Office of Inspector General
United States Department of State

ISP-21-07 Office of Inspections December 2020

# Management Assistance Report: Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts

MANAGEMENT ASSISTANCE REPORT

## Summary of Review

Information systems security officers (ISSO) are responsible for enforcing Department of State (Department) information systems security policies to ensure the protection of the Department's computer infrastructure, networks, and data. However, OIG has found continued deficiencies in the performance of ISSO duties, which places the Department's computer systems and data at risk. Deficiencies in the performance of ISSO duties relate to the ongoing challenge of information security, which OIG identified to be a major management challenge for the Department in the *Inspector General Statement on the Department of State's Major Management and Performance Challenges*.[1]

OIG reviewed 51 overseas inspection reports issued from October 1, 2016, to September 30, 2019, and identified findings on deficiencies in ISSO performance in 25 (49 percent) of reviewed reports. This reflects an increase from the 2017 Management Assistance Report (MAR),[2] where OIG found 33 percent of reviewed reports contained deficiencies in ISSO performance. This MAR identifies additional underlying factors not addressed in the 2017 MAR that contributed to or caused the non-performance of ISSO duties. OIG made five recommendations to address the reported causes for continued overseas ISSO deficiencies. In its comments on the draft report, the Department concurred with four recommendations and disagreed with one recommendation. OIG considers four recommendations resolved and one recommendation unresolved. The Department's response to each recommendation and OIG's reply can be found in the Recommendations section of this report. The Department's formal written responses are reprinted in their entirety in Appendix B.

# BACKGROUND

The ISSO is the Department's designated official to enforce information systems security policies to protect computer infrastructure, networks, and data. ISSOs at overseas posts work closely with information management (IM) staff to perform responsibilities outlined in 5 Foreign Affairs Handbook (FAH)-2 H-120 and 12 Foreign Affairs Manual (FAM) 600. Within the Department, the Bureaus of Information Resource Management (IRM) and Diplomatic Security (DS) coordinate the activities of overseas ISSOs, including policy development, determining required tasks, and responding to cybersecurity incidents when warranted.

Although the ISSO is the Department's designated official to enforce information systems security policies, the Department does not have an ISSO skill code.[3] Typically, ISSO

[1] OIG, *Inspector General Statement on the Department of State's Major Management and Performance Challenges Fiscal Year 2019* 13 (OIG-EX-20-02, January 2020).

[2] OIG, *Management Assistance Report: Non-Performance of Information Systems Security Officer Duties by Overseas Personnel* (ISP-17-24, May 2017). The scope of the 2017 report included inspections conducted from fall FY 2014 to spring FY 2016.

[3] According to 3 FAH-1 H-2623.2, the Department has four main information technology functional skill codes: Information Management, 2880; Information Programs Administration, 2881; Information Management Technical, 2882; and Information Technology Management, 2884.

responsibilities are assigned to an Information Management specialist as a collateral duty. The Department's few full-time overseas ISSOs are located at larger posts. Additionally, IRM designates certain positions in the Department and overseas as regional ISSOs or ISSO liaisons to assist overseas ISSOs and support the program. Regional ISSOs can be located at either domestic or overseas Regional Information Management Centers, within a regional bureau executive office, or at specific overseas posts. Furthermore, regional ISSOs—which can be designated as full-time or part-time positions—may be assigned to either a designated geographic region or to a specific country. ISSO liaisons are located within IRM's ISSO Program Office in Washington, D.C.

In 2017, OIG issued a MAR on the non-performance of ISSO duties by overseas personnel.[4] In the 2017 MAR, OIG found that over a 3-year period, 33 percent of overseas inspection reports included deficiencies related to non-performance of ISSO duties. In response to that MAR, IRM issued cable 17 STATE 104970[5] requiring overseas posts to allow sufficient time and devote sufficient resources for ISSOs to ensure cybersecurity needs are met and documented. Despite this cable, OIG continued to identify deficiencies in the performance of ISSO responsibilities overseas.

# FINDINGS

OIG reviewed 51 overseas inspection reports issued from October 1, 2016, to September 30, 2019, and identified findings on deficiencies in ISSO performance in 25 (49 percent) of reviewed reports. This reflects an increase from the 2017 MAR, where OIG found 33 percent of reviewed reports contained deficiencies in ISSO performance. OIG found the following common deficiencies across the reports reviewed for this MAR:

- ISSOs did not perform random reviews of user accounts or assist with the remediation of identified vulnerabilities as required by Department standards (12 FAH-10 H-112.9-2 and 12 FAH-10 H-332.3-3).
- ISSOs did not review and analyze information systems audit logs for inappropriate or unusual activity (12 FAH-10 H-122.5-2).
- ISSOs did not ensure systems for which they are responsible are configured, operated, and maintained in accordance with standards (5 FAM 824(1)).

The reports cited several causes for the non-performance of ISSO duties, including lack of management oversight, competing priorities, and insufficient time to perform required responsibilities. With cybersecurity listed as one of the Department's objectives in its Information Technology Strategic Plan for Fiscal Years 2019 - 2022,[6] the Department has a responsibility to ensure that ISSOs are performing their duties. Based on the review of the OIG

[4] ISP-17-24, May 2017.

