or insignificant systems cannot be allowed. All information systems—large and small—must have a chance to be randomly selected, and that chance must not be zero. However, the Department would undoubtedly deem many small or insignificant information systems too atypical in most instances to merit inclusion in our sample.

**(U)** Consequently, Williams, Adley employed another type of sample permitted by *Government Auditing Standards*—namely, a non-statistical sample known as a judgment sample. A judgment sample is a sample selected by using discretionary criteria rather than criteria based on the laws of probability. In this audit, Williams, Adley has taken great care in determining the criteria to use for sampling information systems. Moreover, Williams, Adley used, whenever practicable, random numbers to preclude the introduction of any bias in sample selection although a non-statistical technique was utilized. Williams, Adley acknowledges that it is possible that the information security deficiencies identified in this report may not be as prevalent or may not

exist at all in other information systems that were not tested. However, a prudent person without any basis in fact would not automatically assume that these deficiencies are non-existent in other systems. Such a supposition would be especially ill-advised for an issue as important as information security.

(U) Where Williams, Adley deemed it appropriate, Williams, Adley used audit sampling techniques to perform audit procedures to less than 100 percent of the population to enable it to evaluate audit evidence of the items selected to assist in forming a conclusion concerning the population. Generally, for a large population of sample items (more than 2,000), Williams, Adley used non-statistical sampling methods to test 22 items.[10] For small populations and operating controls that operated infrequently, Williams, Adley used guidance from the American Institute of Certified Public Accountants, as shown in Table A.1.

### (U) Table A.1: Number of Items to Test From Small Populations

| (U) Control Frequency and Population Size | (U) Items to Test |
|---|---|
| Quarterly (4) | 2 |
| Monthly (12) | 2 |
| Semimonthly (24) | 3 |
| Weekly (52) | 5 |

**(U) Source:** American Institute of Certified Public Accountants Audit Guide, "Small Populations and Infrequently Operating Controls Table 3-5."

(U) Williams, Adley followed this judgmental sampling methodology for these key process areas:

- (U) Continuous monitoring
- (U) Configuration management
- (U) Identity and access management
- (U) Incident response and reporting
- (U) Security training
- (U) Plans of action and milestones
- (U) Remote access management
- (U) Contingency planning
- (U) Contractor systems

(U) Williams, Adley did not sample for the risk management key process area, as Williams, Adley could not rely on the integrity of the system inventory (further details of the unreliability of the system inventory are in Finding A).

[10] (U) *American Institute of Certified Public Accountants Audit Guide*, "AAG-SAM Appendix A," March 2012.

# (U) APPENDIX B: FOLLOW-UP RECOMMENDATIONS FROM THE FY 2014 AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM

(U) OIG has reviewed actions implemented by management to mitigate the findings identified in the FY 2014 Department of State Federal Information Security Management Act of 2002 (FISMA) report. The current status of each of the recommendations is as follows:

(U) **Recommendation 1**: OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, implement a risk management framework strategy for the Department that is consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(U) *Status: Resolved, pending further action. OIG noted that while the Department implemented a risk management framework strategy a* [redacted] *his recommendation can be closed when OIG receives and accepts documentation showing that the Department ha* [redacted]

(U) *Status: Closed* [redacted]

~~(SBU)~~ *Status: Resolved, pending further action* [Redacted] (b) (5) [redacted] *and therefore was unable to follow*

*up on this prior year recommendation. This recommendation can be closed when OIG receives and accepts documentatio* [Redacted] (b) (5) *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

[Redacted] (b) (5)

~~(SBU)~~ *Status: Resolved, pending further action* [Redacted] (b) (5) *nd therefore was unable to follow up on this prior year recommendation. This recommendation can be closed when OIG receives and accepts documentation showing that the* [Redacted] (b) (5) *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

[Redacted] (b) (5)

~~(SBU)~~ *Status: Resolved, pending further actio* [Redacted] (b) (5) *nd therefore was unable to follow up on this prior year recommendation. This recommendation can be closed when OIG receives and accepts documentation showing that* [Redacted] (b) (5) *IG will follow up on the status of this recommendation during the FY 016 FISMA audit.*

[Redacted] (b) (5)

~~(SBU)~~ *Status: Resolved, pending further action.*

(U) **Recommendation 7**: OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, implement the Department's [Redacted] (b) (5) [Redacted] (b) (5) strategy, that includes a policy, assesses the security state of information systems, and is consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(U) *Status: Resolved, pending further action. OIG noted that while the Department's* [Redacted] (b) (5) *This recommendation can be closed when OIG receives and accepts documentation showing that the Department's* [Redacted] (b) (5) *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 8**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Enterprise Network Management Office, and the Bureau of Diplomatic Security, develop, finalize, and implement

(U) *Status: Resolved, pending further action. OIG noted that the Chief Information Officer has not finalized and implemente his recommendation can be closed when OIG receives and accepts documentation showing that the Department has IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 9**: OIG recommends that the Chief Information Officer, in coordination with all bureaus and/or offices, continue to improve processes

(U) *Status: Resolved, pending further action. OIG noted that while the Department uses* [redacted] *his recommendation can be closed when OIG receives and accepts documentation showing that the Departmen* [redacted] *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

~~(SBU)~~ **Recommendation 10**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, determine an appropriate timeframe to [redacted].

~~(SBU)~~ *Status: Resolved, pending further action. OIG noted that the Department has not fully* [redacted] *This recommendation can be closed when OIG receives and accepts documentation showing that the Departmen* [redacted] *OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

~~(SBU)~~ **Recommendation 11**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, determine whether the [redacted].

~~(SBU)~~ *Status: Resolved, pending further action. OIG noted that while the Department updated the Foreign Affairs Handbook Vulnerability Scanning Policy,* [redacted] *This recommendation can be closed when OIG receives and accepts documentation showing tha* [redacted] *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

~~(SBU)~~ **Recommendation 12**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, research, develop, and implement capabilities to perform [redacted].

