



Office of Inspector General  
United States Department of State

AUD-AOQC-22-07

Office of Audits

December 2021

**(U) Management Assistance Report:  
Support From the Under Secretary for  
Management Is Needed To Facilitate the  
Closure of Office of Inspector General  
Recommendations Addressed to the  
Bureau of Information Resource  
Management**

MANAGEMENT ASSISTANCE REPORT

## CONTENTS

---

(U) OBJECTIVE .....	1
(U) BACKGROUND .....	2
(U) Bureau of Information Resource Management .....	2
(U) OIG Compliance Process .....	2
(U) Scope of Project .....	3
(U) RESULTS .....	4
(U) CONCLUSION .....	20
(U) RECOMMENDATIONS .....	25
(U) APPENDIX A: OPEN RECOMMENDATIONS RELATED TO RISK MANAGEMENT .....	26
(U) APPENDIX B: OPEN RECOMMENDATION RELATED TO SUPPLY CHAIN RISK MANAGEMENT .....	29
(U) APPENDIX C: OPEN RECOMMENDATIONS RELATED TO CONFIGURATION MANAGEMENT .....	30
(U) APPENDIX D: OPEN RECOMMENDATIONS RELATED TO IDENTITY AND ACCESS MANAGEMENT .....	38
(U) APPENDIX E: OPEN RECOMMENDATIONS RELATED TO DATA PROTECTION AND PRIVACY .....	41
(U) APPENDIX F: OPEN RECOMMENDATIONS RELATED TO SECURITY TRAINING .....	43
(U) APPENDIX G: OPEN RECOMMENDATIONS RELATED TO INFORMATION SECURITY CONTINUOUS MONITORING .....	44
(U) APPENDIX H: OPEN RECOMMENDATIONS RELATED TO CONTINGENCY PLANNING .....	45
(U) APPENDIX I: OPEN RECOMMENDATIONS RELATED TO GENERAL IT POLICIES .....	46
(U) APPENDIX J: OPEN RECOMMENDATIONS RELATED TO INFORMATION SYSTEM SECURITY OFFICERS .....	47
(U) APPENDIX K: OPEN RECOMMENDATIONS RELATED TO IT INVESTMENTS .....	48
(U) APPENDIX L: OPEN RECOMMENDATIONS RELATED TO SHARED SERVICES .....	51
(U) APPENDIX M: OPEN RECOMMENDATIONS RELATED TO other IT-related issues .....	53
(U) APPENDIX N: ACTING UNDER SECRETARY FOR MANAGEMENT'S RESPONSE .....	54

## **(U) Summary of Project**

(U) The purpose of this Management Assistance Report is to present the Office of Inspector General's (OIG) analysis of unclassified OIG recommendations addressed to the Bureau of Information Resource Management (IRM) that were open as of July 30, 2021. The OIG analysis was performed to identify duplicative recommendations and to group the open recommendations by topic area (see Appendices A-M) to highlight their importance and facilitate management action to close them.

(U) On the basis of its analysis, OIG determined that 3 of 107 unclassified, open recommendations from 19 reports addressed to IRM were duplicative. As a result, OIG is closing these recommendations with the issuance of this report. Furthermore, in August 2021, OIG closed an additional 14 of 107 recommendations addressed to IRM as part of its compliance process. With respect to the remaining 90 unclassified, open recommendations, it is important to note that some of these recommendations have remained open since 2014. In addition, as of August 2021, OIG has 26 open recommendations related to configuration management, which the National Institute of Standards and Technology (NIST) considers to be critical in "providing adequate information security and supporting an organization's risk management process."<sup>1</sup>

(U) According to the Foreign Affairs Manual (FAM), the Under Secretary for Management is the Department's designated OIG follow-up official who is responsible for ensuring that corrective action is taken on OIG recommendations.<sup>2</sup> Therefore, to facilitate the closure of the unclassified, open recommendations addressed to IRM, OIG offered two recommendations to the Acting Under Secretary for Management. On the basis of the Acting Under Secretary for Management's response to a draft of this report, OIG considers one recommendation unresolved and one recommendation closed. A synopsis of the Acting Under Secretary for Management's response to the recommendations offered and OIG's reply follow each recommendation in the Conclusion section of this report. The Acting Under Secretary for Management's response is reprinted in its entirety in Appendix N.

## **(U) OBJECTIVE**

---

(U) During FY 2021, Department of State (Department) officials stated that they believed that some of OIG's unclassified, open recommendations addressed to IRM were duplicative and requested that OIG review the open recommendations and take action to close any recommendations determined to be duplicative. OIG analyzed its unclassified, open recommendations addressed to IRM (as of July 30, 2021) to identify duplicative recommendations that warrant closure and to group the unclassified, open recommendations by topic area to highlight their importance and facilitate management action to address them.

---

<sup>1</sup> (U) NIST, Special Publication (SP) 800-128, "Guide for Security-Focused Configuration Management of Information Systems," 1 (August 2011).

<sup>2</sup> (U) 1 FAM 044.1(10)(d), "Responsibilities."

## **(U) BACKGROUND**

---

### **(U) Bureau of Information Resource Management**

(U) IRM's objective is to foster innovative, effective, and interconnected diplomacy by improving, modernizing, and refreshing the Department's tools and services. According to the FAM, the Chief Information Officer, who is the head of IRM, is responsible for establishing effective information resource management policies and for developing and administering the Department's computer and information security programs and policies.<sup>3</sup> The FAM also states that the Chief Information Officer is responsible for establishing policies, plans, and programs and overseeing specific operations to ensure that the Department's information resource management, information systems, and information technology is designed, acquired, operated, maintained, monitored, and evaluated. The Department's information resource management, information systems, and information technology must comply with all applicable requirements and support the efficient, cost-effective, and timely achievement of strategic Department missions. The strategic missions include security (in coordination with the Bureau of Diplomatic Security), configuration management (in coordination with the Bureau of Diplomatic Security), workforce planning, information system modernization, and IT architecture.<sup>4</sup>

### **(U) Under Secretary for Management**

(U) The Under Secretary for Management serves as a principal adviser to the Secretary of State on all matters involving the allocation of Department resources and develops and executes management policies.<sup>5</sup> The Under Secretary is also responsible for the Department's information security program.<sup>6</sup> According to the FAM, the Under Secretary for Management is the Department's designated OIG follow-up official who is responsible for ensuring that timely responses are made to all OIG recommendations, regardless of implementation responsibilities, and that corrective actions are actually taken.<sup>7</sup>

### **(U) OIG Compliance Process**

(U) The Office of Management and Budget requires each agency to ensure that systems are in place to promptly and properly resolve and implement audit recommendations.<sup>8</sup> The Department's FAM establishes policies for compliance with OIG recommendations.<sup>9</sup> OIG has implemented a formal compliance process. The OIG compliance process includes the activities

---

<sup>3</sup> (U) 1 FAM 271.1(1) and (4), "Policy."

<sup>4</sup> (U) 1 FAM 271.2e(6), "Responsibilities."

<sup>5</sup> (U) 1 FAM 044.1(2) and (3), "Responsibilities."

<sup>6</sup> (U) 1 FAM 044.1(7).

<sup>7</sup> (U) 1 FAM 044.1(10)(b) and (d).

<sup>8</sup> (U) Office of Management and Budget Circular A-50, "Audit Followup," § 5, "Policy" (September 29, 1982).

<sup>9</sup> (U) 1 FAM 056, "Audit and Inspection Recommendation Compliance."

needed to track the status of recommendations and verify that corrective actions have been taken to implement the reports' agreed-upon findings and recommendations.

(U) Specifically, upon issuance of a draft report, OIG allows bureaus 14 days to provide their official written response related to the recommendations included in the draft report. OIG requests that responses to the draft report include a management decision indicating agreement or disagreement with recommended actions. When issuing a final audit report, OIG instructs action entities to provide OIG with a written response for each recommendation within 30 calendar days from the date of the transmittal memorandum or letter accompanying the final report. When the Department agrees with a recommendation, OIG asks management to provide a progress report describing planned actions to implement the recommendation and the corresponding implementation milestone date. When management disagrees with a recommendation, OIG asks management to explain the reason for the disagreement and provide alternative actions that can be taken to meet the intent of the recommendation.

(U) OIG considers a recommendation unresolved, resolved, or closed based on actions that the Department has taken or plans to take in response to the recommendation. A recommendation is considered unresolved if there is no agreement between OIG and management on the recommendation or proposed corrective action. A recommendation is considered resolved when there is an agreement on the recommendation and proposed corrective action, but implementation has not been completed. Open recommendations include both unresolved and resolved recommendations. A recommendation is considered closed when the agreed-upon action has been completed.

(U) In accordance with the Inspector General Act of 1978, as amended,<sup>10</sup> OIG is required to semiannually provide Congress with a summary of each OIG report "issued before the commencement of the reporting period . . . for which no management decision has been made by the end of the reporting period," and also "for which no establishment comment was returned within 60 days of providing the report to the establishment."

## **(U) Scope of Project**

(U) This project assessed 107 unclassified, open OIG recommendations from 19 reports addressed to IRM as of July 30, 2021. OIG grouped the unclassified, open recommendations by topic area to highlight their importance. For example, to highlight recommendations that are key to improving the Department's IT security posture, OIG grouped recommendations into domains identified in the "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1."<sup>11</sup> The domains are risk

---

<sup>10</sup> (U) 5 United States Code, Appendix, "Inspector General Act of 1978," § 5(10)(A) and (B), "Semiannual reports; transmittal to Congress; availability to public; immediate report on serious or flagrant problems; disclosure of information; definitions."

<sup>11</sup> (U) Office of Management and Budget, Department of Homeland Security, Council of the Inspectors General on Integrity and Efficiency, "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1," 5 (May 12, 2021).

management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, and contingency planning.<sup>12</sup> OIG also identified recommendations that impacted IT security and internal control topics (general IT policies, general Information System Security Officer duties, and IT investments). Furthermore, OIG identified recommendations that related to shared services and recommendations that did not relate to other topics areas, which OIG grouped under the heading of Other IT-Related Issues.

## (U) RESULTS

---

(U) On the basis of its analysis, OIG determined that 3 of 107 unclassified, open recommendations addressed to IRM were duplicative. Specifically, with the issuance of this report, OIG will close one duplicative recommendation related to risk management, one related to data protection and privacy, and one related to general IT policies. OIG closed an additional 14 recommendations in August 2021 as part of its normal compliance process. The remaining 90 unclassified, open recommendations, which OIG grouped by topic area, remain relevant and require attention to close them. To facilitate closing the unclassified, open recommendations addressed to IRM, OIG made two recommendations to the Under Secretary for Management.

### **(U) Risk Management**

(U) OIG identified 11 unclassified, open recommendations that relate to risk management, which are listed in Appendix A. According to NIST, risk management is “the program and supporting processes to manage information security risk.”<sup>13</sup> NIST also states that organizations depend on

information systems to successfully carry out their missions and business functions . . . . Information systems are subject to serious *threats* that can have adverse effects on organizational operations (i.e., 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 availability of the information being processed, stored, or transmitted by those systems . . . . Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk.<sup>14</sup>

(U) IRM officials indicated that they believed that a recommendation related to risk management from a report issued in April 2021 was duplicative with recommendations from a

---

<sup>12</sup> (U) The FISMA Reporting Metrics also include a domain related to incident response. However, OIG did not identify open recommendations related to the incident response metric.