[5] Cable 17 STATE 104970, "Documenting Information Systems Security Officer (ISSO) Duties," October 2017.

[6] Department of State, Bureau of Information Resource Management, *U.S. Department of State Information Technology Strategic Plan for Fiscal Years 2019 - 2020* 9-10 (March 2019).

inspection reports described above, interviews with Department officials, and a review of survey responses from overseas ISSOs, OIG identified additional areas requiring Department attention to address the causes for continued deficiencies in the performance of overseas ISSO responsibilities, as detailed below.

## Information Systems Security Officer Reporting Structure and Accountability

### *Complex Reporting Structure Led to Inadequate Management Oversight, Competing Priorities, and Insufficient Time to Perform Duties*

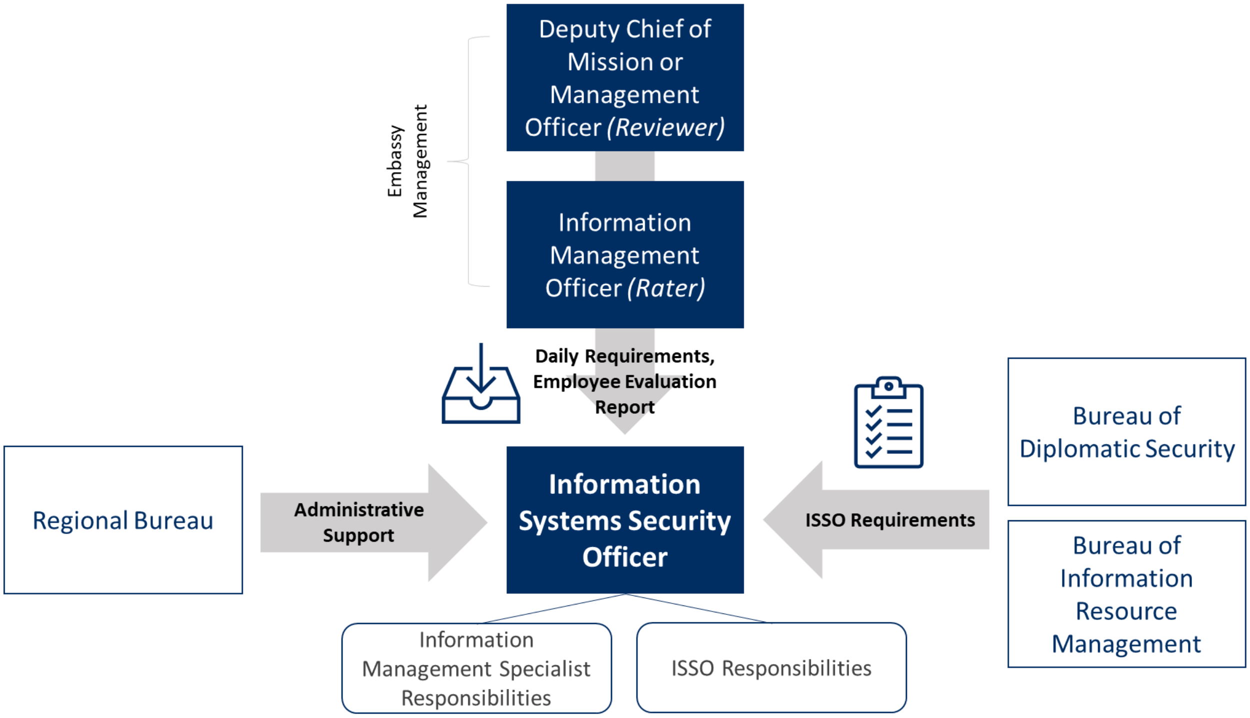
OIG determined that the complex reporting structure for overseas ISSOs prevented adequate management oversight over their performance. Furthermore, and as noted above, because ISSO responsibilities typically are assigned on a collateral basis,[7] this structure also led to competing priorities and a lack of sufficient time for ISSOs to perform required responsibilities. Under this reporting structure, overseas ISSOs receive daily supervision from embassy IM management, administrative support from regional bureaus, and ISSO requirements from IRM and DS (see Figure 1). Specifically, IM leadership at overseas posts provide daily guidance and supervision and rate ISSOs on their work performance, including other IM responsibilities. Regional bureau executive offices provide administrative support for those performing ISSOs duties.[8] Lastly, IRM and DS establish ISSO responsibilities, primarily through the bureaus' information security and management responsibilities for the Department and their policy development roles.[9] Despite their role in defining ISSO responsibilities, neither IRM nor DS are in the ISSO reporting chain of command or have the authority to ensure ISSOs perform their duties. OIG recognizes that designated overseas ISSOs are under chief of mission authority and embassy IM managers are responsible for day-to-day oversight; however, OIG believes that IRM and DS should be involved in providing feedback on the performance of ISSOs considering the bureaus' role in defining ISSO requirements.