~~(SBU)~~ *Status: Resolved, pending further action. OIG noted that the Department did not* [Redacted] (b) (5) *his recommendation can be closed when OIG reviews and accepts documentation showing that the Chief Information Officer, in coordination with DS, Security Infrastructure, Office of Cybersecurity* [Redacted] (b) (5) *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

~~(SBU)~~ **Recommendation 13**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, update the

~~(SBU)~~ *Status: Resolved, pending further action. OIG noted that the Departmen* [redacted] *his recommendation can be closed when OIG reviews and accepts documentation showing that the Department has updated the* [redacted] *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

**(U) Recommendation 14**: OIG recommends the Bureau of Information Resource Management, Office of Information Assurance, in coordination with system owners (bureaus and posts), follow the Foreign Affairs Manual (12 FAM 620) to have the supervisor complete the appropriate system access forms (for example, new user access and elevated rights) prior to granting access.

**(U)** *Status: Resolved, pending further action. OIG noted that the Department was unable to provide new user access and elevated rights request forms for all tested users. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has followed 12 FAM 620 to have the supervisor complete the appropriate system access forms (for example, new user access and elevated rights) prior to granting access. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

**(U) Recommendation 15**: OIG recommends that the Bureau of Information Resource Management, in coordination with Human Resources and system owners, ensure the [Redacted] (b) (5)

[redacted]

(U) *Status: Resolved, pending further action. OIG noted that tested Department separated users accessed their user accounts after employee termination. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has ensured the* [redacted] *as required by 12 FAM 620. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 16**: OIG recommends that the Chief Information Officer, in coordination with bureaus, review its [redacted]

(U) *Status: Resolved, pending further action. OIG noted that* [redacted] *OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 17**: OIG recommends the Bureau of Diplomatic Security revise the Foreign Affairs Manual for unclassified systems to define a [redacted]

(U) *Status: Closed. OIG noted that DS revised the Foreign Affairs Handbook for unclassified systems to state that* [redacted]

(U) **Recommendation 18**: OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, exercise the authorities prescribed in the Foreign Affairs Manual (1 FAM 040 and 5 FAM 119) and direct bureaus and/or offices to prioritize resources to effectively implement and validate remediation actions prior to closing Plans of Action and Milestones.

(U) *Status: Resolved, pending further action. OIG noted that the Department was unable to provide evidence of* [Redacted] (b) (5) *closed in FY 2015. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has effectively implemented and validated* [Redacted] (b) (5)

[Redacted] (b) (5) *OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 19**: OIG recommends that system owners, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, ensure that bureaus, offices, and posts adhere to completion dates for corrective actions and/or ensure that the remediation dates are updated, as needed. In addition, OIG recommends system owners implement processes and procedures to cross-reference Plans of Action and Milestones information, including costs, to the capital planning budget process with a Unique Investment Identifier.

(U) *Status: Resolved, pending further action. OIG noted that while the* [Redacted] (b) (5) *This recommendation can be closed when OIG receives and accepts documentation showing that bureaus, offices, and posts have adhered to completion dates for corrective actions and/or ensured that the remediation dates are updated as needed. In addition, this recommendation can be closed when OIG receives and accepts documentation showing that system owners have implemented* [Redacted] (b) (5) *OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 20**: OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), consistently assess overall bureau risk and provide bureaus with Quarterly Plans of Action & Milestones Grade memoranda. In addition, OIG recommends that bureaus and/or offices provide written responses for the Quarterly Plans of Action & Milestones Grade memoranda to IRM/IA.

(U) *Status: Closed. OIG noted that the Bureau of Information Resource Management,* [Redacted] (b) (5)

(U) **Recommendation 21**: OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), define a time period for bureaus and/or offices to include identified deficiencies resulting from audits into the Plans of Action and Milestones (POA&M) database and communicate findings to IRM/IA in accordance with Office of Management and Budget Memorandum M-11-33.

(U) *Status: Resolved, pending further action. OIG noted that the Department did not define a time period to include* [Redacted] (b) (5)
*This recommendation can be closed when OIG receives and accepts documentation showing that IRM/IA has defined a time period for bureaus and/or offices t* [Redacted] (b) (5)
*to IRM/IA. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit*

(U) **Recommendation 22**: OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, in coordination with system owners, identify deficiencies resulting from the vulnerability scans performed by the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, and include those vulnerabilities that are not immediately remediated in the Plans of Action and Milestones database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) *Status: Resolved, pending further action. OIG noted tha* [redacted] *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 23**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, review system owner-prepared [redacted] in accordance with the applicable Foreign Affairs Manual and National Institute of Standards and Technology guidelines.

(U) *Status: Resolved, pending further action. OIG noted that the Department did not perform* [redacted] *for all tested systems. The Department did annually review all tested* [redacted] *for all systems tested. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has included* [redacted] *OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 24**: OIG recommends that the Chief Information Officer, in coordination with system owners and the Bureau of Information Resource Management, Office of Information Assurance, review [Redacted] (b) (5) with applicable Foreign Affairs Manual and National Institute of Standards and Technology guidelines, including the [redacted]

(U) *Status: Resolved, pending further action. OIG noted that the Department did not document* [Redacted] (b) (5) [redacted] *his recommendation can be closed when OIG receives and accepts documentation showing that the Department has reviewed* [Redacted] (b) (5) [redacted]

[Redacted] (b) (5) *OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 25**: OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, consolidate and track [Redacted] (b) (5) within iMATRIX, in accordance with the Foreign Affairs Manual (5 FAM 600).

(U) *Status: Resolved, pending further action. OIG noted that not all tested* [Redacted] (b) (5) *This recommendation can be closed when OIG receives and accepts documentation showing that the Department has consolidated and tracked all extensions within iMATRIX. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 26**: OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security ensure that Memoranda of Agreement are completed [Redacted] (b) (5) as defined in accordance with the Foreign Affairs Manual [Redacted] (b) (5)

(U) *Status: Resolved, pending further action. OIG noted that not all tested* [Redacted] (b) (5) *had a completed Memorandum of Agreement. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has ensured that Memoranda of Agreement are completed for all* [Redacted] (b) (5) *as defined in accordance with 5 FAM 1065. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 27:** OIG recommends that the Assistant Secretary for Diplomatic Security ensure that [Redacted] (b) (5) are completed for [Redacted] (b) (5) as defined within each Memorandum of Agreement.