<sup>13</sup> (U) NIST SP 800-53, rev. 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” B-19 (January 22, 2015).

<sup>14</sup> (U) NIST SP 800-39, “Managing Information Security Risk: *Organization, Mission, and Information System View*,” 1 (March 2011).

report issued in October 2018. The recommendations identified by IRM are presented as follows.

***(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25, April 2021)***

**Recommendation 24:** ~~(SBU)~~ (b) (7)(E)  
(b) (7)(E)



***(U) Audit of the Department of State Information Security Program (AUD-IT-19-08, October 2018)***

**Recommendation 4:** (U) OIG recommends that the Chief Information Officer (a) develop and maintain a comprehensive, accurate, and up-to-date organization-wide information system inventory in accordance with National Institute of Standards and Technology Special Publication 800-53 and (b) report quarterly to the Deputy Secretary and other Department of State stakeholders about the progress made until an organization-wide information system inventory is realized and independently verified for completeness.

**Recommendation 5:** (U) OIG recommends that the Chief Information Officer identify and assign the necessary resources to develop and maintain a comprehensive, accurate, and up-to-date organization-wide information system inventory in accordance with National Institute of Standards and Technology Special Publication 800-53.

(U) OIG found that the recommendation cited by IRM from AUD-IT-21-25 was not included in the final report. Specifically, as noted in AUD-IT-21-25, OIG removed the recommendation from the final report on the basis of IRM's comments on the draft report. Therefore, there was no duplication related to the recommendations identified by IRM. However, in addition to assessing IRM's comments, OIG analyzed other recommendations related to risk management to identify potential duplication and identified a recommendation from a report issued in November 2014 that was duplicative with a recommendation from a report issued in April 2021. The duplicative recommendations identified by OIG are presented as follows.


***(U) Audit of the Department of State Information Security Program (AUD-IT-15-17, November 2014)***

**Recommendation 21:** (U) 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) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25, April 2021)***

**Recommendation 4:** ~~(SBU)~~ (b) (7)(E)  
(b) (7)(E)

A large black rectangular redaction box covers the majority of the text in this section, starting below the recommendation header and extending down to the start of the next paragraph.

(U) OIG assessed these two recommendations and determined that, although there are some minor differences, the differences are not substantive. Specifically, should IRM implement Recommendation 4 from report AUD-IT-21-25, it would meet the intent of Recommendation 21 in report AUD-IT-15-17. Therefore, OIG is closing Recommendation 21 from report AUD-IT-15-17 with the issuance of this report, and no further action specific to this recommendation is required.

~~(SBU)~~ (b) (7)(E)  
(b) (7)(E)

A large black rectangular redaction box covers the majority of the text in this section, starting below the redaction code and extending down to the start of the next section header.

***(U) Supply Chain Risk Management***

(U) OIG identified one unclassified, open recommendation that relates to supply chain risk management, which is listed in Appendix B. According to NIST, a supply chain is a “[l]inked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing,

---

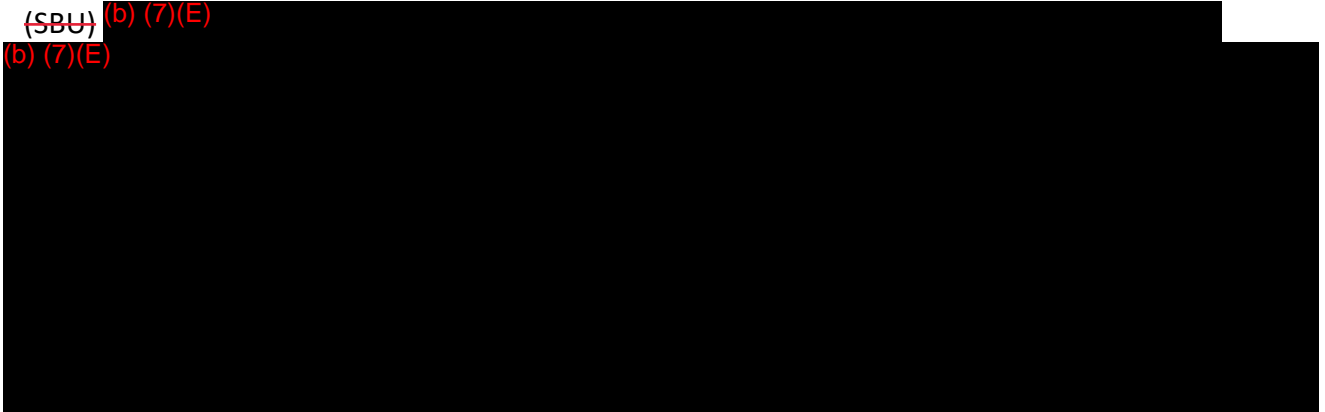
<sup>15</sup> (U) OIG, *Audit of the Department of State FY 2020 Information Security Program* 25-26 (AUD-IT-21-25, April 2021).

<sup>16</sup> (U) According to the “FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0” 6 (April 17, 2020), Level 4 is considered an effective level of security. In AUD-IT-21-25, April 2021, at 25-26, OIG reported that the Department’s risk management program for FY 2020 was at a Level 2. According to the “FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0,” at 6, Level 2 is when policies, procedures, and strategies are formalized and documented, but are not consistently implemented.



processing, handling, and delivery of products and services to the acquirer.”<sup>17</sup> NIST indicates that adversaries are using the supply chain as an attack vector and as an effective means of penetrating an organization’s systems, compromising the integrity of system elements, and gaining access to critical assets.<sup>18</sup> Neither IRM nor OIG identified any duplicate recommendations related to supply chain risk management.

(SBU) (b) (7)(E)  
(b) (7)(E)



### ***(U) Configuration Management***

(U) OIG identified 35 unclassified, open recommendations that relate to configuration management, which are listed in Appendix C. According to NIST, configuration management is a “collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.”<sup>19</sup> A system is composed of many components that can be interconnected in a multitude of arrangements to meet the needs of the organization. NIST states that “[h]ow system components are networked, configured, and managed is critical in providing adequate information security and supporting an organization’s risk management process.” A system is typically in a constant state of change in response to new, enhanced, corrected, or updated hardware and software, which almost always results in changes to system configuration. NIST states that “[t]o ensure that the required adjustments to the system configuration do not adversely affect the security of the system or the organization . . . a well-defined configuration management process that integrates information security is needed.”<sup>20</sup>

(U) IRM officials indicated that they believed that a recommendation related to configuration management from a report issued in April 2021 was duplicative with recommendations from a report issued in September 2017. The recommendations identified by IRM are presented as follows.

---

<sup>17</sup> (U) NIST SP 800-53, rev. 4, at B-24.

<sup>18</sup> (U) NIST SP 800-37, rev. 2, “Risk Management Framework for Information Systems and Organizations,” v (December 2018).

<sup>19</sup> (U) NIST SP 800-53, rev. 4, at B-5.

<sup>20</sup> (U) NIST SP 800-128, at 1.

***(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25, April 2021)***

**Recommendation 8:** ~~(SBU)~~ (b) (7)(E)  
(b) (7)(E)

***(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64, September 2017)***

**Recommendation 1:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a detailed program plan for the Information Technology Configuration Control Board process that includes clear goals and attainable objectives and defines areas of authority and responsibility.

**Recommendation 2:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a process to establish and periodically update a list of system, product, or software owners who will be authorized to make change requests for their system, product, or software. The list should be made available to users and members of the Information Technology Configuration Control Board through the Information Technology Configuration Control Board website or applicable policies and procedures outlined in Recommendation 12.

**Recommendation 3:** (U) OIG recommends that the Bureau of Information Resource Management determine what documentation is needed to support a change request and modify the policies and procedures outlined in Recommendation 12 or other guidance, such as the submitters guide, provided to change request submitters to reflect the documentation that is required for a complete and accurate change request submission.

**Recommendation 4:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement guidance for change requests to require and include: (a) minimum testing standards for change requests, (b) instructions that testing be performed in advance of the change request being submitted and that the testing documentation be submitted as part of the change request process, and (c) a clearly defined technical review of the testing documentation that is submitted to verify the documentation complies with minimum standards.

**Recommendation 5:** (U) OIG recommends that the Bureau of Information Resource Management remove the default proceed ability for Technical Reviewers in the Virtual Information Technology Configuration Control Board application.

**Recommendation 6:** (U) OIG recommends that the Bureau of Information Resource Management formally notify all Technical Reviewers that default proceeds are no longer allowed and that all Technical Reviewers must review all change requests and either

approve, stop, or reject the change request. Policies and procedures outlined in Recommendation 12 or other guidance should be updated to reflect this change to the process.

**Recommendation 7:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a quality assurance assessment process for all change requests going through the enterprise-wide Information Technology Configuration Control Board. At a minimum, the quality assurance process should include periodic evaluation of open “stops,” reviews to ensure retention of all relevant documentation, and a final check prior to adding change to the baseline to ensure all pertinent process controls occurred at a minimum.

**Recommendation 10:** (U) OIG recommends that the Bureau of Information Resource Management define the roles, responsibilities, and technical skillsets for each technical review and voting area and develop and implement a vetting process to verify Technical Reviewers and Voters have the knowledge, skills, and abilities to perform their assigned duties related to the Information Technology Configuration Control Board process.

**Recommendation 11:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a process to verify that Technical Reviewers and Voters have formally appointed alternatives.

**Recommendation 12:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement complete and consistent policies and procedures and supplemental guidance, such as a Submitter’s Guide, for the Information Technology Configuration Control Board process. The policies, procedures, and guidance should, at a minimum, include guidance on roles and responsibilities, detailed procedure steps for submitters, minimum testing requirements, instructions on how Technical Reviewers and Voters should conduct their review, the appropriate use of “stops,” and established timelines for the process.

**Recommendation 13:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a process to periodically review and validate the accuracy and completeness of the data in the Virtual Information Technology Configuration Control Board database and to correct data integrity, omissions and inaccuracies existing between the new and old databases and when identified going forward. As part of this effort, the Bureau of Information Resource Management should ensure that the old database is available solely as a read-only reference resource and that new data cannot be entered into that database.

**Recommendation 14:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement required, periodic, training for Information Technology Configuration Control Board management and personnel, Bureau Sponsors,

Technical Reviewers, Voters, and change request submitters involved in the Information Technology Configuration Control Board process.

**Recommendation 15:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to (a) monitor the status of all change requests throughout each stage of the change request process and (b) notify stakeholders when a request is nearing the end of a deadline or when an event occurs that may affect the deadline for a change request.

**Recommendation 16:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement policies and procedures to hold officials accountable for failure to meet established deadlines in the Information Technology Configuration Control Board change request process. Once completed, the policies, procedures, and supplemental guidance discussed in Recommendation 12 should be updated.

**Recommendation 17:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to periodically gather, assess, and report on its change request review process timeliness metrics and to make those results available to its stakeholders and customers in addition to appropriate bureau officials.

(SBU) (b) (7)(E)

(b) (7)(E)

(U) IRM also indicated that there may be duplication in the recommendations listed related to the Information Technology Change Control Board and recommendations from *Audit of the Department of State's Local Configuration Control Boards* (AUD-IT-19-36, July 2019).<sup>21</sup> However, the recommendations offered in report AUD-IT-19-36 relate to Configuration Control Boards located at posts, while the recommendations from report AUD-IT-21-25 and report AUD-IT-17-64 relate to the Department's domestic Change Control Board. Therefore, OIG did not identify any duplication in the recommendations identified by IRM. In addition to assessing IRM's comments, OIG analyzed other recommendations related to configuration management to identify potential duplication and did not identify any duplicative recommendations.