[7] At overseas posts with no U.S. direct-hire information management personnel, ISSO responsibilities may be assigned to regional security officers or cleared locally employed staff in the information management section.

[8] ISSOs and IM specialists are regional bureau assets.

[9] According to 5 FAH-2 H-121, IRM is tasked to "implement information security policy, create and implement corporate security and system security plans, perform operational monitoring, and jointly develop guidelines for system security plans." Guidance in 5 FAH-2 H-122 states that DS is "responsible for developing information security policies to include the information systems security policies, developing computer security policies, providing security training, evaluating compliance, jointly developing guidelines for systems security plans, and coordinating with other agencies regarding personnel abroad."

**Figure 1: Illustration of Typical Information Systems Security Officer Reporting Structure**


Embassy Management
Deputy Chief of Mission or Management Officer *(Reviewer)*
Information Management Officer *(Rater)*
Daily Requirements, Employee Evaluation Report
Regional Bureau
Administrative Support
Information Systems Security Officer
ISSO Requirements
Bureau of Diplomatic Security
Bureau of Information Resource Management
Information Management Specialist Responsibilities
ISSO Responsibilities

**Source**: OIG generated based on information provided by the Department.

The complex reporting structure also affected the priorities of overseas ISSOs and the time they had to perform required responsibilities. More than 70 percent of overseas ISSOs who responded to OIG's survey[10] stated they are not required to report their work to embassy management and IRM, and, accordingly, they allocated their time to and prioritized the completion of other IM-related tasks over ISSO duties. As a result of prioritizing these tasks, overseas ISSOs also reported a lack of sufficient time to perform ISSO duties. More than 76 percent of overseas ISSOs who responded to OIG's survey stated that they did not have enough time to perform ISSO duties. OIG determined that both issues—the competing priorities and the lack of sufficient time—are the result of overseas ISSOs receiving direction and performance ratings from embassy management, rather than from IRM or DS.

IRM told OIG that issues with management oversight, competing priorities, and a lack of sufficient time for ISSOs to perform required responsibilities can be addressed by creating full-time dedicated ISSO positions under IRM's general oversight and direction. More than 82 percent of overseas ISSOs who responded to the survey supported the need for full-time dedicated positions, citing the breadth of ISSO responsibilities as well as the amount of time required to complete their tasks. Furthermore, in accordance with 5 FAM 824(5), the ISSO should be accountable to IRM's Chief Information Security Officer. Additionally, the Federal Information Security Modernization Act[11] charges the Chief Information Officer with

[10] For this MAR, OIG sent a survey to all primary and alternate overseas ISSOs.

[11] Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3554(3)(B) (2014).

implementing an effective information security program. However, the current reporting structure for overseas ISSOs does not comply with these cited mandates.

The creation of dedicated ISSO positions within the Department would involve several different Department bureaus and funding allocations, as well as the recruitment of staff to fill those positions. Additionally, it would require the involvement of senior-level Department officials to facilitate a change in current cybersecurity practices. Considering the level of complexity involved, OIG determined that an organizational assessment of the ISSO program would assist the Department in deciding how to structure the program in order to perform its mission in an efficient, effective, and accountable manner. The Bureau of Global Talent Management's Office of Organization and Talent Analytics performs organizational assessments for the Department. An organizational assessment would help determine workload distribution in support of dedicated full-time ISSOs and provide information on the appropriate ISSO reporting structure. Furthermore, using the results of an organizational assessment, the Department could address issues with the reporting structure to ensure adequate oversight and management of the ISSO program.

> **Recommendation 1:** The Bureau of Global Talent Management, in coordination with the Under Secretary for Management, the Bureaus of Diplomatic Security and Information Resource Management, and the regional bureaus, should conduct an organizational assessment of the information systems security officer program to determine the feasibility of creating full-time overseas positions and implement the results of the assessment with an appropriate reporting structure for those positions. (Action: GTM, in coordination with M, DS, IRM, AF, EAP, EUR, NEA, SCA, and WHA)

### *Increased Oversight From Chiefs of Mission Needed*

In addition to simplifying the complex reporting structure for ISSO positions, OIG identified the need for increased attention by embassy management over ISSO performance. Lack of management oversight was cited in the reviewed inspection reports as one reason for the non-performance of overseas ISSO responsibilities. To increase the attention of embassy managers, OIG determined that including the evaluation of ISSO performance as part of the annual Chief of Mission Management Control Statement of Assurance process would help achieve this objective.

In accordance with 2 FAM 022.1, the Secretary of State provides an annual Statement of Assurance to the President and Congress on the adequacy of management controls. According to 2 FAM 022.7(5), in support of the Secretary's statement, each chief of mission (COM) completes a Statement of Assurance for their respective overseas post that is submitted to regional bureaus for consolidated reporting to the Secretary. Every year, COMs are required to attest to the effectiveness of their mission's system of management and internal control. Any program areas identified as being at risk of not meeting objectives are to be included in the Statement of Assurance as a significant deficiency.[12]

As stated in cable 20 STATE 16460,[13] one of the critical responsibilities for a COM is to work with the mission's leadership team to provide an environment of strong management controls over post operations. The Bureau of the Comptroller and Global Financial Services (CGFS) provides detailed guidance annually to COMs and mission staff to help them fulfill this critical responsibility.