(U) *Status: Resolved, pending further action. OIG noted that not all teste* [Redacted] (b) (5) *This recommendation can be closed when OIG receives and accepts documentation showing that the Assistant Secretary for Diplomatic Security has ensured th* [Redacted] (b) (5) *IG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 28**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security's Security Infrastructure Directorate, Office of Computer Security, finalize the Information Assurance Training Plan to ensure key information technology personnel with security responsibilities for the Department take specialized role-based security training as

required by National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) *Status: Resolved, pending further action. OIG noted that while the Department initiated Information Systems Security Officer and system owner role-based training courses, not all tested users with significant security responsibilities for the Department had taken specialized role-based security training. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has finalized the Information Assurance Training Plan to ensure that key information technology personnel with security responsibilities for the Department take specialized role-based security training. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 29**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security's Security Infrastructure Directorate, Office of Computer Security, implement a tracking mechanism for role-based training, in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4, to ensure that personnel with significant security responsibilities receive the appropriate training according to the Information Assurance Training Plan.

(U) *Status: Resolved, pending further action. OIG noted that DS has not fully implemented a tracking mechanism for employees who have taken the required role-based training. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has implemented a tracking mechanism for role-based training. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 30**: OIG recommends that the Information System Steering Committee, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security's Security Infrastructure Directorate, Office of Computer Security, implement a general security awareness course, specific to users with only ClassNet access that do not have OpenNet access, to ensure that those personnel receive the appropriate general security awareness training in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) *Status: Resolved, pending further action. OIG noted that tested users with only ClassNet access who do not have OpenNet access were not required to take the security training course. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has implemented a general security awareness course specific to users with only ClassNet access, who do not have OpenNet access, to ensure that those personnel received the appropriate general security awareness training. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 31**: OIG recommends that the Chief Information Officer, in coordination with the Bureau of Administration, finalize the Foreign Affairs Manual [Redacted] (b) (5)

[Redacted] (b) (5) to replace the [Redacted] (b) (5)

(U) *Status: Closed. OIG noted that the Chief Information Officer finalize* [Redacted] (b) (5)

(U) **Recommendation 32**: OIG recommends that the Bureau of Information Resource Management, Operations, [Redacted] (b) (5) have been finalized.

(U) *Status: Closed. OIG noted that the Bureau of Information Resource Management, Operations,* [Redacted] (b) (5) *provided evidence showing that a sample of* [Redacted] (b) (5) *users found in the activ* [Redacted] (b) (5) *console were also enrolled in the* [Redacted] (b) (5)

(U) **Recommendation 33:** OIG recommends that the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, update the Computer Incident Response Team Standard Operating Procedures to require the Computer Incident Response Team to notify the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Information Security, Program Applications Division, and the U.S. Computer Emergency Readiness Team in the event of a potential data spillage prior to closing a security incident ticket.

(U) *Status: Closed. OIG noted that the Computer Incident Response Team Standard Operating Procedures had been updated to require the Computer Incident Response Team to notify DS, Security Infrastructure Directorate, Office of Information Security, Program Applications Division, and the U.S. Computer Emergency Readiness Team in the event of a potential data spillage prior to closing a security incident ticket.*

# (U) APPENDIX C: SYSTEMS TESTED SINCE FY 2010

(U) The system inventory list provided by the Bureau of Information Resource Management on April 22, 2015, contained a population of [Redacted] (b) (5) FY 2015 new and recertified Federal Information Security Management Act of 2002 reportable systems operating at the Department of State. Williams, Adley tested nine of these systems. As shown in table C.1, Williams, Adley has tested [Redacted] (b) (5) systems since FY 2010 ([Redacted] (b) (5) of which were unique).

[Redacted] (b) (5)

[Redacted] (b) (5) [Redacted] (b) (5) [Redacted] (b) (5) [Redacted] (b) (5) in multiple years.

[2] **(U)** According to a Bureau of Diplomatic Security official on June 10, 2015, Williams, Adley determined that this system was a duplicate of the Email system.

**(U) Source:** Williams, Adley prepared based on work performed in prior years.

# (U) APPENDIX D: FY 2015 CONTINUOUS MONITORING MATURITY MODEL

## (U) Table D.1: FY 2015 Continuous Monitoring Maturity Model

| (U) Level | (U) Definition |
|---|---|
| 1<br>Ad-hoc | (U) Information Security Continuous Monitoring (ISCM) program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, SP 800-137, Office of Management and Budget (OMB) M-14-03, and the Chief Information Officer (CIO) ISCM CONOPS [Concept of Operations].<br>• (U) ISCM activities are performed without the establishment of comprehensive policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.<br>• (U) ISCM stakeholders and their responsibilities have not been defined and communicated across the organization.<br>• (U) ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used.<br>• (U) The organization lacks personnel with adequate skills and knowledge to effectively perform ISCM activities.<br>• (U) The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk.<br>• (U) The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management.<br>• (U) ISCM activities are not integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements.<br>• (U) There is no defined process for collecting and considering lessons learned to improve ISCM processes.<br>• (U) The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. |

| (U) Level | (U) Definition |
|---|---|
| 2<br>**Defined** | **(U)** The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.<br>• **(U)** ISCM activities are defined and formalized through the establishment of comprehensive ISCM policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.<br>• **(U)** ISCM stakeholders and their responsibilities have been defined and communicated across the organization, but stakeholders may not have adequate resources (people, processes, tools) to consistently implement ISCM activities.<br>• **(U)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used.<br>• **(U)** The organization 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, these measures are not consistently collected, analyzed, and used across the organization.<br>• **(U)** The organization has identified and fully defined the ISCM technologies it plans to utilize in the ISCM automation areas. Automated tools are implemented to support some ISCM activities but the tools may not be interoperable. In addition, the organization continues to rely on manual/procedural methods in instances where automation would be more effective.<br>• **(U)** The organization has defined how ISCM activities will be integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. However, the organization does not consistently integrate its ISCM and risk management activities.<br>• **(U)** The organization has defined its process for collecting and considering lessons learned to make improvements to its ISCM program. Lessons learned are captured but are not shared at an organizational level to make timely improvements.<br>• **(U)** ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. |
| 3<br>**Consistently Implemented** | **(U)** In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.<br>• **(U)** The ISCM program is consistently implemented across the organization, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS.<br>• **(U)** ISCM stakeholders have adequate resources (people, processes, technologies) to effectively accomplish their duties.<br>• **(U)** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization.<br>• **(U)** The organization has standardized and consistently implemented its defined technologies in all of the ISCM automation areas. ISCM tools are interoperable, to the extent practicable.<br>• **(U)** ISCM activities are fully integrated with organizational risk tolerance, the threat |