(SBU) (b) (7)(E)

(b) (7)(E)

<sup>21</sup> (U) See Appendix C, items 28-33, for details of the recommendations from AUD-IT-19-36.

(b) (7)(E)



**(U) Identity and Access Management**

(U) OIG identified 11 unclassified, open recommendations that relate to identity and access management, which are listed in Appendix D. According to NIST, “digital identity is the unique representation of a subject engaged in an online transaction.” NIST also states that “[i]dentity proofing establishes that a subject is who they claim to be. Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate.”<sup>24</sup> Proving someone is who they say they are—especially remotely—could prevent an attacker from successfully impersonating someone.<sup>25</sup>

(U) IRM officials indicated that they believed that a recommendation related to identity and access management from a report issued in October 2014 was duplicative with recommendations from a report issued in February 2021. The recommendations identified by IRM are presented as follows.

**(U) Audit of the Department of State Implementation and Oversight of Active Directory (AUD-IT-15-05, October 2014)**

**Recommendation 5:** (SBU) (b) (7)(E)

(b) (7)(E)



---

<sup>22</sup> (U) AUD-IT-21-25, April 2021, at 26.

<sup>23</sup> (U) According to the “FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0,” Level 4 is considered an effective level of security, 6. In AUD-IT-21-25, April 2021, at 26, OIG reported that the Department’s configuration management program for FY 2020 was at Level 3. According to the “FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0,” at 6, Level 3 is when policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

<sup>24</sup> (U) NIST SP 800-63-3, “Digital Identity Guidelines,” 2 (June 2017).

<sup>25</sup> (U) Ibid., at iv.

**(U) Management Assistance Report: Deficiencies in Management of Active Directory Privileged Accounts and Security Groups at Overseas Posts (ISP-21-13, February 2021)**

**Recommendation 1:** (SBU) (b) (7)(E)

(b) (7)(E)

**Recommendation 2:** (SBU) (b) (7)(E)

(b) (7)(E)

**Recommendation 3:** (SBU) (b) (7)(E)

(b) (7)(E)

(SBU) (b) (7)(E)

(b) (7)(E)

(U) IRM officials also indicated that they believed that a recommendation related to identity and access management from a report issued in October 2014 was duplicative with a recommendation from a report issued in September 2017. The recommendations identified by IRM are presented as follows.

**(U) Audit of the Department of State Implementation and Oversight of Active Directory (AUD-IT-15-05, October 2014)**

**Recommendation 4:** (SBU) (b) (7)(E)

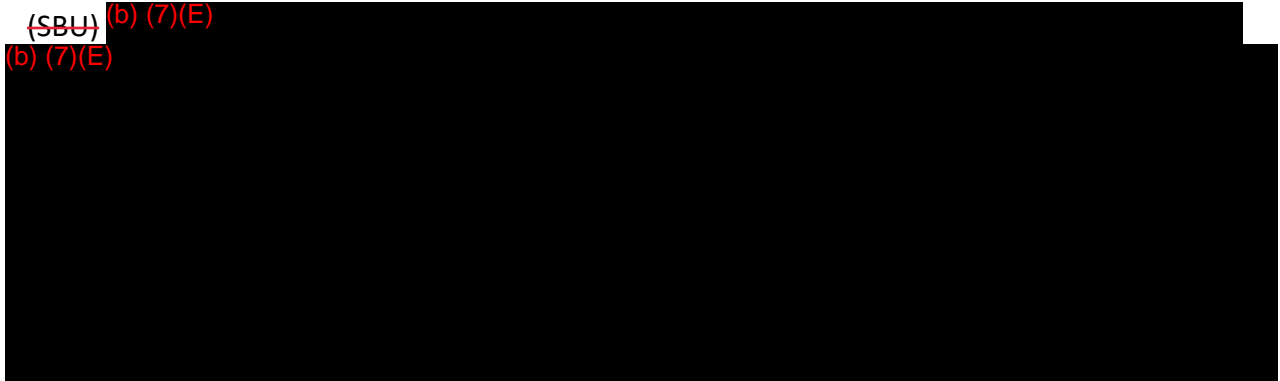
(b) (7)(E)

***(U) Audit of the Department of State Access Controls for Major Applications (AUD-IT-17-62, September 2017)***


**Recommendation 13:** (SBU) (b) (7)(E)

(b) (7)(E)

(SBU) (b) (7)(E)  
(b) (7)(E)



(SBU) (b) (7)(E)  
(b) (7)(E)



***(U) Data Protection and Privacy***

(U) OIG identified six unclassified, open recommendations that relate to data protection and privacy, which are listed in Appendix E. According to NIST, data about individuals flow through a complex IT ecosystem. Failure to manage privacy risks can have direct, adverse consequences at both the individual and societal levels. Finding ways to process data while protecting individuals' privacy is challenging.<sup>28</sup>

(U) IRM did not identify any recommendations that it considered to be duplicative related to data protection and privacy. However, OIG analyzed recommendations related to data protection and privacy to identify potential duplication and identified a recommendation from a report issued in October 2018 that was duplicative of a recommendation from a report issued in April 2021. The duplicative recommendations identified by OIG are presented as follows.

---

<sup>26</sup> (U) AUD-IT-21-25, April 2021, at 26.

<sup>27</sup> (U) According to the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0" 6, Level 4 is considered an effective level of security. In AUD-IT-21-25, April 2021, at 26, OIG reported that the Department's identity and access management program for FY 2020 was at a Level 2. According to the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0," at 6, Level 2 is when policies, procedures, and strategies are formalized and documented, but are not consistently implemented.

<sup>28</sup> (U) NIST, "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0," 1 (January 16, 2020).

***(U) Audit of the Department of State Sanitization of Information Technology Media Before Disposal (AUD-IT-19-02, October 2018)***

**Recommendation 6:** (U) OIG recommends that the Bureau of Information Resource Management, unless designated otherwise by the Under Secretary for Management, establish and implement a process to periodically, but not less than annually, review and update, as necessary, the Department of State IT media sanitization policies to reflect current Federal requirements for IT media sanitization.

***(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25, April 2021)***

**Recommendation 2:** (SBU) (b) (7)(E)

(b) (7)(E)

(SBU) (b) (7)(E)

(b) (7)(E)

(SBU) (b) (7)(E)

(b) (7)(E)

***(U) Security Training***

(U) OIG identified four unclassified, open recommendations that related to security training, which are listed in Appendix F. According to NIST

[a] strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical

---

<sup>29</sup> (U) AUD-IT-21-25, April 2021, at 26.

<sup>30</sup> (U) According to the “FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0,” at 6, Level 4 is considered an effective level of security. In AUD-IT-21-25, April 2021, at 26, OIG reported that the Department’s data protection and privacy program for FY 2020 was at Level 3. According to the “FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0,” at 6, Level 3 is when policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.



controls necessary and available to secure IT resources. In addition, those in the agency who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because security of agency resources is as much a *human issue* as it is a technology issue.<sup>31</sup>

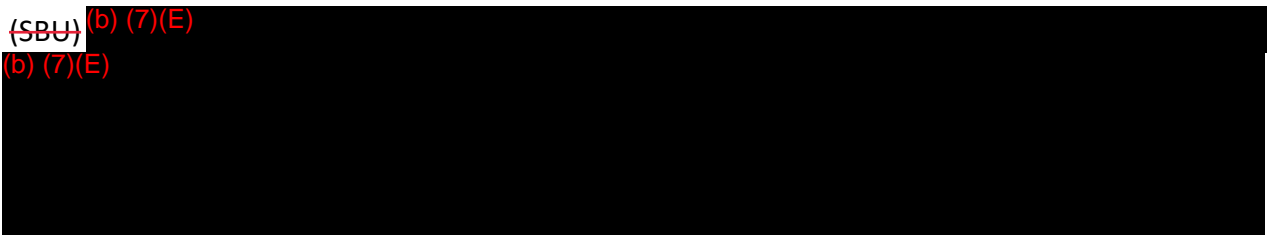
Neither IRM nor OIG identified any duplicative recommendations related to security training.

(U) It is important that IRM take action to address the four open recommendations involving security training because without an adequate security training program, Department users may compromise the security of the network, which may result in the loss of information or the introduction of vulnerabilities to systems. In its FY 2020 FISMA report, OIG reported that the Department's security training program was ineffective.<sup>32,33</sup> Therefore, to improve its cybersecurity posture, it is essential that the Department address the four open OIG recommendations related to data protection and privacy.

**(U) Information System Continuous Monitoring**

(U) OIG identified four unclassified, open recommendations that relate to information system continuous monitoring, which are listed in Appendix G. NIST defines information security continuous monitoring as "maintaining ongoing awareness of information security, vulnerabilities, and threats." NIST states that "many, if not all, of an organization's mission-critical functions are dependent upon [IT]" and so the ability to "assure confidentiality, integrity, and availability of information is . . . mission-critical." Therefore, NIST states that ongoing monitoring is a critical part of the risk management process.<sup>34</sup> Neither IRM nor OIG identified any duplicative recommendations related to information system continuous monitoring.

(SBU) (b) (7)(E)  
(b) (7)(E)



---

<sup>31</sup> (U) NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," ES-1 (October 2003).

<sup>32</sup> (U) AUD-IT-21-25, April 2021, at 27.

<sup>33</sup> (U) According to the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0," at 6, Level 4 is considered an effective level of security. In AUD-IT-21-25, at 27, OIG reported that the Department's security training program for FY 2020 was at Level 2. According to the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0," at 6, Level 2 is when policies, procedures, and strategies are formalized and documented, but are not consistently implemented.

<sup>34</sup> (U) NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," vi (September 2011).

(b) (7)(E)



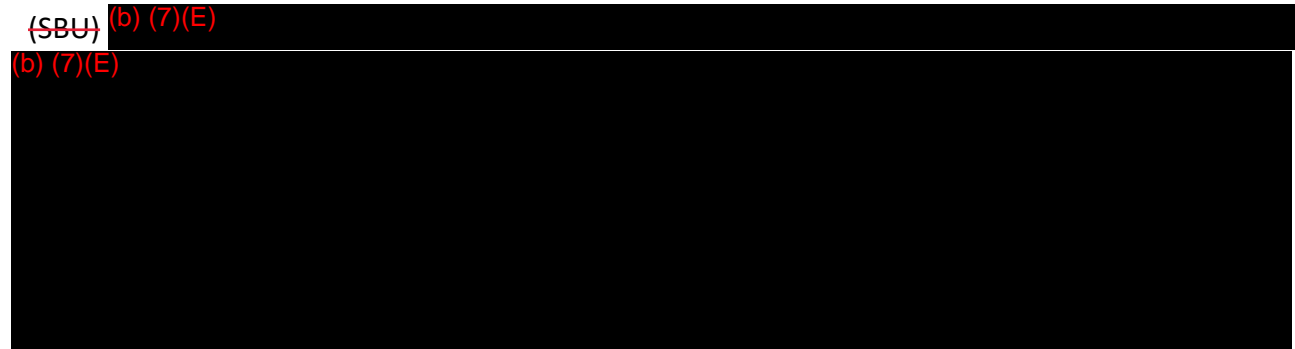
**(U) Contingency Planning**

(U) OIG identified four unclassified, open recommendations that relate to contingency planning, which are listed in Appendix H. According to NIST

[i]nformation systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.<sup>37</sup>

Neither IRM nor OIG identified any duplicative recommendations related to contingency planning.