For the FY 2020 Statement of Assurance process, CGFS cited information systems security as an area of increased focus. However, OIG found that CGFS' current Management Controls Checklist and reporting template for the Statement of Assurance lacked specific questions on the performance of information systems security responsibilities. For example, the information technology (IT) and management portion of the checklist contains questions on training requirements, access controls, security encryption, and communications tests, among others. However, the checklist does not ask embassy management to assess the performance of required ISSO responsibilities. Furthermore, the COM's attestations in the Statement of Assurance[14] do not include ISSO responsibilities. Only the Statement of Assurance annex, where the COM attests to effective internal controls over IT contingency planning, mentions information security.

Although IRM acknowledged to OIG the need for all ISSOs to perform their responsibilities, OIG found the bureau did not use the Statement of Assurance process as a way to achieve this outcome. OIG believes adding an attestation relating to the completion of ISSO responsibilities in the annual Statement of Assurance would increase the attention of embassy managers on the important duties that ISSOs should perform and would assist ISSOs in receiving the necessary time and priority from post management to perform required tasks. Without embassy management oversight of ISSO duties, the lack of performance of required information management and security responsibilities by overseas ISSOs will continue to negatively affect the Department's cybersecurity.

[12] According to 2 FAM 021.3, a significant deficiency is a "deficiency, or combination of deficiencies, that in management's judgment should be communicated [in the Statement of Assurance] because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives."

[13] Cable 20 STATE 16460, "Your Role in Assuring Strong Management Controls and Oversight Over Post Operations," February 2020.

[14] The cornerstone of the Statement of Assurance process is the COM's memorandum to the head of the regional bureau attesting to management controls in "program areas that are of greater risk and/or due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation." The Management Controls Checklist, described by CGFS as "an optional tool…to supplement [post's] management control reviews," covers a range of functional areas, including IT and management. Annex 1 of the Statement of Assurance lists attestations related to specific functional areas. *See* Department of State June 28, 2019, memorandum "Guidance for the Fiscal Year (FY) 2019 Reporting Requirements for the Federal Managers' Financial Integrity Act (FMFIA)" 2; U.S. Department of State, Bureau of the Comptroller and Global Financial Services, Management Controls Checklist Fiscal Year 2019 3 (April 2019); and Annex 1 to the FY 2019 Statement of Assurance Template.

**Recommendation 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. (Action: IRM, in coordination with CGFS)

## Available Resources to Assist Information Systems Security Officers

### *Unclear Roles and Responsibilities Among Regional Information Systems Security Officers and Liaison Staff Affected Performance and Communication*

As described above, certain positions domestically and overseas are designated as regional ISSOs or ISSO liaison staff. OIG identified a lack of clarity regarding how regional ISSOs and ISSO liaison staff support the ISSO program and work with overseas ISSOs in fulfilling their responsibilities. OIG found Department standards contain minimal guidance on the purpose of regional ISSOs and ISSO liaisons and how these positions work with overseas ISSOs to meet program goals. For example, OIG found the Department had no standards that describe when a regional ISSO is assigned or what level of support they should provide to a certain geographic region. In addition, for ISSO liaison staff, OIG found only one mention of these positions in 5 FAM 1064.1-1. That guidance states that ISSO liaisons provide liaison and technical assistance to ISSOs but lacks specific information on what kind of support they should provide and the level of interaction they should have with overseas ISSOs. Without Department standards that clearly define roles and responsibilities for regional ISSOs and ISSO liaison staff, overseas ISSOs may be unable to take full advantage of the assistance available from these positions.

Regional ISSOs told OIG they provide assistance—primarily information and guidance on new policies or help with troubleshooting a specific problem—as needed to overseas ISSOs. ISSO liaisons told OIG they support ISSOs by deploying automated tools to help them complete their duties and maintaining the mailing list used to keep ISSOs aware of new Department policies affecting ISSOs. However, both regional ISSOs and ISSO liaisons told OIG they were uncertain about the level of interaction they should provide and whether they met ISSOs' expectations. OIG also found that not all regional ISSOs provided support to overseas ISSOs, even though their position title would indicate their focus would primarily be on the ISSO program. For example, one regional ISSO told OIG he does not visit posts to provide support while another said he is a regional ISSO in title only because he does not provide any ISSO-related support.

According to the Government Accountability Office's *Standards for Internal Control in the Federal Government*,[15] management should establish clear roles and responsibilities for positions and define how those positions interact and communicate with one another. Unclear roles and responsibilities hinder the ability of overseas ISSOs to perform their duties, resulting in potential cybersecurity vulnerabilities for the Department.

[15] Government Accountability Office, *Standards for Internal Control in the Federal Government* 28 (GAO-14-704G, September 2014).

