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

ISP-17-24 | Office of Inspections | May 2017

Management Assistance Report: Non-Performance of Information Systems Security Officer Duties by Overseas Personnel

MANAGEMENT ASSISTANCE REPORT

Summary of Review

OIG reviewed reports of overseas inspections conducted from fall FY 2014 to spring FY 2016 to determine common findings on the performance of Information Systems Security Officer (ISSO) duties. OIG found that 33 percent (17 out of 51) of overseas inspections reported findings involving non-performance of ISSO duties, including findings that personnel did not perform regular reviews and analyses of information systems audits logs, user libraries, emails, workstations, servers, and hard drives for indications of inappropriate or unusual activity. OIG recommended that the Bureau of Information Resource Management develop and implement a plan to ensure overseas information management personnel perform ISSO duties in accordance with Department standards.

BACKGROUND

The Federal Information Security Management Act (FISMA) of 2002 and the Federal Information Security Modernization Act of 2014[1] required all federal agencies to develop, document, and implement an effective information security program that supports agency operations and assets. The Office of Management and Budget (OMB) through Circular A-130, Managing Information as a Security Resource, requires executive agencies to plan for security and to ensure appropriate individuals are assigned security responsibility. ISSOs are responsible for implementing the Department's information systems security program and for working closely with system managers on compliance with information systems security standards per 5 Foreign Affairs Handbook (FAH)-2 H-128.5.

The Bureaus of Information Resource Management and Diplomatic Security handle different aspects of the Department's ISSO program. The Bureau of Information Resource Management's Office of ISSO Oversight, Regional, and Domestic Division, assists, supports, and coordinates the activities of domestic and overseas ISSOs. The Bureau of Diplomatic Security's training center delivers ISSO training via a course that discusses ISSO responsibilities and gives the officers information on how they can ensure the systems' security. The course content supports the FISMA requirements for role-based training for ISSOs.

OIG inspection reports have repeatedly found deficiencies in the performance of ISSO duties. Although OIG inspection reports have highlighted embassy-specific improvements needed in this area, OIG has not conducted a Department-wide assessment. This management assistance report seeks to bring systemic issues associated with ISSO performance to the attention of Department senior management for corrective action.

[1] The Federal Information Security Modernization Act of 2014 repealed the provisions of the 2002 law relevant to this report but re-enacted identical requirements.

FINDINGS

Thirty-Three Percent of Overseas Inspections Reported Non-Performance of Information Systems Security Officer Duties

OIG reviewed information management findings in reports of overseas inspections conducted from fall FY 2014 to spring FY 2016 and found that 33 percent (17 out of 51) reported findings on the non-performance of ISSO duties. Specifically, the reports noted that information management personnel failed to perform regular reviews and analyses of information systems audits logs, user libraries, emails, workstations, servers, and hard drives for indications of inappropriate or unusual activity in accordance with Department standards.[2] OIG inspection reports identified several reasons for this lack of performance. For example, nine reports cited competing priorities because the ISSO duties had been assigned on a collateral basis. Other reports attributed these problems to supervisors who did not hold ISSOs accountable for performance of security duties and to inadequate training.

Failure by overseas information management personnel to perform information systems security duties creates vulnerabilities for Department networks. In fact, the Bureau of Diplomatic Security reported in 2016[3] that penetration tests successfully exploited vulnerabilities in email accounts of Department personnel as well as Department applications and operating systems. The Bureau of Diplomatic Security reported that ISSOs could have prevented such attempts through proactive monitoring processes and reviews of systems event logs. The exploitable vulnerabilities demonstrate that ISSOs have a valuable role to play in protecting Department networks.

Per FISMA, the Chief Information Officer is responsible for implementing an effective information security program to protect the information and information systems that support the operations and assets of the Department. Accordingly, the Chief Information Officer must enforce ISSO requirements to decrease potential risks.