(SBU) (b) (7)(E)



(b) (7)(E)

---

<sup>35</sup> (U) AUD-IT-21-25, April 2021, at 27.

<sup>36</sup> (U) According to the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0," at 6, Level 4 is considered an effective level of security. In AUD-IT-21-25, OIG reported that the Department's information system continuous monitoring program for FY 2020 was at Level 1. According to the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0," at 6, Level 1 is when policies, procedures, and strategies are not formalized and activities are performed in an ad-hoc, reactive manner.

<sup>37</sup> (U) NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal information Systems," 1 (May 2010).

<sup>38</sup> (U) AUD-IT-21-25, April 2021, at 28.

<sup>39</sup> (U) According to the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0," at 6, Level 4 is considered an effective level of security. In AUD-IT-21-25, at 28, OIG reported that the Department's contingency planning program for FY 2020 was at Level 2. According to the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0," at 6, Level 2 is when policies, procedures, and strategies are formalized and documented, but are not consistently implemented.

**(U) General IT Policies**

(U) OIG identified two unclassified, open recommendations that relate to general IT policies, which are listed in Appendix I. Developing policies and procedures is an important component of an agency's internal control environment.<sup>40</sup> Agencies should document in their policies the design of control activities, how those control activities should be implemented, and guidance on how to determine if the control activities are operating effectively. Agencies should also document policies at the appropriate level to allow management to effectively monitor control activities. Offices may further define policies through day-to-day procedures. Management should communicate policies and procedures so employees can implement control activities for their assigned responsibilities.<sup>41</sup>

(U) IRM officials indicated that they believed that a recommendation related to general IT policies from a report issued in April 2018 was duplicative with a recommendation from a report issued in April 2021. The recommendations identified by IRM are presented as follows.

**(U) Inspection of the Bureau of Information Resource Management's Office of Governance, Resource, and Performance Management (ISP-I-18-15, April 2018)**

**Recommendation 10:** (U) The Bureau of Information Resource Management should implement procedures to ensure regularly scheduled reviews and updates to the Department's information technology management policies and procedures in Volume 5 of the Foreign Affairs Manual and its associated Foreign Affairs Handbooks.

**(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25, April 2021)**

**Recommendation 2:** (SBU) (b) (7)(E)  
(b) (7)(E)

(U) OIG assessed the two recommendations and determined that they are duplicative. Because Recommendation 2 from report AUD-IT-21-25 addresses all IT security-related policies and procedures, which would include Volume 5 of the FAM and the Foreign Affairs Handbook, OIG is closing Recommendation 10 from ISP-I-18-15 with the issuance of this report, and no further action specific to this recommendation is required.

(U) It is important that IRM take action to address the open recommendation involving general IT policies because information security policies are an essential component of information security governance—without the policy, governance has no substance and rules to enforce. NIST states that “[a]gencies should ensure that their information security policy is sufficiently

<sup>40</sup> (U) The Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014), 5, defines internal control as a process “that provides reasonable assurance that the objectives of an entity will be achieved.”

<sup>41</sup> (U) *Ibid.*, at 56.

current to accommodate the information security environment and agency mission and operational requirements. To ensure that information security does not become obsolete, agencies should implement a policy review and revision cycle.”<sup>42</sup> Therefore, to improve cybersecurity and internal controls, it is essential that the Department address the open OIG recommendation related to IT policies.

### **(U) Information System Security Officers**

(U) OIG identified three unclassified, open recommendations that relate to Information System Security Officers, which are listed in Appendix J. According to NIST, an Information System Security Officer is an “[i]ndividual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.”<sup>43</sup> Neither IRM nor OIG identified any duplicate recommendations related to Information System Security Officers.

(U) OIG first identified pervasive Information System Security Officer concerns in 2017, and OIG continues to identify these concerns. It is important that IRM take action to address the three open recommendations involving Information System Security Officers because failure to perform required Information System Security Officer responsibilities increases the risk of unauthorized access and malicious activity to the Department’s networks. Also, without a systemic approach to monitoring networks and recording findings, Department networks could be breached, and information security compromised.<sup>44</sup> Therefore, it is essential that the Department address the three open OIG recommendations related to Information System Security Officers.

### **(U) IT Investments**

(U) OIG identified 13 unclassified, open recommendations that relate to IT investments, which are listed in Appendix K. IT resources are critical to the U.S. social, political, and economic well-being. Specifically, IT resources allow agencies to provide quality services to citizens, generate and disseminate knowledge, and facilitate greater productivity and advancement. Because of the importance of IT resources, the Office of Management and Budget requires agencies to establish “a comprehensive approach to improve the acquisition” of information systems, including “implementing an IT investment management process that links to and supports budget formulation and execution.”<sup>45</sup> NIST also states that “[i]ncreased competition for limited [F]ederal budgets and resources requires that agencies allocate available funding toward their highest-priority information security investments.” The goal can be achieved through a formal

---

<sup>42</sup> (U) NIST SP 800-100, “Information Security Handbook: A Guide for Managers,” 14 (October 2006).

<sup>43</sup> (U) NIST SP 800-53, rev. 4, at B-11.

<sup>44</sup> (U) OIG, *Inspector General Statement on the Department of State’s Major Management and Performance Challenges, Fiscal Year 2020* 10 (OIG-EX-21-01).

<sup>45</sup> (U) Office of Management and Budget Circular A-130, “Managing Information as a Strategic Resource,” 4 (July 28, 2016).

enterprise capital planning and investment control process designed to facilitate and control the expenditure of funds.<sup>46</sup>

(U) Neither IRM nor OIG identified any duplicative recommendations related to IT investments. However, in August 2021, OIG closed five recommendations (Recommendations 8, 12, 13, 14, and 17) from report AUD-FM-16-31 based on work performed during a compliance follow-up audit,<sup>47</sup> which are presented as follows.

**(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31, March 2016)**

**Recommendation 8:** (U) OIG recommends that the Bureau of Information Resource Management establish and implement a plan to review IT investment reorganizations that occurred since FY 2010 to ensure that the investments resulting from the reorganizations comply with Office of Management and Budget requirements for information technology investments.

**Recommendation 12:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a process to perform periodic, but no less than annual, reviews of the entire agency IT portfolio to enforce bureau accountability and identify potential duplicative systems.

**Recommendation 13:** (U) For duplicative systems that are identified by the new process implemented to perform periodic reviews of the entire agency IT portfolio (Recommendation 12), OIG recommends that the Bureau of Information Resource Management develop and implement a strategy to combine, eliminate, or replace duplicative systems, as practicable.

**Recommendation 14:** (U) OIG recommends that the Bureau of Information Resource Management develop and implement a strategy to perform semiannual or more frequent reviews of bureau-funded IT contracts to identify new IT investments developed as part of the contracts.

**Recommendation 17:** (U) OIG recommends that the Bureau of Information Resource Management (a) develop and implement a policy requiring bureaus and offices to provide details of IT investments, programs, and projects in iMatrix and (b) develop and disseminate guidance specifying the level of detail necessary for each investment, including general descriptions and technical capabilities.

---

<sup>46</sup> (U) NIST SP 800-100, at 35.

<sup>47</sup> (U) OIG, *Compliance Follow-up Audit of the Department of State Process To Select and Approve IT Investments* (AUD-IT-21-34, August 2021).

(U) The Government Accountability Office identified the management of IT acquisitions and operations to be a high-risk area in the Government.<sup>48</sup> The Government Accountability Office stated that “[F]ederal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes. These investments often suffer from a lack of disciplined and effective management.”<sup>49</sup> Therefore, to improve its IT system environment and ensure the effective use of taxpayer funds, it is essential that the Department address the eight open OIG recommendations related to IT investments.

### **(U) Shared Services**

(U) OIG identified 10 unclassified, open recommendations that relate to shared services, which are listed in Appendix L. A shared service is a business or mission function that is provided for consumption by multiple organizations within an agency. The goal of shared services is to efficiently aggregate resources and systems to improve the quality, timeliness, and cost-effectiveness of service delivery to customers. Intra-agency shared services can be impactful in improving mission functions, reducing costs, and increasing collaboration. Neither IRM nor OIG identified any duplicate recommendations related to shared services. The use of shared services provides an opportunity to drive efficiencies and cost savings. Therefore, to ensure that bureaus and offices take full advantage of services offered, it is essential that IRM address the 10 open recommendations related to shared services.

### **(U) Other IT-Related Issues**

(U) OIG identified three unclassified, open recommendations that relate to other IT topics, which are listed in Appendix M. Neither IRM nor OIG identified any duplicate recommendations related to other IT-related issues.

## **(U) CONCLUSION**

---

(U) OIG considers information security and management to be a major management challenge for the Department. Specifically, for FY 2020, OIG reported that

[t]he Department depends on information systems to function, and the security of these systems is vital to protecting national and economic security, public safety, and the flow of commerce. The Department acknowledges that its information systems and networks are subject to serious threats that can exploit and compromise sensitive information, and it has taken some steps to address these concerns. However, notwithstanding the expenditure of substantial resources by the Department, OIG continues to identify significant issues that put Department information at risk.<sup>50</sup>

---

<sup>48</sup> (U) Government Accountability Office, *High Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP, March 2, 2021).

<sup>49</sup> (U) *Ibid.*, at 103.

<sup>50</sup> (U) OIG-EX-21-01, at 9-10.

(U) As of July 30, 2021, there were 107 unclassified, open OIG recommendations that were addressed to IRM. Although OIG is closing 3 recommendations with the issuance of this report and closed an additional 14 recommendations in August 2021 as part of its compliance process, the number of open recommendations addressed to IRM is concerning, considering the fundamental IT issues that these recommendations involve. Moreover, 57 percent (61 of 107) of the open recommendations, as of July 30, 2021, are from FY 2019 or earlier, as shown in Table 1.

**(U) Table 1: Number of Unclassified, Open Recommendations Addressed to IRM (as of July 30, 2021) by Fiscal Year of Report Issuance Date**

<b>(U) Fiscal Year</b>	<b>(U) Number of Open Recommendations</b>
(U) 2015	(U) 7
(U) 2016	(U) 13
(U) 2017	(U) 19
(U) 2018	(U) 7
(U) 2019	(U) 15
(U) 2020	(U) 3
(U) 2021	(U) 43
<b>(U) Total</b>	<b>(U) 107</b>

(U) According to NIST, a plan of action and milestones should be prepared for IT controls that have been determined, through independent assessments, to be less than effective.<sup>51</sup> Furthermore, NIST states that organizations should develop a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified and to reduce or eliminate known vulnerabilities.<sup>52</sup> NIST also states that the plan of action and milestones should identify the tasks needed to be accomplished, the resources needed to accomplish the elements of the plan, any milestones to meet the tasks, and scheduled completion dates for the milestones.<sup>53</sup>

(U) Because the Under Secretary for Management is responsible for ensuring that corrective actions on OIG recommendations are actually taken,<sup>54</sup> OIG recommends that the Under Secretary monitor the status of corrective actions for the open recommendations addressed to IRM and take actions if necessary until they have been implemented and closed. OIG is therefore offering the following recommendations to the Under Secretary for Management.