**Recommendation 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. (Action: IRM, in coordination with DS, AF, EAP, EUR, NEA, SCA, and WHA)

### *The Information Systems Security Officer Checklist Was Ineffective for Overseas Use*

OIG found that IRM's ISSO Program Office had not reviewed and substantially updated the ISSO checklist since 2014,[16] resulting in a tool that was ineffective for overseas use. The official ISSO checklist, developed by IRM's ISSO Program Office, is to be used by both domestic and overseas ISSOs in performing their responsibilities and provides the minimum requirements and procedures for the Department's ISSO Program.[17] However, OIG determined that the version of the checklist in use at the time of this review[18] included 13 tasks that non-ISSO staff overseas could perform, according to Department standards.[19] Reassigning these duties would reduce the amount of time overseas ISSOs need to perform their responsibilities. These 13 tasks include, among others, reviewing and coordinating resolution of security alerts, reviewing the naming convention in Active Directory[20] to ensure compliance with systems administrator standards, and checking printers or other peripherals for proper configuration. OIG also identified 12 additional checklist tasks that IRM could perform centrally with available technology and automation. Among these are the network shared data review to verify that classified files are not stored on unclassified systems as well as the review of users' activities, files, and folders for security violations.

More than 72 percent of overseas ISSOs who responded to OIG's survey cited an up-to-date and accurate checklist as being relevant to the performance of their ISSO work. However, OIG found that although the ISSO Program Office had made minor changes to the checklist since it was first created in 2014, it had yet to update the checklist to identify which tasks could be performed by other IM personnel at post or centrally by IRM. By reassigning appropriate tasks on the ISSO checklist, IRM could streamline the number of tasks overseas ISSOs must perform and reduce the amount of time required to do so. Without a comprehensive update of the ISSO checklist, overseas ISSOs will continue to spend time and resources performing tasks that can be done by others, risking their ability to complete essential information security tasks.

[16] The ISSO checklist includes a description of 41 tasks, an explanation of minimum tasks to be performed, and how often they need to be performed.

[17] 5 FAH-11 H-116.

[18] Official ISSO Checklist, version 4.6, dated February 2020.

[19] Department standards include 12 FAH-10 H-112.9-2, 5 FAM 724, 12 FAM 645.5, 12 FAM 632.1-8c, 12 FAM 642.4-5, and 12 FAH-10 H-212.1-2.

[20] Active Directory is a Microsoft technology for centrally managing users, computers, and other devices on a network.

**Recommendation 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. (Action: IRM)

### *Overseas Information Systems Security Officers Stated the Foundations Training Course Did Not Adequately Prepare Them to Perform Required Responsibilities*

Overseas ISSOs told OIG that the Department's ISSO foundations training course did not adequately prepare them to perform their required duties. Specifically, 54 percent of ISSOs who responded to OIG's survey and also attended the ISSO foundations training course within the 3 years prior to this review reported the training did not sufficiently prepare them to do their duties. OIG's survey results also showed that 52 percent of the ISSOs who attended the training course found the time spent on hands-on exercises to be insufficient, 59 percent found time spent discussing how to perform required tasks to be insufficient, and 52 percent found time spent discussing how to use provided tools, such as the ISSO checklist and software tools, to be insufficient. In addition, OIG's review of the ISSO foundations training course materials found the curriculum focused on tools[21] that IRM does not provide to overseas ISSOs. OIG also found that the curriculum included high-level discussions about tasks but did not adequately cover how to actually perform the ISSO checklist duties.

Responsibility for ISSO training transitioned from DS to IRM in October 2019. At the same time, the Department's Foreign Service Institute School of Applied Information Technology assumed responsibility for teaching the course. Since the transition, IRM has worked with the School of Applied Information Technology to better align its role-based cyber training with the actual duties ISSOs and other security professionals perform. Although there was some progress, no official changes had been made to the course content and objectives at the time of this review.

The *Standards for Internal Control in the Federal Government*[22] state that management should establish expectations of competence, which includes ensuring that personnel possess and maintain a level of competence that allows them to accomplish their assigned responsibilities. As noted above, OIG's survey results showed that ISSOs found the training to be insufficient and reported that not enough time was spent on hands-on exercises and on how to perform required tasks and use Department-provided tools. Increasing the time spent on these activities would assist overseas ISSOs in performing their responsibilities. The failure to adequately prepare overseas ISSOs hinders their ability to complete required duties, resulting in potential cybersecurity vulnerabilities for the Department.

[21] Department tools include Hyena and the ISSO Toolkit. Although ISSOs are encouraged to use these tools to perform their duties, IRM does not provide them. Instead, overseas posts are responsible for their purchase and associated licenses using their own funding and, as a result, do not always purchase them.

[22] GAO-14-704G, September 2014, at 30.

**Recommendation 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. (Action: IRM, in coordination with FSI)

# RECOMMENDATIONS

OIG provided a draft of this report to Department stakeholders for their review and comment on the findings and recommendations. OIG issued the following recommendations to the Bureaus of Information Resource Management and Global Talent Management. The Department's complete responses can be found in Appendix B.[1]

**Recommendation 1:** The Bureau of Global Talent Management, in coordination with the Under Secretary for Management, the Bureaus of Diplomatic Security and Information Resource Management, and the regional bureaus, should conduct an organizational assessment of the information systems security officer program to determine the feasibility of creating full-time overseas positions and implement the results of the assessment with an appropriate reporting structure for those positions. (Action: GTM, in coordination with M, DS, IRM, AF, EAP, EUR, NEA, SCA, and WHA)

**Management Response:** In its November 27, 2020, response, the Bureau of Global Talent Management concurred with this recommendation.

**OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Global Talent Management conducted an organizational assessment of the information systems security officer (ISSO) program to determine the feasibility of creating full-time overseas positions and implemented the results of the assessment with an appropriate reporting structure for those positions.

**Recommendation 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. (Action: IRM, in coordination with CGFS)

**Management Response:** In its November 19, 2020, response, the Bureau of Information Resource Management concurred with this recommendation.

**OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Information Resource Management incorporated an attestation relating to the completion of ISSO responsibilities in the annual Chief of Mission Management Control Statement of Assurance.

**Recommendation 3:** The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security and regional bureaus, should define the roles and

[1] OIG faced delays in completing this work because of the COVID-19 pandemic and resulting operational challenges. These challenges included the inability to conduct most in-person meetings, limitations on our presence at the workplace, difficulty accessing certain information, prohibitions on travel, and related difficulties within the agencies we oversee, which also affected their ability to respond to our requests.

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. (Action: IRM, in coordination with DS, AF, EAP, EUR, NEA, SCA, and WHA)

**Management Response:** In its November 19, 2020, response, the Bureau of Information Resource Management disagreed with this recommendation. The bureau noted that it has an oversight role with respect to regional ISSOs and does not have authority over these regional bureau resources. As such, it defers to the regional bureaus to determine the level of support overseas ISSOs need.

**OIG Reply:** OIG considers the recommendation unresolved. OIG acknowledges that regional ISSOs are regional bureau assets. Although the Bureau of Information Resource Management currently does not have authority over regional ISSOs, it has authority for ISSO liaisons, and it is responsible for establishing ISSO responsibilities across the Department. According to 5 Foreign Affairs Handbook-2 H-121, the bureau is "tasked to implement information security policy, create and implement corporate security and system security plans, perform operational monitoring, and jointly develop guidelines for system security plans." Furthermore, 1 Foreign Affairs Manual 273.1(1) states that the bureau's ISSO oversight office "is responsible for directing the coordination of ISSO activities through the [Department of State] enterprise that includes its domestic facilities and overseas missions." Accordingly, OIG determined that the Bureau of Information Resource Management is responsible for coordinating with the Bureau of Diplomatic Security and the regional bureaus to define regional ISSO and liaison roles. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security and the regional bureaus, has defined the roles and responsibilities for regional ISSOs and liaisons, clarified the level of interaction and support these positions are to give to overseas ISSOs, and updated applicable Department standards as needed.

**Recommendation 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. (Action: IRM)

**Management Response:** In its November 19, 2020, response, the Bureau of Information Resource Management concurred with this recommendation.

**OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Information Resource Management reviewed and updated the ISSO checklist and clearly stated for each task whether it should be performed by overseas ISSOs, by other overseas post information management personnel, or by the bureau.

**Recommendation 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. (Action: IRM, in coordination with FSI)

**Management Response:** In its November 19, 2020, response, the Bureau of Information Resource Management concurred with this recommendation.

**OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Information Resource Management updated the ISSO foundations training course to increase both hands-on exercises and discussion on how to perform specific tasks and use Department-provided tools.

# APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

This review was conducted from March 9 to August 24, 2020, in accordance with the Quality Standards for Inspection and Evaluation, as issued in 2012 by the Council of the Inspectors General on Integrity and Efficiency, and the Inspections Handbook, as issued by the Office of Inspector General (OIG) for the Department and the U.S. Agency for Global Media (USAGM).

The Office of Inspections provides the Secretary of State, the Chief Executive Officer of USAGM, and Congress with systematic and independent evaluations of the operations of the Department and USAGM. Consistent with Section 209 of the Foreign Service Act of 1980, this review focused on information systems security officer (ISSO) duties and responsibilities.

OIG's specific objectives for this management assistance report are to determine: (1) what findings related to non-performance of ISSO duties by overseas personnel were reported in OIG inspection reports issued in FY 2017, FY 2018, and FY 2019; and (2) what underlying factors contributed to or caused the non-performance of ISSO duties.

OIG reviewed all overseas inspection reports issued from October 1, 2016, to September 30, 2019. OIG used professional judgment, along with documentary, testimonial, and analytical evidence collected or generated, to develop its finding and an actionable recommendation. OIG also reviewed responses to an OIG survey sent to 516 overseas ISSOs soliciting information on their responsibilities and thoughts on resources, tool, and management. OIG received responses from 176 ISSOs—a return rate of 34 percent.

Spry Baltz, Brett Fegley, and Vandana Patel conducted this review. Cindy Cobham, Ellen Engels, Caroline Mangelsdorf, Kathryn McMahon, and Rebecca Sawyer also contributed to this report.

