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

ISP-17-39 | Office of Inspections | July 2017

Management Assistance Report: Deficiencies Reported in Cyber Security Assessment Reports Remain Uncorrected

MANAGEMENT ASSISTANCE REPORT

Summary of Review

OIG's review of 50 overseas inspection reports published from February 2014 through March 2017 found 18 instances where recommendations in a Bureau of Diplomatic Security (DS) Cyber Security Assessment (CSA) report were repeated in a subsequent OIG inspection. OIG found 23 instances where DS performed a CSA—a detailed review of technical, operational, and management controls of unclassified and classified computer systems at overseas posts—at the same post before the OIG inspection. Of these 23 CSA reports, in 18 instances the subsequent OIG inspection performed at that post made the same information technology (IT) recommendations. These recommendations addressed weaknesses in information systems security officer programs, incomplete and untested IT contingency plans, noncompliant dedicated internet networks, and various physical, technical, and administrative cyber security control weaknesses. OIG conducted this management assistance review to determine why posts did not correct the cyber security weaknesses cited in CSA reports in a timely manner. OIG recommends that DS establish a process to track and verify compliance with recommendations made in CSA reports.

BACKGROUND

The Federal Information Security Management Act (FISMA) of 2002[1] and the Federal Information Security Modernization Act of 2014[2] require all federal agencies to develop, document, and implement an effective information security program that supports agency operations and assets. The Department of State (Department) assigned to DS numerous information security program responsibilities in support of FISMA.[3] One of the methods DS uses to meet FISMA requirements is the Regional Cyber Security Officer (RCSO) program, whose mission is to protect and secure information on Department computer systems. To do this, RCSOs perform on-site assessments of, and consultations with, embassies, consulates, and other sites worldwide to evaluate compliance with government policies, identify any vulnerabilities to advanced threats, and assess whether industry best practices are being used.[4] Each on-site assessment results in a CSA report—a detailed review of technical, operational, and management controls of unclassified and classified computer systems at overseas posts.[5] These reports contain recommendations for posts to address cyber security deficiencies identified by DS during the review. CSAs also include narrative and descriptions of results and suggestions for improvements in areas that passed minimum tests but still could be enhanced. DS has a target to perform a CSA of each overseas post at least once every 18 months with no more than a 36-month gap between CSAs. CSAs are advisory reports, and posts are not required to implement CSA recommendations or suggestions.

[1] 44 U.S.C. Sections 3541-3549.

[2] 44 U.S.C. Sections 3551-3558.

[3] 1 FAM 262.7-2, Office of Cybersecurity (updated June 30, 2015); 1 FAM 272.3, Office of Information Technology Security Compliance (December 5, 2016).

[4] RCSO home page https://intranet.ds.state.sbu/DS/SI/CS/ESS/RCSO/default.aspx, April 26, 2017.

[5] 1 FAM 262.7-2, Office of Cybersecurity (DS/SI/CS) (updated June 30, 2015).

OIG found in many of its recent overseas inspections that CSA recommendations had yet to be implemented. OIG conducted this management assistance review to determine why posts did not comply with CSA findings and recommendations to mitigate cyber security risks and vulnerabilities.

FINDING: NO PROCESS IN PLACE TO VERIFY COMPLIANCE WITH CYBER SECURITY ASSESSMENT RECOMMENDATIONS

OIG reviewed 50 overseas inspection reports published from February 2014 through March 2017 and found 23 instances where DS performed a CSA before the OIG inspection. Of these 23 CSA reports, in 18 instances the subsequent OIG inspection made the same IT recommendations. Issues included inadequate performance of information systems security officer duties, incomplete or untested IT contingency plans, unidentified dedicated internet networks, physical control deficiencies, administrative control weaknesses, and technical controls issues.[6] Six OIG reports specifically cited instances in which the embassy did not address findings or recommendations previously included in CSA reports.[7]

In accordance with FISMA, 1 Foreign Affairs Manual (FAM) 262.7(1) and 1 FAM 262.7-2, DS, through the CSA reports, provides policy and implementation guidance to overseas posts with detailed, technical analyses of weaknesses and vulnerabilities for the post's information and computer systems. However, DS does not require posts to implement CSA recommendations or have any process to verify that compliance or remediation activities have addressed findings and recommendations in CSA reports. Without such a requirement to implement CSA recommendations, and without any process or mechanism in place to monitor compliance, potential risks that Department information and computer systems could be compromised will remain unmitigated.

