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

ISP-16-05 Office of Inspections February 2016

Management Assistance Report: Continued Deficiencies Identified in Information Technology Contingency Planning

MANAGEMENT ASSISTANCE REPORT

~~IMPORTANT NOTICE: This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

Summary of Review

OIG identified IT contingency planning deficiencies in 69 percent (20 out of 29) of overseas inspections performed during FYs 2014 and 2015. The issues identified ranged from information management staff at posts not developing, updating, or testing IT contingency plans to plans that lacked appropriate key stakeholders and contact information as part of emergency preparedness, contrary to requirements set forth in 5 Foreign Affairs Manual (FAM) 1064, 12 FAM 623.7, 12 FAM 632.3, and National Institute of Standards and Technology Special Publication 800-34. This report recommends that the Department take action to ensure that information management personnel are held accountable for IT contingency planning by making this responsibility explicit in their work requirements.

BACKGROUND

Information systems are vital to the business processes that support an agency mission, and as such it is critical that personnel are able to ensure continuity of operations. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a post to recover as quickly and effectively as possible after an unforeseen incident. Contingency planning puts measures in place to recover information system services after a disruption, which could include relocation to an alternate site, recovery using alternate equipment, or performance of information system functions using manual methods. An IT contingency planning process involves several steps:[1]

- Developing a contingency planning policy
- Conducting a business impact analysis
- Identifying preventive controls
- Creating contingency strategies
- Developing a contingency plan
- Ensuring contingency plan testing and training
- Maintaining and updating the contingency plan on a regular basis

Effective IT contingency planning is crucial to overseas posts should they encounter any unforeseen incidents. The 2014 Department network intrusion, for example, highlighted the importance of being prepared to restore operations in a prompt manner while protecting information and the systems that process it. Embassy Mexico City recently relied on IT contingency plans as part of emergency actions during the September 2014 hurricane that impacted the region. The embassy reported on its lessons learned and noted that attention needed to be placed on ensuring that key personnel were included in IT contingency plan

[1] Guidance from National Institute of Standards and Technology Special Publication 800-34.

testing exercises and ongoing planning as well as the need to adopt a mission-wide approach to emergency preparedness.

Recommendations from 2011 OIG Memorandum Report Unimplemented

OIG inspection teams continue to report IT contingency planning findings in overseas inspection reports, despite a December 2011 OIG memorandum[2] to the Bureau of Information Resource Management with two recommendations addressing the topic. The memorandum identified IT contingency planning issues involving bureaus' and posts' lack of attention to developing and testing IT contingency plans as part of their emergency preparedness activities. The Bureau of Information Resource Management stated in compliance responses that it was planning to implement a tracking mechanism and develop a SharePoint site to capture risk scoring compliance for posts and bureaus. However, after 4 years the bureau still lacks a tracking mechanism and a SharePoint site as mentioned in their compliance responses. The September 2015 compliance response noted that the bureau is researching other alternatives to comply with OIG recommendations.[3]

FINDING

Work Requirements of Information Management Staff

A review of Foreign Service employee evaluation reports for information management officers or the most senior information management personnel at embassies and consulates revealed that only 12 percent (32 out of 272) had a stated work requirement to develop and test IT contingency plans. According to 5 FAM 825 and 5 FAM 826, responsibility for the development and testing of IT contingency plans lies with the information management staff overseas.

> **Recommendation 1:** The Bureau of Information Resource Management, in coordination with the regional bureaus, should include the requirement to complete and test information technology contingency plans in the work requirements for information management personnel. (Action: IRM, in coordination with AF, EAP, EUR, NEA, SCA, and WHA)

[2] OIG, *Improvements Needed in Information Technology Contingency Planning* (ISP-I-12-04, December 2011).

[3] Department of State September 3, 2015, memorandum "IRM/BMP/SPO/SPD – Perry Romeo to OIG/ISP".

RECOMMENDATIONS

Recommendation 1: The Bureau of Information Resource Management, in coordination with the regional bureaus, should include the requirement to complete and test information technology contingency plans in the work requirements for information management personnel. (Action: IRM, in coordination with AF, EAP, EUR, NEA, SCA, and WHA)

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