## APPENDIX B: MANAGEMENT RESPONSES

**United States Department of State**

***Washington, D.C. 20520***

UNCLASSIFIED

November 19, 2020

TO: OIG – Sandra Lewis, Assistant Inspector General for Inspections

FROM: CIO – Stuart M. McGuigan (signed)

SUBJECT: Response to OIG Draft Report - Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts

The Information Resource Management Bureau has reviewed the draft OIG inspection report. We provide the following comments in response to the recommendations provided by OIG:

**Recommendation 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. (Action: IRM, in coordination with CGFS)

**Management Response (November 2020):** IRM concurs with this recommendation. CGFS agrees that ISSO responsibilities are an important issue requiring more attention, and as such, incorporated an attestation into its FY 2020 reporting templates. In this report the OIG acknowledged the ISSO related attestation within the Annex 1 reporting template (to the COM Statement of Assurance) for FY 2020. The Deputy Chief of Mission is required to attest to every attestation within the Annex 1; however, the Chief of Mission is required to attest to not only all of the attestations within the COM Statement of Assurance, but also to all of the attestations within the Annex 1 template. Please see the second attestation on page 2 of the COM Statement of Assurance template used during FY 2020, which says: "Also taking this evaluation into consideration, As Chief of Mission, I also consider this evaluation when making other specific attestations. **I certify, to the best of my knowledge, that the statements contained in Annex 1 regarding each specific attestation listed are accurate and true."** As such, we respectfully request that this recommendation be closed.

**Recommendation 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. (Action: IRM, in coordination with DS, AF, EAP, EUR, NEA, SCA, and WHA)

**Management Response (November 2020):** IRM non-concurs with this recommendation. The recommendation language in the draft report is requesting IRM define roles and responsibilities for regional ISSO's and defines the level of support that is needed for overseas ISSO that rely on this regional service. IRM does not have the authority over regionals bureau resources and would defer to the regional bureaus on the level of support their ISSO's need to perform. IRM provides an oversight role when dealing with ISSOs, whether regional or not.

IRM suggests that this recommendation be issued to the regional bureaus for action.

**Recommendation 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. (Action: IRM)

**Management Response (November 2020):** IRM concurs with this recommendation and provides the updated link to the ISSO Checklist ver. 5.0 **ISSO Checklist**

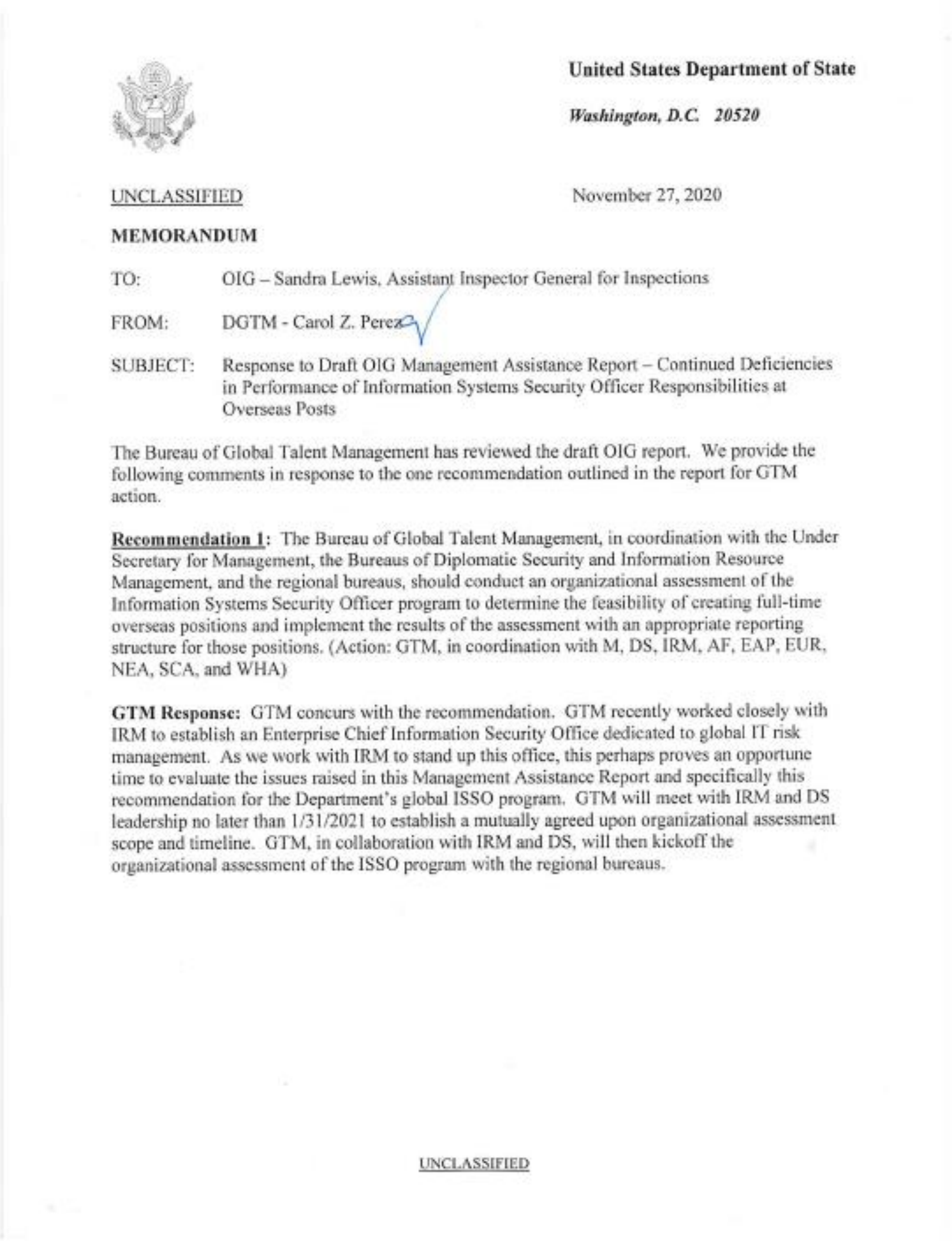
**Recommendation 5:** The Bureau of Information Resource Management, in coordination with the Foreign Service Institute, should update the information systems security officer foundations training course to increase both hands-on exercises and discussion on how to perform specific tasks and use Department-provided tools. (Action: IRM, in coordination with FSI)