---

<sup>51</sup> (U) NIST SP 800-53, rev. 4, at 15.

<sup>52</sup> (U) Ibid., at F-59.

<sup>53</sup> (U) Ibid., at B-16.

<sup>54</sup> (U) 1 FAM 044.1(10)(b) and (d).

**Recommendation 1:** (U) OIG recommends that the Under Secretary for Management verify that the Bureau of Information Resource Management (IRM) has developed plans of action and milestones, as required by the National Institute of Standards and Technology, Special Publication 800-53, rev. 4, to address each open OIG recommendation. The plans of action and milestones should document planned remedial actions to correct the deficiencies identified. If the Under Secretary for Management determines that IRM has not developed or maintained plans of action and milestones for each open OIG recommendation, the Under Secretary for Management should direct IRM to take action to comply with standards.

**(U) Management Response:** The Acting Under Secretary for Management did not concur with this recommendation, stating that the Acting Under Secretary for Management consistently reviews all OIG compliance updates from IRM to ensure that the recommendations are appropriately addressed. Furthermore, the Acting Under Secretary for Management stated that “developing a separate action plan for each recommendation would prove overly cumbersome” and that “IRM’s staff, time, and resources are better spent working on compliance related activities, maintaining a high standard of day-to-day operations, and communicating directly with OIG.” The Acting Under Secretary for Management also stated that OIG closed 21 IRM recommendations since March 2021, “which shows significant progress at the current level of oversight.”

**(U) OIG Reply:** On the basis of the Acting Under Secretary for Management’s response, OIG considers this recommendation unresolved. It is important to note that Federal agencies are required to develop plans of action and milestones (POA&M) to correct identified deficiencies. Specifically, NIST<sup>55</sup> states that organizations must develop a POA&M “for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.”<sup>56</sup> Additionally, the Department’s Foreign Affairs Manual<sup>57</sup> states that POA&Ms are the steps that describe the measures planned to correct deficiencies noted.

(SBU) (b) (7)(E)

(b) (7)(E) 58 (b) (7)(E)

(b) (7)(E) 59 (b) (7)(E)

(b) (7)(E)

<sup>55</sup> (U) Office of Management and Budget, Circular A-130, at Appendix I – 16, states that “[f]or non-national security programs and information systems, agencies must apply NIST guidelines unless otherwise stated by OMB.”

<sup>56</sup> (U) NIST, SP 800-53, rev. 4, Section CA-5, “Plan of Action and Milestones,” F-59.

<sup>57</sup> (U) Department, 5 Foreign Affairs Manual 1066.2-2, “Plan of Action & Milestones (POA&M) Management.”

<sup>58</sup> (U) “FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.1,” at 20.

<sup>59</sup> (U) OIG, *Audit of the Department of State FY 2021 Information Security Program* (AUD-IT-22-06, October 2021), at 7-8.

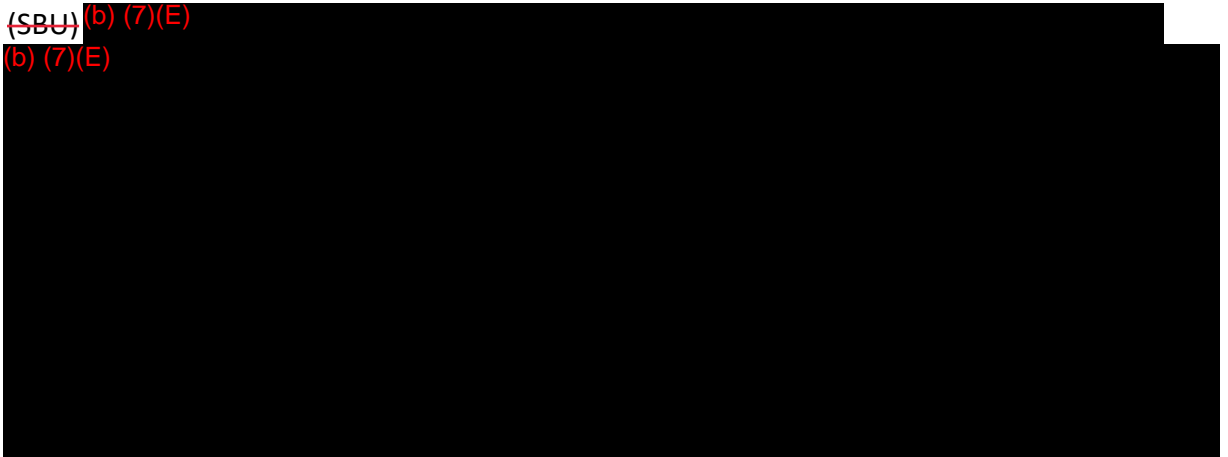


(b) (7)(E)



(U) The Acting Under Secretary for Management's response also pointed out that OIG closed a number of recommendations addressed to IRM. Specifically, from March 2021 (the date cited in the Acting Under Secretary for Management's response) through October 5, 2021 (the date of the Acting Under Secretary for Management's response), OIG closed 23 recommendations addressed either to IRM or the Chief Information Officer. Of those 23 recommendations, 8 (35 percent) were closed when a new OIG report was issued, and the remaining 15 (65 percent) were closed in response to information provided by IRM.<sup>61</sup>

(SBU) (b) (7)(E)  
(b) (7)(E)



(U) Therefore, OIG maintains that the involvement of the Acting Under Secretary for Management is necessary to verify that IRM is developing POA&Ms for each open recommendation as required. In addition, should the Acting Under Secretary for Management determine that IRM has not developed or maintained POA&MS for each open OIG recommendation, the Acting Under Secretary for Management should direct IRM to take action to comply with standards.

(U) This recommendation will be considered resolved when the Acting Under Secretary for Management provides a plan of action for addressing the recommendation or provides an acceptable alternative that meets the intent of the recommendation. The recommendation

---

<sup>60</sup> (U) NIST SP 800-53, rev. 4, at B-19.

<sup>61</sup> (U) OIG reflected the closure of a number of IRM recommendations in this report.

<sup>62</sup> (U) OIG, *Audit of the Department of State Information Security Program* (AUD-IT-15-17, November 2014), 28.

will be closed when OIG receives documentation demonstrating that the Acting Under Secretary for Management has verified that IRM has developed POA&Ms, as required by NIST, to address each open OIG recommendation.

**Recommendation 2:** (U) OIG recommends that the Under Secretary for Management develop and implement a methodology to periodically review the status of the Bureau of Information Resource Management's efforts to implement open OIG recommendations, as described in its plans of action and milestones (Recommendation 1).

**(U) Management Response:** The Acting Under Secretary for Management accepted this recommendation, stating that the Acting Under Secretary for Management already performs oversight activities. For example, the office of the Acting Under Secretary for Management provides a spreadsheet of open recommendations from OIG to IRM, with a high-level visual depiction of IRM's compliance. After IRM provides a response to the Acting Under Secretary for Management, she reviews the data and ensures that IRM is up to date on compliance efforts.

**(U) OIG Reply:** On the basis of the Acting Under Secretary for Management's response, OIG considers this recommendation closed, and no other action is required.

## (U) RECOMMENDATIONS

---

**Recommendation 1:** (U) OIG recommends that the Under Secretary for Management verify that the Bureau of Information Resource Management (IRM) has developed plans of action and milestones, as required by the National Institute of Standards and Technology, Special Publication 800-53, rev. 4, to address each open OIG recommendation. The plans of action and milestones should document planned remedial actions to correct the deficiencies identified. If the Under Secretary for Management determines that IRM has not developed or maintained plans of action and milestones for each open OIG recommendation, the Under Secretary for Management should direct IRM to take action to comply with standards.

**Recommendation 2:** (U) OIG recommends that the Under Secretary for Management develop and implement a methodology to periodically review the status of the Bureau of Information Resource Management's efforts to implement open OIG recommendations, as described in its plans of action and milestones (Recommendation 1).

## (U) APPENDIX A: OPEN RECOMMENDATIONS RELATED TO RISK MANAGEMENT

(U) Table A.1 lists the unclassified Office of Inspector General (OIG) recommendations related to risk management that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table A.1: Unclassified, Open Recommendations Related to Risk Management**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State Information Security Program (AUD-IT-19-08)	(U) 10/30/2018	(U) 4. OIG recommends that the Chief Information Officer (a) develop and maintain a comprehensive, accurate, and up-to-date organization-wide information system inventory in accordance with National Institute of Standards and Technology Special Publication 800-53 and (b) report quarterly to the Deputy Secretary and other Department of State stakeholders about the progress made until an organization-wide information system inventory is realized and independently verified for completeness.
(U) 2	(U) Audit of the Department of State Information Security Program (AUD-IT-19-08)	(U) 10/30/2018	(U) 5. OIG recommends that the Chief Information Officer identify and assign the necessary resources to develop and maintain a comprehensive, accurate, and up-to-date organization-wide information system inventory in accordance with National Institute of Standards and Technology Special Publication 800-53.
(U) 3	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 1. (b) (7)(E) (b) (7)(E)
(U) 4	(U) Audit of the Department of State Information Security Program (AUD-IT-20-04)	(U) 10/31/2019	(U) 1. OIG recommends that the Chief Information Officer define and implement an information system component inventory, including a complete hardware and software inventory in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53 and NIST Cybersecurity Framework, to identify all components within the boundaries of the Department of State's information systems.

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 5	<i>(U) Audit of the Department of State Information Security Program (AUD-IT-19-08)</i>	(U) 10/30/2018	(U) 2. OIG recommends that the Chief Information Officer (a) revise and update the information security risk management strategy issued in August 2018 to align with all requirements outlined in National Institute of Standards and Technology Special Publication 800-39 to include processes and methodologies for categorizing risk, developing a risk profile, assessing risk, determining tolerance levels, responding to risk, and monitoring risk, and (b) report quarterly to the Deputy Secretary, other Department of State stakeholders, and OIG about the progress made until an adequate and complete information security risk management strategy is fully implemented.
(U) 6	<i>(U) Audit of the Department of State Information Security Program (AUD-IT-19-08)</i>	(U) 10/30/2018	(U) 3. OIG recommends that the Chief Information Officer identify and assign the necessary resources to develop and implement a Department of State-wide information security risk management strategy for all three levels—organization, bureau, and information systems—in accordance with National Institute of Standards and Technology Special Publication 800-39.
(U) 7	<i>(U) Audit of the Department of State Information Security Program (AUD-IT-20-04)</i>	(U) 10/31/2019	(U) 2. OIG recommends that the Chief Information Officer fully define and implement an information security architecture to support the Department of State's enterprise architecture, in accordance with National Institute of Standards and Technology Special Publications 800-39 and 800-37, including a description of the structure and behavior for the enterprise's security processes, information security systems, and personnel and organizational subunits, and that shows the alignment with the enterprise's mission and strategic plans.
(U) 8	<i>(U) Management Assistance Report: Remote Missions Face Challenges Maintaining Communications With Locally Employed Staff and Host Country Government Officials (AUD-MERO-21-16)</i>	(U) 03/01/2021	(U) 4. OIG recommends that the Bureau of Information Resource Management establish and maintain a webpage on OpenNet that will be considered the authoritative source for all up-to-date information regarding the use of specific electronic messaging applications and other communication platforms. Once the webpage is established, Department of State personnel should be notified about where the information can be found.