> **Recommendation**: The Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management and regional bureaus, should require implementation of Cyber Security Assessment report recommendations and establish a process to track and verify that overseas posts comply with those recommendations. (Action: DS, in coordination with IRM, AF, EAP, EUR, NEA, SCA, and WHA)

[6] Specific technical details are purposefully excluded to keep this document unclassified.

[7] The time between Cyber Security Assessment reports and OIG Inspection reports for identified posts ranged from one month to forty-one months with an average of over ten months between the two reports.

RECOMMENDATION

OIG provided a draft of this report to Department stakeholders for their review and comment on the findings and recommendation. OIG issued the following recommendation to the Bureau of Diplomatic Security. Its complete response can be found in Appendix B.

Recommendation: The Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management and regional bureaus, should require implementation of Cyber Security Assessment report recommendations and establish a process to track and verify that overseas posts comply with those recommendations. (Action: DS, in coordination with IRM, AF, EAP, EUR, NEA, SCA, and WHA)

Management Response: In its July 19, 2017, response, the Bureau of Diplomatic Security concurred with the recommendation. The bureau noted that it will coordinate with IRM to determine the best tracking and verification processes to meet the requirements of the recommendations.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of a process to ensure overseas posts' compliance with recommendations in Cyber Security Assessment reports.

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 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 (1) identify recurring findings and recommendations cited in both Cyber Security Assessment reports and OIG inspection reports, and (2) identify factors contributing to non-compliance with recommendations made in Cyber Security Assessment reports.

OIG reviewed and analyzed all Cyber Security Assessment reports and OIG inspection reports published from February 2014 through March 2017. OIG also reviewed Department guidelines to understand the roles, responsibilities, and processes involved in the performance of Cyber Security Assessments. Finally, OIG used professional judgment, along with documentary, testimonial, and analytical evidence collected or generated, to develop its finding and an actionable recommendation.

Timothy Williams conducted this review.

APPENDIX B: MANAGEMENT RESPONSES

United States Department of State

Assistant Secretary of State
for Diplomatic Security
Washington, D.C. 20520

UNCLASSIFIED

July 18, 2017

INFORMATION MEMO TO INSPECTOR GENERAL LINICK - OIG

FROM: DS – Bill A. Miller, Acting JUL 19 2017

SUBJECT: Bureau of Diplomatic Security Response to the Office of Inspector General (OIG) Management Assistant Report Deficiencies Reported in Cyber Security Assessment (CSA) Reports Remain Uncorrected, ISP-17-39

Below is the Bureau of Diplomatic Security's response to Recommendation 1 of the draft report.

Recommendation 1: The Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management and regional bureaus, should require implementation of CSA report recommendations and establish a process to track and verify that overseas posts comply with those recommendations.

DS Response (7/18/17): DS concurs that more formal tracking of the CSA findings and recommendations identified by Regional Computer Security Officers is necessary to drive prompt remediation of cybersecurity vulnerabilities by all stakeholders, to include: posts, regional bureaus, and IRM. DS will coordinate with IRM to determine the best tracking and verification processes to meet this recommendation.

UNCLASSIFIED

Approved: DS – Bill A. Miller

Drafted: DS/CTS – W. Stevens (x5-2593)

Cleared: M – D. Winters (ok)
IRM – C. Eckert (ok)
DS/DSS – C. Schurman (ok)
DS/EX – W. Terrini (ok)
DS/EX/MGT – J. Schools (ok)
DS/MGT/PPD – M. Scherger (ok)
DS/MGT/PPD – L. Long (ok)
DS/CTS – L. Price (ok)
DS/CTS – M. Holland (ok)

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