| (U) Level | (U) Definition |
|---|---|
| | environment, and business/mission requirements.<br>• **(U)** The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes.<br>• **(U)** ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. |
| **4 Managed and Measurable** | **(U)** In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.<br>• **(U)** Qualitative and quantitative measures on the effectiveness of the ISCM program are collected across the organization and used to assess the ISCM program and make necessary changes.<br>• **(U)** Data supporting ISCM metrics is obtained accurately, consistently, and in a reproducible format, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS.<br>• **(U)** ISCM data is analyzed consistently and collected and presented using standard calculations, comparisons, and presentations.<br>• **(U)** ISCM metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities, including situational awareness and risk response.<br>• **(U)** ISCM metrics provide persistent situational awareness to stakeholders across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations, the organization's infrastructure, and security domains.<br>• **(U)** ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and [plans of action and milestones] POA&M) up to date on an ongoing basis. |
| **5 Optimized** | **(U)** In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.<br>• **(U)** Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.<br>• **(U)** The ISCM program is integrated with strategic planning, enterprise architecture, and capital planning and investment control processes.<br>• **(U)** The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. |

**(U) Source:** DHS, FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics.

# (U) APPENDIX E: CRITERIA FOR FINDINGS

## (U) Table E.1: Continuous Monitoring Requirements

| (U) Law or Regulation | (U) Requirement |
|---|---|
| **(U)** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137[1] | **(U)** NIST SP 800-137 "assist[s] organizations in the development of an ISCM [Information Security Continuous Monitoring] strategy and the implementation of an ISCM program that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls. The ISCM strategy and program support ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance, as well as the ability to provide the information needed to respond to risk in a timely manner."<br><br>**(U)** "System-level ISCM addresses monitoring security controls for effectiveness (assessments), monitoring for security status, and reporting findings. At a minimum, all security controls, including common and hybrid controls implemented at the system level, are assessed for effectiveness in accordance with the system security plan and the methods described in NIST SP 800-53A, as amended." |

**(U) Source:** NIST SP 800-137.

## (U) Table E.2: Configuration Management Requirements

| (U) Law or Regulation | (U) Requirement |
|---|---|
| **(U)** NIST SP 800-53, rev. 4[2] | **(U)** The organization identifies, reports, and corrects information system flaws. |
| **(U)** NIST SP 800-115[3] | **(U)** The organization's information security assessment policy should address the following:<br>1. **(U)** Organizational requirements with which assessments must comply.<br>2. **(U)** Appropriate roles and responsibilities (at a minimum, for those individuals approving and executing assessments).<br>3. **(U)** Adherence to established methodology.<br>4. **(U)** Assessment frequency.<br>5. **(U)** Documentation requirements, such as assessment |

[1] **(U)** NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," September 2011.
[2] **(U)** NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "SI-2 Flaw Remediation," January 2015.
[3] **(U)** NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," "6.1 Developing a Security Assessment Policy," September 2008.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | plans and assessment results. |
| **(U)** Foreign Affairs Manual (FAM) | **(U)** 5 FAM 1060[4] states:<br>a. **(U)** Using appropriate techniques and IT CCB [Information Technology Configuration Control Board]-approved vulnerability scanning tools, DS/SI/CS [Bureau of Diplomatic Security/Security Infrastructure/Office of Cybersecurity], the Evaluation and Verification Program personnel, must scan for vulnerabilities in the information system periodically, as well as when significant new vulnerabilities affecting the system are identified and reported.<br>b. **(U)** Vulnerability scanning tools should include the capability to readily update the list of vulnerabilities scanned.<br>d. **(U)** Vulnerability scanning procedures must include steps to ensure adequate scan coverage and include both vulnerabilities checked and information system components scanned.<br><br>**(U)** 5 FAM 860[5] states:<br>c. **(U)** Information Management Officers/Information Security Officers/system administrators must follow guidelines and procedures established by the Department's Enterprise Patch Management Program and apply patches in an expeditious manner.<br><br>**(U)** 5 FAM 1060[6] states:<br>b. **(U)** Patch management compliance is defined as:<br>1) **(U)** For critical patches: achieving and maintaining a patch installation rate of 100%, as designated by the Enterprise Network Management Office;<br>2) **(U)** For all workstations and servers on [Redacted] (b) (5) [redacted] achieving and maintaining a patch installation rate 90% of all patches within 15 days after patch release.<br><br>**(U)** 5 FAM 1060[7] states:<br>f. **(U)** The CISO [Chief Information Security Officer] must send an official memorandum (domestically) or telegram (abroad) to the requesting system owner detailing the final |

[4] **(U)** 5 FAM 1065.5, "Information Assurance Management," "Vulnerability Scanning," February 2007.
[5] **(U)** 5 FAM 866c, "Hardware and Software Maintenance," "Patch Management," July 2013.
[6] **(U)** 5 FAM 1067.3b, "Information Assurance Management," "Patch Management Compliance Program," January 2009.
[7] **(U)** 5 FAM 1065.3-2, "Information Assurance Management," "Request for Waivers, Exceptions, and Deviations," January 2009.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | decision (approval or disapproval) on the waiver, exception, or deviation request:<br>1) **(U)** If the CISO approves the request for implementation domestically, the system owner must:<br>a) **(U)** Within 30 days, endorse the memorandum, in writing, acknowledging his or her understanding and acceptance of the decision and any terms/conditions; and<br>b) **(U)** Make a copy of the endorsed memorandum for his or her record, and return the original memorandum with endorsement to the CISO.<br>2) **(U)** If the CISO approves the request for implementation abroad, the system owner must:<br>a. **(U)** Send a telegram to the CISO acknowledging acceptance of the decision and any terms/conditions; and<br>b. **(U)** For future reference and inspection, ensure copies of all documents related to the request are on file at post. |

**(U) Source:** NIST SP 800-53, rev. 4; NIST SP 800-115; 5 FAM 1060; and 5 FAM 860.

## (U) Table E.3: Identity and Access Management Requirements

| (U) Law or Regulation | (U) Requirement |
|---|---|
| **(U)** FAM | **(U)** In regard to obtaining administrative access, 12 FAM 620[8] states:<br>c. **(U)** The form must include the user's name, the applications involved, and the type of access required within each application. Whenever a user's functional responsibilities change and the user still requires system access, the user's current supervisor must complete a new system access request form for access privileges commensurate with the user's new responsibilities.<br>d. **(U)** The data center manager and the system manager must sign the access request form when the information provided is adequate, indicating approval for automated information system access. The data center manager and the system manager retain all approved automated information system access request forms for at least six months after the date of removal from the automated information system.<br><br>**(U)** In regard to termination of accounts, 12 FAM 620[9] states:<br>g. **(U)** The data center manager and the system manager |