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 9	(U) <i>Audit of the Department of State Information Security Program</i> (AUD-IT-15-17)	(U) 11/05/2014	(U) 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) 10	(U) <i>Audit of the Department of State FY 2020 Information Security Program</i> (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 4. (b) (7)(E) (b) (7)(E)
(U) 11	(U) <i>Management Assistance Report: Deficiencies Identified in Communications Security Account Management</i> (ISP-21-01)	(U) 10/06/2020	(U) 2. The Bureau of Information Resource Management should implement an automated system to electronically track compliance with corrective actions reported in the Cryptographic Services Branch communications security audits.

(U) **Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX B: OPEN RECOMMENDATION RELATED TO SUPPLY CHAIN RISK MANAGEMENT

---

(U) Table B.1 lists the unclassified Office of Inspector General (OIG) recommendation related to supply chain risk management that was addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

### (U) Table B.1: Unclassified, Open Recommendation Related to Supply Chain Risk Management

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 3. (b) (7)(E) (b) (7)(E)

(U) Source: OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX C: OPEN RECOMMENDATIONS RELATED TO CONFIGURATION MANAGEMENT

---

(U) Table C.1 lists the unclassified Office of Inspector General (OIG) recommendations related to configuration management that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table C.1: Unclassified, Open Recommendations Related to Configuration Management**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 5. (b) (7)(E) (b) (7)(E)
(U) 2	(U) Audit of the Department of State Information Security Program (AUD-IT-15-17)	(U) 11/05/2014	(U) 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 the Cyber Security Architecture for end-to-end configuration management in accordance with the National Institute of Standards and Technology Special Publication 800-53, Revision 4.
(U) 3	(U) Audit of the Department of State Information Security Program (AUD-IT-15-17)	(U) 11/05/2014	(SBU) 10. (b) (7)(E) (b) (7)(E)
(U) 4	(U) Audit of the Department of State Information Security Program (AUD-IT-15-17)	(U) 11/05/2014	(SBU) 12. (b) (7)(E) (b) (7)(E)



(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
			(b) (7)(E)
			(SBU) 13. (b) (7)(E)
			(b) (7)(E)
(U) 5	<i>(U) Audit of the Department of State Information Security Program (AUD-IT-15-17)</i>	(U) 11/05/2014	
(U) 6	<i>(U) Management Assistance Report: The Department of State Is Not Managing Unsupported Operating Systems in Accordance With Federal Requirements (AUD-IT-18-43)</i>	(U) 05/15/2018	(U) 2. OIG recommends that the Bureau of Information Resource Management develop and implement policies and procedures for managing unsupported operating systems that comply with National Institute for Standards and Technology requirements, including identifying the risks associated with using unsupported operating systems, implementing sufficient security measures to mitigate these risks, and developing strategies to replace each unsupported operating system.
(U) 7	<i>(U) Management Assistance Report: The Department of State Is Not Managing Unsupported Operating Systems in Accordance With Federal Requirements (AUD-IT-18-43)</i>	(U) 05/15/2018	(U) 3. OIG recommends that the Bureau of Information Resource Management develop and implement a policy requiring the Information Technology Configuration Control Board to remove all unsupported operating systems from the list of approved software.
(U) 8	<i>(U) Management Assistance Report: The Department of State Is Not Managing Unsupported Operating Systems in Accordance With Federal Requirements (AUD-IT-18-43)</i>	(U) 05/15/2018	(U) 4. Once policies and procedures have been implemented to maintain an inventory of operating systems (Recommendation 1), OIG recommends that the Bureau of Information Resource Management identify and record all operating systems within the Department of State.

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 9	(U) Management Assistance Report: The Department of State Is Not Managing Unsupported Operating Systems in Accordance With Federal Requirements (AUD-IT-18-43)	(U) 05/15/2018	(U) 5. Once all operating systems have been recorded (Recommendation 4), OIG recommends that the Bureau of Information Resource Management identify all unsupported operating systems in use at the Department of State.
(U) 10	(U) Management Assistance Report: The Department of State Is Not Managing Unsupported Operating Systems in Accordance With Federal Requirements (AUD-IT-18-43)	(U) 05/15/2018	(U) 6. Once unsupported operating systems have been identified (Recommendation 5), OIG recommends that the Bureau of Information Resource Management develop and implement a corrective action plan to (a) perform a risk assessment of the unsupported system and (b) develop a mitigation plan for replacing the systems or justifying their continued use.
(U) 11	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 6. (b) (7)(E)
(U) 12	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 7. (b) (7)(E)
(U) 13	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 1. OIG recommends that the Bureau of Information Resource Management develop and implement a detailed program plan for the Information Technology Configuration Control Board process that includes clear goals and attainable objectives and defines areas of authority and responsibility.
(U) 14	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 2. OIG recommends that the Bureau of Information Resource Management develop and implement a process to establish and periodically update a list of system, product, or software owners who will be authorized to make change requests for their system, product, or software. The list should be made available to users and members of the Information Technology Configuration Control Board through the Information Technology Configuration Control Board website or applicable

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
			policies and procedures outlined in Recommendation 12.
(U) 15	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 3. OIG recommends that the Bureau of Information Resource Management determine what documentation is needed to support a change request and modify the policies and procedures outlined in Recommendation 12 or other guidance, such as the submitters guide, provided to change request submitters to reflect the documentation that is required for a complete and accurate change request submission.
(U) 16	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 4. OIG recommends that the Bureau of Information Resource Management develop and implement guidance for change requests to require and include: (a) minimum testing standards for change requests, (b) instructions that testing be performed in advance of the change request being submitted and that the testing documentation be submitted as part of the change request process, and (c) a clearly defined technical review of the testing documentation that is submitted to verify the documentation complies with minimum standards.
(U) 17	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 5. OIG recommends that the Bureau of Information Resource Management remove the default proceed ability for Technical Reviewers in the Virtual Information Technology Configuration Control Board application.
(U) 18	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 6. OIG recommends that the Bureau of Information Resource Management formally notify all Technical Reviewers that default proceeds are no longer allowed and that all Technical Reviewers must review all change requests and either approve, stop, or reject the change request. Policies and procedures outlined in Recommendation 12 or other guidance should be updated to reflect this change to the process.
(U) 19	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 7. OIG recommends that the Bureau of Information Resource Management develop and implement a quality assurance assessment process for all change requests going through the enterprise-wide Information Technology Configuration Control Board. At a minimum, the quality assurance process should include periodic

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
			evaluation of open “stops,” reviews to ensure retention of all relevant documentation, and a final check prior to adding change to the baseline to ensure all pertinent process controls occurred at a minimum.
(U) 20	(U) <i>Audit of the Department of State’s Information Technology Configuration Control Board</i> (AUD-IT-17-64)	(U) 9/27/2017	(U) 10. OIG recommends that the Bureau of Information Resource Management define the roles, responsibilities, and technical skillsets for each technical review and voting area and develop and implement a vetting process to verify Technical Reviewers and Voters have the knowledge, skills, and abilities to perform their assigned duties related to the Information Technology Configuration Control Board process.
(U) 21	(U) <i>Audit of the Department of State’s Information Technology Configuration Control Board</i> (AUD-IT-17-64)	(U) 9/27/2017	(U) 11. OIG recommends that the Bureau of Information Resource Management develop and implement a process to verify that Technical Reviewers and Voters have formally appointed alternatives.
(U) 22	(U) <i>Audit of the Department of State’s Information Technology Configuration Control Board</i> (AUD-IT-17-64)	(U) 9/27/2017	(U) 12. OIG recommends that the Bureau of Information Resource Management develop and implement complete and consistent policies and procedures and supplemental guidance, such as a Submitter’s Guide, for the Information Technology Configuration Control Board process. The policies, procedures, and guidance should, at a minimum, include guidance on roles and responsibilities, detailed procedure steps for submitters, minimum testing requirements, instructions on how Technical Reviewers and Voters should conduct their review, the appropriate use of “stops,” and established timelines for the process.
(U) 23	(U) <i>Audit of the Department of State’s Information Technology Configuration Control Board</i> (AUD-IT-17-64)	(U) 9/27/2017	(U) 13. OIG recommends that the Bureau of Information Resource Management develop and implement a process to periodically review and validate the accuracy and completeness of the data in the Virtual Information Technology Configuration Control Board database and to correct data integrity, omissions and inaccuracies existing between the new and old databases and when identified going forward. As part of this effort, the Bureau of Information Resource Management should ensure that the old database is available

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
			solely as a read-only reference resource and that new data cannot be entered into that database.
(U) 24	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 14. OIG recommends that the Bureau of Information Resource Management develop and implement required, periodic, training for Information Technology Configuration Control Board management and personnel, Bureau Sponsors, Technical Reviewers, Voters, and change request submitters involved in the Information Technology Configuration Control Board process.
(U) 25	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 15. OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to (a) monitor the status of all change requests throughout each stage of the change request process and (b) notify stakeholders when a request is nearing the end of a deadline or when an event occurs that may affect the deadline for a change request.
(U) 26	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 16. OIG recommends that the Bureau of Information Resource Management develop and implement policies and procedures to hold officials accountable for failure to meet established deadlines in the Information Technology Configuration Control Board change request process. Once completed, the policies, procedures, and supplemental guidance discussed in Recommendation 12 should be updated.
(U) 27	(U) Audit of the Department of State's Information Technology Configuration Control Board (AUD-IT-17-64)	(U) 9/27/2017	(U) 17. OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to periodically gather, assess, and report on its change request review process timeliness metrics and to make those results available to its stakeholders and customers in addition to appropriate bureau officials.
(U) 28	(U) Audit of the Department of State's Local Configuration Control Boards (AUD-IT-19-36)	(U) 07/24/2019	(U) 1. OIG recommends that the Bureau of Information Resource Management require that all IT configuration changes approved by the Local Configuration Control Boards at overseas posts be tested before implementation, in accordance with Federal requirements and Department of State policies.
(U) 29	(U) Audit of the Department of State's Local Configuration Control Boards (AUD-IT-19-36)	(U) 07/24/2019	(U) 2. OIG recommends that the Bureau of Information Resource Management require Local Configuration Control Boards to perform and document security impact analyses on all configuration change requests before approval, in

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
			accordance with National Institute of Standards and Technology guidance.
(U) 30	(U) Audit of the Department of State's Local Configuration Control Boards (AUD-IT-19-36)	(U) 07/24/2019	(U) 3. OIG recommends that the Bureau of Information Resource Management provide guidance to Local Configuration Control Boards on the documentation regarding IT configuration change requests that must be retained at a post.
(U) 31	(U) Audit of the Department of State's Local Configuration Control Boards (AUD-IT-19-36)	(U) 07/24/2019	(U) 4. OIG recommends that the Bureau of Information Resource Management develop and issue standard operating procedures for overseas posts' Local Configuration Control Boards to follow when reviewing, approving, and implementing IT configuration change requests. These standard operating procedures should establish and implement a process that provides for the evaluation, approval, and documentation of IT change requests in accordance with Department of State policies and National Institute of Standards and Technology requirements.
(U) 32	(U) Audit of the Department of State's Local Configuration Control Boards (AUD-IT-19-36)	(U) 07/24/2019	(U) 5. OIG recommends that the Bureau of Information Resource Management develop and implement a methodology to oversee Local Configuration Control Board (LCCB) activities, including LCCB approval of IT configuration change requests at the local level. This methodology should include specific procedures for verification of the LCCB's testing of approved changes, security impact analyses, and retention of required documentation.
(U) 33	(U) Audit of the Department of State's Local Configuration Control Boards (AUD-IT-19-36)	(U) 07/24/2019	(U) 6. OIG recommends that the Bureau of Information Resource Management (IRM) formally designate oversight responsibility for Local Configuration Control Board activities to a specific position or office within IRM and establish a formal mechanism for communicating the oversight roles and responsibilities.
(U) 34	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 8. (b) (7)(E) (b) (7)(E)

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 35	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Governance, Resource, and Performance Management</i> (ISP-I-18-15)	(U) 04/24/2018	(U) 12. The Bureau of Information Resource Management should update all Department guidance to reflect the Office of Governance, Resource, and Performance Management's responsibility for the Information Technology Configuration Control Board.