Recommendation 1: The Bureau of Information Resource Management, in coordination with the regional bureaus, should implement a plan to enforce the performance of information systems security officer duties by overseas information management personnel in accordance with Department standards. (Action: IRM, in coordination with AF, EAP, EUR, NEA, SCA, and WHA)

[2] In keeping with FISMA and OMB Circular A-130, the Department has outlined guidance on ISSO duties in 5 Foreign Affairs Manual (FAM) 824, 5 FAH-2 H-128, 12 FAM 640, 12 FAH-10 H-122, 12 FAH-10 H-112, 12 FAH-10 H-163, and 12 FAH-10 H-350.

[3] 2015 OpenNet Penetration Test Executive Report, dated February 2016.

RECOMMENDATIONS

Recommendation 1: The Bureau of Information Resource Management, in coordination with the regional bureaus, should implement a plan to enforce the performance of information systems security officer duties by overseas information management personnel in accordance with Department standards. (Action: IRM, in coordination with AF, EAP, EUR, NEA, SCA, and WHA)

Management Response: IRM concurs that a plan to enforce the performance of information systems security officer duties by overseas information management personnel should be created. As these positions currently report to local post management in the regional bureaus, IRM believes it has limited ability at this time to enforce OIG's recommendation. IRM said it will work with the regional bureaus in this effort but ultimate success will depend on each regional bureau's level of participation.

OIG Response: OIG considers the recommendation resolved. The recommendation will be closed when OIG receives and accepts documentation from each regional bureau that a plan has been implemented to enforce the performance of information systems security officer duties by overseas information management personnel.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

This review was conducted 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 Inspector's Handbook, as issued by OIG for the Department and the Broadcasting Board of Governors.

The Office of Inspections provides the Secretary of State, the Chairman of the Broadcasting Board of Governors, and the Congress with systematic and independent evaluations of the operations of the Department and the Broadcasting Board of Governors. Consistent with Section 209 of the Foreign Service Act of 1980, this review focused on the Department's management controls—whether the administration of activities and operations meets the requirements of applicable laws and regulations and whether internal management controls have been instituted to ensure quality of performance and reduce the likelihood of mismanagement.

OIG's specific inspection objectives were to determine (1) what findings have been reported in OIG overseas inspection reports from fall FY 2014 to spring FY 2016 regarding deficiencies in the performance of information systems security officer duties, and (2) what underlying factors contributed to or caused the deficiencies.

OIG reviewed and analyzed all inspection reports and supporting documentation for overseas inspections performed from fall FY 2014 to spring FY 2016. OIG also reviewed Department guidelines to understand the roles, responsibilities, and processes involved in the performance of information systems security officer duties. Finally, OIG used professional judgment, along with documentary, testimonial, and analytical evidence collected or generated, to develop its finding and an actionable recommendation.

This review was conducted by Vandana Patel.

APPENDIX B: MANAGEMENT RESPONSES

United States Department of State

Washington, D.C. 20520

UNCLASSIFIED

May 11, 2017

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

FROM: IRM/PDCIO – Robert L. Adams

SUBJECT: Response to Draft OIG Report – Management Assistance Report: Non-Performance of Information System Security Officer Duties by Overseas Personnel

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

OIG Recommendation 1: The Bureau of Information Resource Management, in coordination with the regional bureaus, should implement a plan to enforce the performance of information systems security officer duties by overeseas information management personnel in accordance with Department standards. (Action: IRM, in coordination with AF, EAP, EUR, NEA, SCA, and WHA)

Management Response: IRM agrees that a plan to enforce the performance of information systems security officer duties by overseas information management personnel should be created. IRM has developed regulation, policy, and procedures thru FAM/FAH. As these positions currently report to local post management in the regional bureaus, IRM has limited ability at this time to enforce the OIG findings. IRM will work with the regionals in this effort but ultimate success will depend upon each regional bureau's level of participation.

The point of contact for this memorandum is Craig Hootselle.

UNCLASSIFIED

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
OIG.state.gov/HOTLINE
If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:
OIGWPEAOmbuds@state.gov