[8] **(U)** 12 FAM 629.2-1, "Unclassified Automated Information Systems," "System Access Control," June 2008.
[9] **(U)** 12 FAM 622.1-3, "Unclassified Automated Information Systems," "Password Controls," August 2008.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | must immediately delete individual user IDs and passwords under the following conditions:<br>1) **(U)** Whenever notified by a user's supervisor that the user no longer requires automated information system access; or<br>2) **(U)** Whenever notified by a proper authority, such as the human resources officer, that the user's employment has been terminated with the Department or has been transferred to another office or post. |
| | **(U)** In regard to obtaining new user access, 12 FAM 620[10] states:<br>**(U)** Supervisors must complete a system access request form for each staff member who requires automated information system access. |
| | **(U)** In regard to password requirements for accounts on [Redacted] (b) (5) 12 FAM 620[11] states:<br>e. **(U)** The data center manager and the system manager must ensure that all passwords are changed under the following conditions:<br>1) **(U)** At least once every 60 days<br>f. **(U)** To ensure that all passwords are changed every 60 days, the data center manager and the system manager must configure the system to automatically prompt users to change their passwords for at least 14 days prior to the expiration date. |
| | **(U)** In regard to password configuration for classified and unclassified systems, 12 FAM 620[12] states:<br>a. **(U)** The data center manager and the system manager must initially assign each new user a unique user ID and a minimum 12 character, alphanumeric, randomly generated password. Once the new user has accessed the system for the first time, the system must force the user to immediately change this issued password. The password construction and specifications for user-created passwords are the same for both classified and unclassified systems. |
| | **(U)** In regard to classified systems, 12 FAM 630[13] states: |

[10] **(U)** 12 FAM 622.1-2, "Unclassified Automated Information Systems," "System Access Control," June 2008.
[11] **(U)** 12 FAM 622.1-3, Unclassified Automated Information Systems," "Password Controls," August 2008.
[12] **(U)** 12 FAM 623.3-1, "Unclassified Automated Information Systems," "Identification and Authentication," February 2013.
[13] **(U)** 12 FAM 632.1-3, "Classified Automated Information Systems," "Controlling Access to Systems," May 2013.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | h. **(U)** The system administrator must ensure that accounts are temporarily disabled after 90 days of inactivity. Before reactivating the account, the user's supervisor must recertify in writing, e.g., via email or memo that the user still requires the account. |
| **(U)** Foreign Affairs Handbook (FAH) | **(U)** 12 FAH-10 H-110[14] states:<br>f. **(U)** The Diplomatic Security (DS) Office of Computer Security (DS/SI/CS) must ensure that DS Security Configuration Standards configure information systems to:<br>1) **(U)** Automatically disable inactive accounts after 90 days." |
| **(U)** Department of State Global Address List and Active Directory Standardization[15] | **(U)** "Shared mailboxes must be populated with the name of the Primary User Account who is responsible for its management (i.e. password management of the service account)." |
| **(U)** All Diplomatic and Consular Posts Telegram 2008 STATE 8277 | **(U)** The Department should "implement the following password requirements for users, local PC accounts and Active Directory service accounts…" with a "maximum password age [of] 60 days."[16] |

**(U) Source:** 12 FAM 620; 12 FAM 630; 12 FAH-10 H-110; *Department of State Global Address List (GAL) and Active Directory (AD) Standardization*; and ALDAC Telegram 2008 STATE 8277.

## (U) Table E.4: Security Training Requirements

| (U) Law or Regulation | (U) Requirement |
|---|---|
| **(U)** NIST SP 800-53, rev. 4 | **(U)** The "organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training."[17] |
| **(U)** FAM | **(U)** 5 FAM 1060[18] states:<br>b. **(U)** Training programs must include annual awareness training for all system users.<br>c. **(U)** Training program must include specific role-based security training for identified Department personnel with significant information security responsibilities. |
| **(U)** Cybersecurity Awareness and Training Program | **(U)** The Department's *Cybersecurity Awareness and Training Program*[19] states:<br>**(U)** The PS800 course must be completed within 10 days of a user gaining access to OpenNet and annually thereafter. Once |

[14] **(U)** 12 FAH-10 H-112.1-1, "Unclassified/SBU Information System Security Technical Controls," "Account Management – Management Responsibilities," September 2014.
[15] **(U)** *Department of State Global Address List (GAL) and Active Directory (AD) Standardization*, "Shared Mailbox Accounts," September 2014.
[16] **(U)** ALDAC Telegram 2008 STATE 8277, "Change to Password Policy," January 2008.
[17] **(U)** NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "AT-4 Security Training Records," January 2014.
[18] **(U)** 5 FAM 1067.2-2, "Information Assurance Management," "Training and Education Program," January 2009.
[19] **(U)** *Cybersecurity Awareness and Training Program*, "5.1 Awareness Training," October 2014.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | a user completes the course, their user account is automatically set to expire 365 days from their date of course completion." |

**(U) Source:** NIST SP 800-53, rev 4; 5 FAM 1060; and *Cybersecurity Awareness and Training Program*.

## (U) Table E.5: Plans of Action and Milestones (POA&Ms) Requirements

| (U) Law or Regulation | (U) Requirement |
|---|---|
| **(U)** FAM | **(U)** 5 FAM 110[20] states:<br>a. **(U)** The ISSC [Information Security Steering Committee]<br>1. **(U)** Develops priorities and advocates for the availability of resources for security of Department information systems. |
| **(U)** NIST SP 800-53, rev. 4[21] | **(U)** The organization updates existing plans of action and milestones...based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. |
| **(U)** OMB | **(U)** "The required data elements are weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the status."[22]<br><br>**(U)** "A POA&M...details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones."[23]<br><br>**(U)** "Specifically, for each POA&M that relates to a project (including systems) for which a capital asset plan and justification was submitted or was a part of the exhibit 53, the unique project identifier must be reflected on the POA&M. This identifier will provide the link to agency budget materials."[24]<br><br>**(U)** "Program officials shall regularly (at the direction of the CIO [Chief Information Officer]) update the agency CIO on their |