**Management Response (November 2020):** IRM concurs with this recommendation. In coordination with the Bureau of Information Resource Management, the Foreign Service Institute has taken steps to update the information systems security officer foundations training course to increase both hands-on exercises and discussions on how to perform specific tasks and use Department tools in the following manner:

**Increase hands-on exercises:** To increase hands-on exercises for the students, SAIT opened up access to OpenNet in 2019 at student workstations allowing the classes to provide hands-on experience with iPost. If a student was unable to obtain an iPost account, the instructors would demonstrate iPost: its appearance, functions, report generation, and how to access and assess an individual post. Additionally, starting in the 4th quarter, the ISSO Tool Kit, which previously was only shown using Microsoft Power Point, is now illustrated live allowing for an interactive experience. This was completed in FY2019 – Q4.

**Increase discussion on how to perform specific tasks:** The addition of real hands-on experience with iPost and the live demonstration of the ISSO Took Kit has allowed our instructors to elevate the level of discussion on specific tasks that are of interest to the students. The manipulation of the Post's iPost score is broken down and analyzed allowing the students to discuss specific points such as how to increase their score. This was completed in FY2020 – Q1.

**Increase discussion on how to use Department-provided tools:** The instructors have incorporated specific lessons on how to increase the iPost scores for the different posts. By requiring the students to manipulate and learn the functions of iPost; the quantity and quality of questions regarding the Department-provided tools has greatly increased. This was completed in FY2020 – Q1.



**United States Department of State**

*Washington, D.C. 20520*

UNCLASSIFIED

November 27, 2020

**MEMORANDUM**

TO: OIG – Sandra Lewis, Assistant Inspector General for Inspections

FROM: DGTM - Carol Z. Perez

SUBJECT: Response to Draft OIG Management Assistance Report – Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts

The Bureau of Global Talent Management has reviewed the draft OIG report. We provide the following comments in response to the one recommendation outlined in the report for GTM action.

**Recommendation 1:** The Bureau of Global Talent Management, in coordination with the Under Secretary for Management, the Bureaus of Diplomatic Security and Information Resource Management, and the regional bureaus, should conduct an organizational assessment of the Information Systems Security Officer program to determine the feasibility of creating full-time overseas positions and implement the results of the assessment with an appropriate reporting structure for those positions. (Action: GTM, in coordination with M, DS, IRM, AF, EAP, EUR, NEA, SCA, and WHA)

**GTM Response:** GTM concurs with the recommendation. GTM recently worked closely with IRM to establish an Enterprise Chief Information Security Office dedicated to global IT risk management. As we work with IRM to stand up this office, this perhaps proves an opportune time to evaluate the issues raised in this Management Assistance Report and specifically this recommendation for the Department's global ISSO program. GTM will meet with IRM and DS leadership no later than 1/31/2021 to establish a mutually agreed upon organizational assessment scope and timeline. GTM, in collaboration with IRM and DS, will then kickoff the organizational assessment of the ISSO program with the regional bureaus.

UNCLASSIFIED

# ABBREVIATIONS

| | |
|---|---|
| CGFS | Bureau of the Comptroller and Global Financial Services |
| COM | Chief of Mission |
| DS | Bureau of Diplomatic Security |
| FAH | Foreign Affairs Handbook |
| FAM | Foreign Affairs Manual |
| IM | Information Management |
| IRM | Bureau of Information Resource Management |
| ISSO | Information Systems Security Officer |
| MAR | Management Assistance Report |

# HELP FIGHT

## FRAUD, WASTE, AND ABUSE

1-800-409-9926
**www.stateoig.gov/HOTLINE**

If you fear reprisal, contact the
OIG Whistleblower Coordinator to learn more about your rights.
**WPEAOmbuds@stateoig.gov**