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX D: OPEN RECOMMENDATIONS RELATED TO IDENTITY AND ACCESS MANAGEMENT

(U) Table D.1 lists the unclassified Office of Inspector General (OIG) recommendations related to identity and access management that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table D.1: Unclassified, Open Recommendations Related to Identity and Access Management**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 9. (b) (7)(E) (b) (7)(E)
(U) 2	(U) Audit of the Department of State Implementation and Oversight of Active Directory (AUD-IT-15-05)	(U) 10/31/2014	(SBU) 4. (b) (7)(E) (b) (7)(E)
(U) 3	(U) Compliance Follow-up Audit of Department of State Access Controls for Major Applications (AUD-IT-17-62)	(U) 9/25/2017	(SBU) 13. (b) (7)(E) (b) (7)(E)
(U) 4	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 10. (b) (7)(E) (b) (7)(E)



(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 5	(U) Audit of the Department of State Implementation and Oversight of Active Directory (AUD-IT-15-05)	(U) 10/31/2014	(SBU) 5. (b) (7)(E) (b) (7)(E)
(U) 6	(U) Compliance Follow-up Audit of Department of State Access Controls for Major Applications (AUD-IT-17-62)	(U) 9/25/2017	(SBU) 8. (b) (7)(E) (b) (7)(E)
(U) 7	(U) Compliance Follow-up Audit of Department of State Access Controls for Major Applications (AUD-IT-17-62)	(U) 9/25/2017	(SBU) 9. (b) (7)(E) (b) (7)(E)
(U) 8	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 11. (b) (7)(E) (b) (7)(E)
(U) 9	(U) Management Assistance Report: Deficiencies in Management of Active Directory Privileged Accounts and Security Groups at Overseas Posts (ISP-21-13)	(U) 02/25/2021	(SBU) 1. (b) (7)(E) (b) (7)(E)
(U) 10	(U) Management Assistance Report: Deficiencies in Management of Active Directory Privileged Accounts and Security Groups at Overseas Posts (ISP-21-13)	(U) 02/25/2021	(SBU) 2. (b) (7)(E) (b) (7)(E)

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 11	(U) Management Assistance Report: Deficiencies in Management of Active Directory Privileged Accounts and Security Groups at Overseas Posts (ISP-21-13)	(U) 02/25/2021	(SBU) 3. (b) (7)(E) (b) (7)(E)

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX E: OPEN RECOMMENDATIONS RELATED TO DATA PROTECTION AND PRIVACY

(U) Table E.1 lists the unclassified Office of Inspector General (OIG) recommendations related to data protection and privacy that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table E.1: Unclassified, Open Recommendations Related to Data Protection and Privacy**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 14. (b) (7)(E) (b) (7)(E)
(U) 2	(U) Audit of the Department of State Sanitization of Information Technology Media Before Disposal (AUD-IT-19-02)	(U) 10/29/2018	(U) 2. OIG recommends that the Bureau of Information Resource Management, unless designated otherwise by the Under Secretary for Management, document in the Department of State IT media sanitization policy the program management role and responsibilities and the roles of other key officials responsible for IT media sanitization.
(U) 3	(U) Audit of the Department of State Sanitization of Information Technology Media Before Disposal (AUD-IT-19-02)	(U) 10/29/2018	(U) 3. OIG recommends that the Bureau of Information Resource Management, unless designated otherwise by the Under Secretary for Management, develop and implement controls to enforce and verify domestic and overseas locations, including destruction facilities, are in compliance with the Department of State IT media sanitization policy.
(U) 4	(U) Audit of the Department of State Sanitization of Information Technology Media Before Disposal (AUD-IT-19-02)	(U) 10/29/2018	(U) 4. OIG recommends that the Bureau of Information Resource Management, unless designated otherwise by the Under Secretary for Management, develop and implement a process to periodically, but not less than semiannually, notify Department of State personnel involved in the IT media sanitization process of applicable and relevant policies and procedures.

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 5	<i>(U) Audit of the Department of State Sanitization of Information Technology Media Before Disposal (AUD-IT-19-02)</i>	(U) 10/29/2018	(U) 5. OIG recommends that the Bureau of Information Resource Management, unless designated otherwise by the Under Secretary for Management, revise IT media sanitization policies. The revisions should include the: a. Removal of obsolete information. b. Update of policy information to align with National Institute of Standards and Technology guidance. c. Consolidation of sanitization requirements, for both domestic and overseas locations, into one policy. d. Standardization of sanitization requirements and processes across the Department of State. e. Inclusion of clear instructions that provide steps to be followed.
(U) 6	<i>(U) Audit of the Department of State Sanitization of Information Technology Media Before Disposal (AUD-IT-19-02)</i>	(U) 10/29/2018	(U) 6. OIG recommends that the Bureau of Information Resource Management, unless designated otherwise by the Under Secretary for Management, establish and implement a process to periodically, but not less than annually, review and update, as necessary, the Department of State IT media sanitization policies to reflect current Federal requirements for IT media sanitization.

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX F: OPEN RECOMMENDATIONS RELATED TO SECURITY TRAINING

(U) Table F.1 lists the unclassified Office of Inspector General (OIG) recommendations related to security training that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table F.1: Unclassified, Open Recommendations Related to Security Training**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 16. (b) (7)(E) (b) (7)(E)
(U) 2	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 17. (b) (7)(E) (b) (7)(E)
(U) 3	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 18. (b) (7)(E) (b) (7)(E)
(U) 4	(U) Management Assistance Report: Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts (ISP-21-07)	(U) 12/11/2020	(U) 5. The Bureau of Information Resource Management, in coordination with the Foreign Service Institute, should update the information systems security officer foundations training course to increase both hands-on exercises and discussion on how to perform specific tasks and use Department-provided tools.

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX G: OPEN RECOMMENDATIONS RELATED TO INFORMATION SECURITY CONTINUOUS MONITORING

(U) Table G.1 lists the unclassified Office of Inspector General (OIG) recommendations related to information security continuous monitoring that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table G.1: Unclassified, Open Recommendations Related to Information Security Continuous Monitoring**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 19. (b) (7)(E) (b) (7)(E)
(U) 2	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 20. (b) (7)(E) (b) (7)(E)
(U) 3	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 21. (b) (7)(E) (b) (7)(E)
(U) 4	(U) Management Assistance Report: The Process to Authorize and Track Information Technology Systems Needs Improvement (AUD-IT-17-56)	(U) 08/29/2017	(U) 7. OIG recommends that the Bureau of Information Resource Management develop and implement a corrective action plan that addresses how the Department will comply with Department policy on the Systems Authorization Process. The corrective action plan should identify the root cause of compliance failures, action steps to resolve such compliance failures, improvement benchmarks and a timeframe for completion, and an escalation process to hold system owners accountable.

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX H: OPEN RECOMMENDATIONS RELATED TO CONTINGENCY PLANNING

(U) Table H.1 lists the unclassified Office of Inspector General (OIG) recommendations related to contingency planning that were addressed to the Bureau of Information Resource Management remained open as of July 30, 2021.

**(U) Table H.1: Unclassified, Open Recommendations Related to Contingency Planning**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 22. (b) (7)(E) (b) (7)(E)
(U) 2	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 23. (b) (7)(E) (b) (7)(E)
(U) 3	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 24. (b) (7)(E) (b) (7)(E)
(U) 4	(U) Audit of the Department of State FY 2020 Information Security Program (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 25. (b) (7)(E) (b) (7)(E)

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX I: OPEN RECOMMENDATIONS RELATED TO GENERAL IT POLICIES

---

(U) Table I.1 lists the unclassified Office of Inspector General (OIG) recommendations related to general IT policies that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table I.1: Unclassified, Open Recommendations Related to General IT Policies**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Governance, Resource, and Performance Management</i> (ISP-I-18-15)	(U) 04/24/2018	(U) 10. The Bureau of Information Resource Management should implement procedures to ensure regularly scheduled reviews and updates to the Department's information technology management policies and procedures in Volume 5 of the Foreign Affairs Manual and its associated Foreign Affairs Handbooks.
(U) 2	(U) <i>Audit of the Department of State FY 2020 Information Security Program</i> (AUD-IT-21-25)	(U) 04/13/2021	(SBU) 2. (b) (7)(E) (b) (7)(E)

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.



## (U) APPENDIX J: OPEN RECOMMENDATIONS RELATED TO INFORMATION SYSTEM SECURITY OFFICERS

---

(U) Table J.1 lists the unclassified Office of Inspector General (OIG) recommendations related to Information System Security Officers that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table J.1: Unclassified, Open Recommendations Related to Information System Security Officers**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Management Assistance Report: Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts (ISP-21-07)	(U) 12/11/2020	(U) 2. The Bureau of Information Resource Management, in coordination with the Bureau of the Comptroller and Global Financial Services, should incorporate an attestation relating to the completion of information systems security officer responsibilities in the annual Chief of Mission Management Control Statement of Assurance.
(U) 2	(U) Management Assistance Report: Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts (ISP-21-07)	(U) 12/11/2020	(U) 3. The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security and regional bureaus, should define the roles and responsibilities for regional information systems security officers and liaisons and clarify the level of interaction and support these positions are to give to overseas information systems security officers, and update applicable Department standards as needed.
(U) 3	(U) Management Assistance Report: Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts (ISP-21-07)	(U) 12/11/2020	(U) 4. The Bureau of Information Resource Management should review and update the information systems security officer checklist and clearly state for each task whether it should be performed by overseas information systems security officers, by other overseas post information management personnel, or by the Bureau of Information Resource Management.

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX K: OPEN RECOMMENDATIONS RELATED TO IT INVESTMENTS

---

(U) Table K.1 lists the unclassified Office of Inspector General (OIG) recommendations related to IT investments that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table K.1: Unclassified, Open Recommendations Related to IT Investments**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)	(U) 03/23/2016	(U) 8. OIG recommends that the Bureau of Information Resource Management establish and implement a plan to review IT investment reorganizations that occurred since FY 2010 to ensure that the investments resulting from the reorganizations comply with Office of Management and Budget requirements for information technology investments.
(U) 2	(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)	(U) 03/23/2016	(U) 10. OIG recommends that the Bureau of Information Resource Management develop and implement a process to (a) identify and review all bureau-specific IT investment methodologies (ones currently in place as well as ones that will be developed in the future); (b) determine whether the bureau-specific IT investment methodologies comply with Office of Management and Budget Circular A-130; and, if they do not comply, (c) provide bureaus with guidance regarding the modifications needed to fully comply and verify that the methodologies were modified as necessary. This effort should include reviewing the standard forms used by each bureau during the IT selection process to ensure consistency and compliance with Office of Management and Budget Circular A-130.
(U) 3	(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)	(U) 03/23/2016	(U) 11. OIG recommends that the Bureau of Information Resource Management develop and implement policies and procedures to oversee and enforce requirements for bureaus and offices to avoid duplicative IT investments.