[20] **(U)** 5 FAM 119, "Information Technology Management," "Information Security Steering Committee (ISSC)," February 2008.
[21] **(U)** NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "CA-5 Plan of Action and Milestones," January 2014.
[22] **(U)** OMB Memorandum M-11-33, "FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf>, accessed on September 25, 2015.
[23] Ibid.
[24] **(U)** OMB Memorandum M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," <https://www.whitehouse.gov/omb/memoranda_m02-01/>, accessed on September 24, 2015.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | progress to enable the CIO to provide the agency's quarterly update to OMB."[25] |
| **(U)** The Department's POA&M Toolkit[26] | **(U)** Sometimes security weaknesses are identified when a security incident occurs or a new threat source is identified. An action needs to be created whenever the weakness is not immediately corrected. The POA&M Tester Database is currently designed to create a record of each weakness found during testing. After testing is completed, the Bureau submits the tester database to [Office of Information Assurance]. [Office of Information Assurance] integrates the open items into the Bureau's master POA&M.<br><br>**(U)** The POA&M data for each action includes documentation of the…budgeted (amount in dollars, adequately budgeted)…remediation plan (point of contact, date, remediation action required, other resources)…and actual remediation action (actual remediation action taken, completed by, and actual completion date).<br><br>**(U)** If managers don't have resources to close a Finding, then it will remain an open weakness. Budgeting to close Findings is required by OMB so that resources needed to close items will be available and Findings can be closed in a timely manner, and the risk/cost ratio can be used to prioritize work to close Findings, and those with the highest risk/cost ratio can be closed first. If no resources are entered, management will assume that the problem can be fixed at no cost. That means it should be fixed immediately.<br><br>**(U)** Once the Actual Completion Date and Verifier Action fields have been entered into the testing or bureau-tracking database, the item will be considered closed.<br><br>**(U)** Information System Owners of information systems with significant numbers of late actions can expect OMB to reduce the system's budget for maintenance and development, and divert |

[25] **(U)** OMB Memorandum M-02-09, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones," <https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/m02-09.pdf>, accessed on September 25, 2015.

[26] **(U)** *POA&M Toolkit*, "8. How does a Bureau (and its Information System Owners) record that POA&M actions are closed?," "4. How should a Bureau (and its Information System Owners) identify and enter security weaknesses as POA&M actions?," "13. How does the CIO provide oversight and review of the POA&M process?," "2. Why is the process to manage POA&Ms and their actions important?," "1. What is a Plan of Action and Milestones (POA&M) action?," "5. How can a Bureau (and its Information System Owners) tell when actions have been properly entered?," and "12. How are Bureaus affected by the reporting of the status of POA&Ms to OMB?," <http://irm.m.state.sbu/sites/ia/SiteDirectory/poams/Pages/default.aspx>, accessed September 28, 2015.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | resources to closing outstanding security weaknesses as a higher priority. The summary of the status of efforts to close POA&Ms must be reported to OMB quarterly by the Department for each FISMA [Federal Information Security Management Act of 2002] reportable system. The summary includes four categories for each system including Red – 90 or more days overdue, Orange – less than 90 days overdue, Yellow – un-remediated actions not yet overdue, and Green – closed actions (with completed remediation and verification). The Department expects Information System owners to close most items within 180 days.<br><br>**(U)** FISMA and OMB require the CIO to conduct a quarterly review of the status of remediation. This review shall determine which bureaus are not making adequate progress toward remediation of their outstanding actions.<br><br>**(U)** A POA&M action is a mutual commitment made between remediators who promise management that the security weakness will be corrected by the due date and management who promise remediators that the specified resources will be provided. |

**(U) Source:** 5 FAM 110; NIST SP 800-53, rev. 4; OMB Memoranda M-11-33, M-02-01, and M-02-09; and the Department's POA&M Toolkit.

## (U) Table E.6: Contingency Planning Requirements

| (U) Law or Regulation | (U) Requirement |
|---|---|
| **(U)** NIST SP 800-34, rev. 1 | **(U)** An up-to-date ISCP [information system contingency plan] is essential for successful ISCP operations. As a general rule, the ISCP should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the ISCP, system, mission/business processes supported by the system, or resources used for recovery procedures. Deficiencies identified through testing should be addressed during plan maintenance. Elements of the plan subject to frequent changes, such as contact lists, should be reviewed and updated more frequently.[27]<br><br>**(U)** The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.[28]<br><br>**(U)** Provide a statement in accordance with the agency's contingency planning policy to affirm that the ISCP is complete |

[27] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "3.6 Plan Maintenance," May 2010.
[28] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "CP-10 Information System Recovery and Reconstitution," May 2010.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | and has been tested sufficiently. The statement should also affirm that the designated authority is responsible for continued maintenance and testing of the ISCP. This statement should be approved and signed by the system designated authority. Space should be provided for the designated authority to sign, along with any other applicable approving signatures.[29]<br>**(U)** The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.[30]<br><br>**(U)** The organization establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable.[31]<br><br>**(U)** The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.[32]<br><br>**(U)** The [business impact analysis] is a key step in implementing the CP [Contingency Planning] controls in NIST SP 800-53 and in the contingency planning process overall. The [business impact analysis] enables the ISCP Coordinator to characterize the system components, supported mission/business processes, and interdependencies.[33] |
| **(U)** NIST SP 800-53, rev. 4[34] | **(U)** The contingency plan for the information system is reviewed and approved by designated officials within the organization. |

[29] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "Plan Approval," May 2010.
[30] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "CP-6 Alternate Storage Site," May 2010.
[31] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "CP-7 Alternate Processing Site," May 2010.
[32] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "CP-8 Telecommunications Services," May 2010.
[33] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "3.2 Conduct the Business Impact Analysis (BIA)," May 2010.
[34] **(U)** NIST SP 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems and Organizations," "CP-2 Contingency Plan," January 2014.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| **(U)** FAM | **(U)** 5 FAM 1060[35] states:<br>a. **(U)** System owners and non-Department entities (i.e., organizations, individuals, or other agencies) that process Federal information on behalf of the Department must:<br>1) **(U)** Develop and maintain contingency plans for the major applications and general support systems under their control that process, store, or transmit Federal information;<br>2) **(U)** Use the Department's Contingency Plan template to prepare the contingency plan (see the Contingency Plan template available on the Information Assurance Web site);<br>3) **(U)** For purposes of inspection, retain copies of the contingency plan and test results for the life of the system;<br>4) **(U)** Update and test the contingency plan when the major application or general support system has undergone a major change to its operational baseline configuration; and<br>5) **(U)** For moderate and high impact systems, test the contingency plan at least annually to verify the entities' ability to recover and/or restore the application or system to operation in the event of a system or application failure.<br>b. **(U)** [The Bureau of Information Resource Management, Office of Information Assurance] will assess system security, contingency planning, and continuity of operations efforts, and assist system owners in correcting deficiencies.<br><br>**(U)** 5 FAM 850[36] states:<br>a. **(U)** Regardless of the size of the system, system and data files must be backed up regularly (at least once per week). The [Information Management Officer]/[Information Systems Officer]/System Administrator has responsibility to:<br>1) **(U)** Establish a method and time for backups and adhere to the schedules;<br>2) **(U)** Determine which files are to be backed up, and when and how they will do it;<br>3) **(U)** Decide when to back up based on the local |

[35] **(U)** 5 FAM 1064.2, "Information Assurance Management," "Contingency Planning and Continuity of Operations," February 2007.
[36] **(U)** 5 FAM 852, "Continuity of Operations and Contingency Planning for Information Systems," "Backups," September 2008.

| (U) Law or Regulation | (U) Requirement |
|---|---|
| | operational environment; and<br>4) **(U)** Notify users of backup schedules.<br><br>**(U)** 6 FAM 400[37] states:<br>**(U)** The responsibilities of each Assistant Secretary, or equivalent, in the Domestic Emergency Management Program include…reviewing, updating, and certifying its [Bureau Emergency Action Plan] on an annual basis and providing [Bureau of Administration/Office of Emergency Management] a copy of the certification page from the [Bureau Emergency Action Plan]. |

**(U) Source:** NIST SP 800-34, rev. 1; NIST SP 800-53, rev. 4; 5 FAM 1060; 5 FAM 850; and 6 FAM 400.

## (U) Table E.7: Contractor Systems Requirements

| (U) Law or Regulation | (U) Requirement |
|---|---|
| **(U)** FAM | **(U)** "The Bureau of Diplomatic Security's Evaluation and Verification Program, in compliance with the FISMA reporting requirements, must evaluate and validate location-specific system security controls. Location-specific system security controls must be verified yearly as well as part of the systems authorization process."[38]<br><br>**(U)** "Connectivity requests must include a signed Memorandum of Agreement or Understanding."[39]<br><br>**(U)** "All systems (including applicable contractor systems) and applications associated with any projects must be registered in [Redacted] (b) (5) |

**(U) Source:** 5 FAM 1060 and 5 FAM 600.

[37] **(U)** 6 FAM 416.1, "General Services and Domestic Emergency Management," "Assistant Secretary," May 2012.
[38] **(U)** 5 FAM 1065.4-1, "Risk Management," "Department Information Systems," January 2009.
[39] **(U)** 5 FAM 1065.3-1, "Risk Management," "Requests for Interagency and Non-Department Connectivity," January 2009.
[40] **(U)** 5 FAM 611, "Information Technology Systems," "General," June 2009.

# (U) APPENDIX F: FISMA REPORTABLE AREAS FOR FY 2015

(U) Table F.1 describes the 10 FISMA reportable areas for FY 2015.

## (U) Table F.1: FISMA FY 2015 Reportable Areas

| (U) FISMA Reportable Area | (U) Definition |
|---|---|
| (U) Continuous Monitoring | (U) The purpose of continuous monitoring is to make hardware assets harder to exploit through hardware asset management, software asset management, secure configuration management, and vulnerability management. |
| (U) Configuration Management | (U) The purpose of configuration management is to manage the effects of changes or differences in configurations on an information system or network. Configuration management is an essential component of monitoring the status of security controls and identifying potential security-related problems in information systems. This information can help security managers understand and monitor the evolving nature of vulnerabilities as they appear in a system under their responsibility, thus enabling managers to direct appropriate changes as required. The goal of configuration management is to make assets harder to exploit through better configuration. |
| (U) Identity and Access Management | (U) Users and devices must be authenticated to ensure that they are who or what they identify themselves to be. The purpose of identity and access management is to ensure that users and devices are properly authorized to access information and information systems. |
| (U) Incident Response and Reporting | (U) The purpose of incident response and reporting is to determine the kinds of attacks that have been successful and position the organization to make a risk-based decision about where it is most cost effective to focus its security resources. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations quickly. |
| (U) Risk Management | (U) The purpose of risk management focuses on how the organization is evaluating risk and prioritizing security issues. |
| (U) Security Training | (U) Establishing and maintaining a robust and relevant information security training process as part of the overall information security program is the primary conduit for providing a workforce with the information and tools needed to protect an agency's vital information resources. This will ensure that personnel at all levels of the organization understand their information security |

| (U) FISMA Reportable Area | (U) Definition |
|---|---|
| | responsibilities to properly use and protect the information and resources entrusted to them. Organizations that continually train their workforce in organizational security policy and role-based security responsibilities will have a higher rate of success in protecting information. |
| **(U)** POA&Ms | **(U)** The purpose of POA&Ms is to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. POA&Ms track the measures implemented to correct deficiencies and to reduce or eliminate known vulnerabilities. POA&Ms can also assist in identifying performance gaps, evaluating an organization's security performance and efficiency, and conducting oversight. POA&Ms are an essential part of the risk management process to track problems and to decide which issues to address, and they show an organization's efforts to address corrective action with a standard and centralized approach. |
| **(U)** Remote Access Management | **(U)** The purpose of remote access management is to help deter, detect, and defend against unauthorized network connections/access to internal and external networks. Secure remote access is essential to an organization's operations because the proliferations of system access through telework, mobile devices, and information sharing means that information security is no longer confined within system perimeters. "Organizations also rely on remote access as a critical component of contingency planning and disaster recovery." |
| **(U)** Contingency Planning | **(U)** Contingency planning involves the actions required to plan for, respond to, and mitigate damaging events. As such, the primary purpose of contingency planning is to give attention to rare events that have the potential for significant consequences and promoting first priority risk. |
| **(U)** Contractor Systems | **(U)** The purpose of contractor systems is to ensure that information systems operated by contractors and other external entities on behalf of the Federal Government meet all applicable security requirements. |

**(U) Source:** DHS, FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics; OMB, "Annual Report to Congress: Federal Information Security Management Act;" Public Law 113-283, Federal Information Security Modernization Act of 2014.