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 4	<i>(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)</i>	(U) 03/23/2016	(U) 12. OIG recommends that the Bureau of Information Resource Management develop and implement a process to perform periodic, but no less than annual, reviews of the entire agency IT portfolio to enforce bureau accountability and identify potential duplicative systems.
(U) 5	<i>(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)</i>	(U) 03/23/2016	(U) 13. For duplicative systems that are identified by the new process implemented to perform periodic reviews of the entire agency IT portfolio (Recommendation 12), OIG recommends that the Bureau of Information Resource Management develop and implement a strategy to combine, eliminate, or replace duplicative systems, as practicable.
(U) 6	<i>(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)</i>	(U) 03/23/2016	(U) 14. OIG recommends that the Bureau of Information Resource Management develop and implement a strategy to perform semiannual or more frequent reviews of bureau-funded IT contracts to identify new IT investments developed as part of the contracts.
(U) 7	<i>(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)</i>	(U) 03/23/2016	(U) 17. OIG recommends that the Bureau of Information Resource Management (a) develop and implement a policy requiring bureaus and offices to provide details of IT investments, programs, and projects in iMatrix and (b) develop and disseminate guidance specifying the level of detail necessary for each investment, including general descriptions and technical capabilities.
(U) 8	<i>(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)</i>	(U) 03/23/2016	(U) 20. OIG recommends that the Bureau of Information Resource Management develop and issue a policy stating that bureaus must update the information on non-major investments in iMatrix quarterly, rather than only when the reports are due to be submitted to the Office of Management and Budget.

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 9	(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)	(U) 03/23/2016	(U) 22. OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureau of Budget and Planning, develop and implement a process to verify that all bureau and office IT investment managers and budget analysts complete the respective training courses related to IT capital planning and reporting that are provided annually.
(U) 10	(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)	(U) 03/23/2016	(U) 25. OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureau of Budget and Planning, develop and implement a process to validate the completeness of the data in iMatrix. At a minimum, this process should include an analysis of IT expenditures in the financial management system to ensure expenditures are reported in iMatrix, as needed.
(U) 11	(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)	(U) 03/23/2016	(U) 26. OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureau of Budget and Planning, develop and implement a process to validate the accuracy of data in iMatrix. This could include developing and implementing analytical procedures to identify anomalies in iMatrix data.
(U) 12	(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)	(U) 03/23/2016	(U) 27. OIG recommends that the Bureau of Information Resource Management develop and implement a policy requiring bureaus and offices to submit source documents to support the information entered into iMatrix.
(U) 13	(U) Audit of the Department of State Process To Select and Approve Information Technology Investments (AUD-FM-16-31)	(U) 03/23/2016	(U) 28. OIG recommends that the Bureau of Information Resource Management develop and implement a process to verify that bureaus and offices are submitting source documents to support the information entered into iMatrix in accordance with the policy developed that requires bureaus and offices to submit source documents that support the information entered into iMatrix.

(U) Source: OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX L: OPEN RECOMMENDATIONS RELATED TO SHARED SERVICES

(U) Table L.1 lists the unclassified Office of Inspector General (OIG) recommendations related to shared services that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table L.1: Unclassified, Open Recommendations Related to Shared Services**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) <i>Inspection of the Bureau of European and Eurasian Affairs</i> (ISP-I-20-15)	(U) 09/28/2020	(U) 5. The Bureau of Information Resource Management, in coordination with the Bureau of European and Eurasian Affairs, should update the master service level agreement governing roles and responsibilities related to information technology services.
(U) 2	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support</i> (ISP-I-21-19)	(U) 07/01/2021	(U) 1. The Bureau of Information Resource Management should review and update the Enterprise IT Help Desk and Desktop Support Master Service Level Agreement to align with the current Bureau of Information Resource Management service catalog.
(U) 3	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support</i> (ISP-I-21-19)	(U) 07/01/2021	(U) 2. The Bureau of Information Resource Management should define out-of-scope services in the Enterprise IT Help Desk and Desktop Support Master Service Level Agreement.
(U) 4	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support</i> (ISP-I-21-19)	(U) 07/01/2021	(U) 3. The Bureau of Information Resource Management should update the Enterprise IT Help Desk and Desktop Support Master Service Level Agreement to include the methodology for calculating the incident resolution time.
(U) 5	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support</i> (ISP-I-21-19)	(U) 07/01/2021	(U) 4. The Bureau of Information Resource Management should update the Enterprise IT Help Desk and Desktop Support Master Service Level Agreement to reflect the current technology modernization policy.

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 6	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support (ISP-I-21-19)</i>	(U) 07/01/2021	(U) 5. The Bureau of Information Resource Management should review its technology modernization purchasing policies and determine if the Enterprise IT Help Desk and Desktop Support Master Service Level Agreement requires updates to these policies based on its review.
(U) 7	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support (ISP-I-21-19)</i>	(U) 07/01/2021	(U) 6. The Bureau of Information Resource Management should establish a process to update operational level agreements when a new service is added to the bureau's service catalog or an existing service is modified in a way that affects documented service targets.
(U) 8	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support (ISP-I-21-19)</i>	(U) 07/01/2021	(U) 8. The Bureau of Information Resource Management should conduct semiannual customer feedback surveys in accordance with the Enterprise IT Help Desk and Desktop Support Master Service Level Agreement.
(U) 9	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support (ISP-I-21-19)</i>	(U) 07/01/2021	(U) 9. The Bureau of Information Resource Management should establish a communication forum for regular communication and interaction with its customers.
(U) 10	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support (ISP-I-21-19)</i>	(U) 07/01/2021	(U) 10. The Bureau of Information Resource Management, in coordination with the Bureau of Administration should, upon completion of the comprehensive cost model study, adjust the Office of Consolidated Customer Support's desktop service fee, if necessary, and publish a pricing schedule for all customers.

(U) Source: OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.

## (U) APPENDIX M: OPEN RECOMMENDATIONS RELATED TO OTHER IT-RELATED ISSUES

---

(U) Table M.1 lists the unclassified Office of Inspector General (OIG) recommendations related to other IT-related issues that were addressed to the Bureau of Information Resource Management and remained open as of July 30, 2021.

**(U) Table M.1: Unclassified, Open Recommendations Related to Other IT-Related Issues**

(U) #	(U) REPORT TITLE (NUMBER)	(U) ISSUE DATE	(U) RECOMMENDATION
(U) 1	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Governance, Resource, and Performance Management</i> (ISP-I-18-15)	(U) 04/24/2018	(U) 11. The Bureau of Information Resource Management should revise and promulgate the bureau process for timely handling of responses to U.S. Government Accountability Office recommendations.
(U) 2	(U) <i>Management Assistance Report: Deficiencies Identified in Communications Security Account Management</i> (ISP-21-01)	(U) 10/06/2020	(U) 1. The Bureau of Information Resource Management, in coordination with the regional bureaus, should establish escalation procedures to be used by the Cryptographic Services Branch to ensure timely corrective actions from overseas communications security custodians.
(U) 3	(U) <i>Inspection of the Bureau of Information Resource Management's Office of Consolidated Customer Support</i> (ISP-I-21-19)	(U) 07/01/2021	(U) 7. The Bureau of Information Resource Management should establish and implement procedures that comply with the Department's separation of duties requirement for the receipt, storage, or disposition of expendable and nonexpendable property in the Office of Consolidated Customer Support.

**(U) Source:** OIG generated based on an analysis of audit compliance records involving unclassified recommendations addressed to the Bureau of Information Resource Management that remained open as of July 30, 2021.



## (U) APPENDIX N: ACTING UNDER SECRETARY FOR MANAGEMENT'S RESPONSE

---



United States Department of State  
*Under Secretary of State  
for Management*  
Washington, D.C. 20520

UNCLASSIFIED

October 5, 2021

### MEMORANDUM

TO:                   OIG Deputy Assistance Inspector General for Audits –  
                          Gayle Voshell

FROM:               Acting Under Secretary for Management (M) – Carol  
                          Z. Perez

SUBJECT:           Response to OIG draft Management Assistance Report:  
                          Support from the Under Secretary for Management is  
                          Needed To Facilitate the Closure of Office of Inspector  
                          General Recommendations Addressed to the Bureau of  
                          Information Resource Management

Thank you for the opportunity to respond to OIG's draft report regarding the facilitation of closure of OIG Recommendations addressed to the Bureau of Information Resource Management.

**Recommendation 1:** OIG recommends that the Under Secretary for Management verify that the Bureau of Information Resource Management (IRM) has developed plans of action and milestones, as required by the National Institute of Standards and Technology, Special Publication 800-53, rev. 4, to address each open OIG recommendation. The plans of action and milestones should document planned remedial actions to correct the deficiencies identified. If the Under Secretary for Management determines that IRM has not developed or maintained plans of action and milestones for each open OIG recommendation, the Under Secretary for Management should direct IRM to take action to comply with standards.

UNCLASSIFIED



UNCLASSIFIED

-2-

**Management Response (10/5/2021):** M appreciates and understands OIG's concern regarding IRM's open OIG recommendations. However, at this time M declines OIG's recommendation 1. M and M/SS have been consistently reviewing all OIG compliance updates from IRM since March 2021 to ensure OIG's recommendations are being appropriately addressed. All responses to OIG must be reviewed and cleared by representatives from M/SS and M prior to IRM sending OIG an update.

If the end goal is for IRM to close their open recommendations with OIG, a realistic concern is that developing a separate action plan for each recommendation would prove overly cumbersome. IRM's staff, time, and resources are better spent working on compliance related activities, maintaining a high standard of day-to-day operations, and communicating directly with OIG. Furthermore, since M started reviewing IRM's OIG recommendations in March, OIG has closed 21 of IRM's recommendations, which shows significant progress at the current level of oversight from M.

**Recommendation 2:** OIG recommends that the Under Secretary for Management develop and implement a methodology to periodically review the status of the Bureau of Information Resource Management's efforts to implement open OIG recommendations, as described in its plans of action and milestones (Recommendation 1).

**Management Response (10/5/2021):** M accepts OIG's recommendation 2 but notes the activities recommended are already being conducted regularly.

Each month M staff send IRM a detailed spreadsheet with all open recommendations from OIG as well as a visual placemat with a high-level look at IRM's compliance (Tab 1). IRM verifies the information is accurate and responds back to M staff with any additional relevant information, such as expected dates for closure or if they are experiencing any particular difficulties. After that, M reviews IRM's

UNCLASSIFIED

UNCLASSIFIED

-3-

placemat and data to ensure she is up-to-date on their compliance efforts. These actions occur monthly and have been since March 2021. For this reason, M asks OIG to close this recommendation based on satisfactory compliance.

UNCLASSIFIED



## **HELP FIGHT** FRAUD, WASTE, AND ABUSE

1-800-409-9926

[Stateoig.gov/HOTLINE](https://stateoig.gov/HOTLINE)

If you fear reprisal, contact the  
OIG Whistleblower Coordinator to learn more about your rights.

[WPEAOmbuds@stateoig.gov](mailto:WPEAOmbuds@stateoig.gov)