# (U) APPENDIX G: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE

United States Department of State

*Chief Information Officer*
*Information Resource Management*

*Washington, D.C. 20520-6311*

~~SENSITIVE BUT UNCLASSIFIED~~
Unclassified When Separated from Attachment

November 6, 2015

FROM: IRM – Steven C. Taylor ST

SUBJECT: Response to Draft Memo for Audit of the Department of State Information Security Program

Thank you for the opportunity to review the subject draft audit report. As conveyed in our response to the notice of findings and recommendations, we concur with comments as noted in the attachment for recommendations one, three, and four. We yield to the Deputy Secretary for Management and Resources for comment on recommendation two.

This year has been, and continues to be a very active year with the implementation of new information security capabilities, policy promulgation, and procedural changes. The Department took meaningful and deliberative steps to improve our ability to detect and deter potential attacks, implemented two-factor authenticated access for all general and privileged users domestically, and will complete the same for posts by early December. We have implemented requirements for mission owners to jointly accept risk to their operations when relying on systems employing personally identifiable information, and have begun implementation of data at rest encryption for all moderate and high impact systems. We also have issued policies on the use of demilitarized zones, cloud services, and dedicated internet networks. In addition, we are accelerating segmentation for our network to improve security for specific sensitive information. Every year we have made progress and are highly committed to continued improvements in advancing information security in the Department.

Lastly, we noted one item in the report of concern. On page 12, reference is made to a press article to support a causal relationship between the Department's management of risk and the occurrence of an incident. As this is not primary evidence and its accuracy is in question, we recommend consideration be given to its removal from the report.

Attachment: As noted.

~~SENSITIVE BUT UNCLASSIFIED~~

SENSITIVE BUT UNCLASSIFIED

**Attachment**

**(U) Recommendation 1**: OIG recommends that the Chief Information Officer [Redacted] (b) (5) [Redacted] (b) (5) in accordance with National Institute of Standards and Technology Special Publication 800-39.

**(U) IRM Response (November 6, 2015)**: IRM concurs with this recommendation. As noted in the response to the Notification of Finding and Recommendation (NFR) #1, IRM developed and shared the Information Security Risk Management Strategy with the OIG and will use the feedback provided now to amend the strategy as appropriate.

**(U) Recommendation 2**: OIG recommends that the Deputy Secretary of State for Management and Resources review the organizational placement of the Chief Information Officer, with respect to the Clinger-Cohen Act and Office of Management and Budget Memorandum M-11-29 and make a determination as to whether the Chief Information Officer (CIO) should be realigned within the Department of State's (Department) organizational structure to carry out the CIO's lead role in managing information security for the Department.

**(U) IRM Response (November 6, 2015)**: IRM defers to the Deputy Secretary of State for Management and Resources.

**(U) Recommendation 3**: OIG recommends that the Chief Information Officer, [Redacted] (b) (5)

**(U) IRM Response (November 6, 2015)**: IRM concurs with this recommendation. IRM noted in the response to NFR #2 that the Department's overall risk management plan is being addressed by the Office of Management Policy, Rightsizing, and Innovation (M/PRI); IRM will continue to support M/PRI in this organization-wide effort and will work to further develop and refine its risk management approach for the Department's bureau-owned information systems.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

**(U) Recommendation 4**: OIG recommends that the Chief Information Officer define and implement the [Redacted] (b) (5) [redacted]

**(SBU) IRM Response (November 6, 2015)**: IRM concurs with this recommendation. The Department is in the implementation stage of its multi-year collaboration with the Department of Homeland Security (DHS) to expand its implementation of iPost continuous monitoring capability upon which the DHS Continuous Diagnostics & Mitigation program was built. This effort is guided by a suggested memorandum of understanding (MOU) with DHS to further this capability. The kickoff meeting with DHS and their prime contractor, Northrup Grumman, was held October 27, 2015. The primary focus of the meeting was; the addition of licenses to tools the Department already procured and implemented, the upload of raw data to DHS for government-wide visibility and the addition of a new agency-level dashboard called Archer.

SENSITIVE BUT UNCLASSIFIED

# (U) APPENDIX H: DEPUTY SECRETARY OF STATE FOR MANAGEMENT AND RESOURCES RESPONSE

United States Department of State

*The Deputy Secretary of State*

*Washington, D.C. 20520*

~~SENSITIVE BUT UNCLASSIFIED~~

November 9, 2015

MEMORANDUM

TO: OIG/AUD – Norman P. Brown

FROM: D-MR – Julie Fisher, Chief of Staff JDF

SUBJECT: Response to Recommendation 2 in Draft Report on FY 2015 Audit of the Department of State Information Security Program

The Deputy Secretary for Management and Resources has reviewed Recommendation 2 in the draft report to review the organizational placement of the Chief Information Officer (CIO) and make a determination as to whether the CIO should be realigned within the Department's organizational structure. She agrees with this recommendation.

# (U) ABBREVIATIONS

| | |
|---|---|
| A&A | assessment and authorization |
| AD | Active Directory |
| ATO | Authority to Operate |
| CIO | Chief Information Officer |
| CONOPS | Concept of Operations |
| DHS | Department of Homeland Security |
| DMZ | Demilitarized Zone |
| DS | Bureau of Diplomatic Security |
| FAM | Foreign Affairs Manual |
| FISMA | Federal Information Security Management Act of 2002 |
| IRM | Bureau of Information Resource Management |
| ISCM | Information Security Continuous Monitoring |
| ISRMS | Information Security Risk Management Strategy |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| OMB | Office of Management and Budget |
| POA&Ms | plans of action and milestones |
| SP | Special Publication |
| UII | Unique Investment Identifier |

# HELP FIGHT

**FRAUD. WASTE. ABUSE.**

1-800-409-9926
**OIG.state.gov/HOTLINE**

If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:

**OIGWPEAOmbuds@state.gov**