



United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

DEC 15 2011

SENSITIVE BUT UNCLASSIFIED

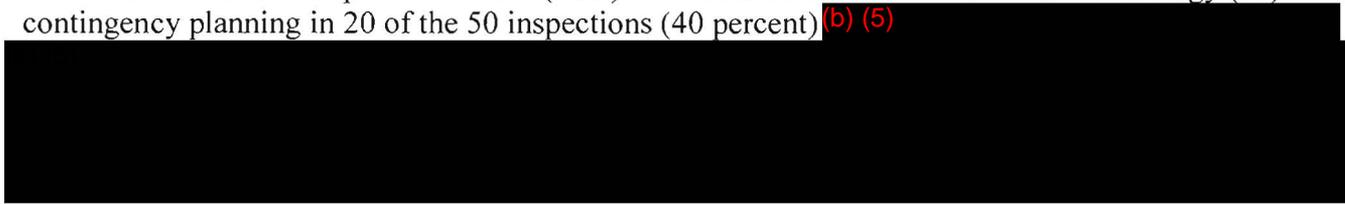
MEMORANDUM

TO: IRM – Ms. Susan Swart

FROM: OIG – Harold W. Geisel 

SUBJECT: Memorandum Report - Improvements Needed in Information Technology Contingency Planning, ISP-I-12-04

The Office of Inspector General (OIG) identified issues with information technology (IT) contingency planning in 20 of the 50 inspections (40 percent) (b) (5)



A properly documented and tested IT contingency plan has a direct impact on whether a bureau or post can operate effectively after an unforeseen incident. Information systems are vulnerable to a variety of disruptions, from short-term power outages or disk drive failures to equipment destruction. While some system vulnerabilities can be minimized, it is virtually impossible to eliminate all the risks to an information system. Effective IT contingency planning—including thorough testing of the plan—is essential, to mitigate the risk of system and service unavailability.

An IT contingency planning process involves several steps:

- developing a contingency planning policy;
- conducting a business impact analysis;
- identifying preventive controls;
- creating contingency strategies;
- performing test and training exercises; and
- maintaining and updating the contingency planning document on a regular basis.¹

SENSITIVE BUT UNCLASSIFIED

¹ National Institute of Standards and Technology Special Publication 800-34, Revision 1, Chapter 3, *Contingency Planning Guide for Federal Information Systems*, May 2010.

Proper IT contingency planning was crucial to several overseas posts that dealt with unforeseen, catastrophic incidents in the last year. The earthquake and tsunami in Japan, for example, highlighted the importance of post personnel reviewing IT operations and assessing which critical functions and systems would be required in the event of an emergency. In a “lessons learned” document prepared for the Bureau of Information Resource Management (IRM), Embassy Tokyo cited preparation as a key to their ability to resume critical operations after the natural disaster. As stated by Embassy Tokyo’s information management officer, the level of advanced IT preparation made it easier for them to set up their alternate communications site. In addition to having a complete and pretested IT contingency plan, the embassy described the importance of having all required equipment, contact information, and instructions ready and distributed. All these elements are necessary for a smooth recovery.

Inspection Findings

Given the importance of maintaining telecommunications and IT operations in the aftermath of catastrophic incidents, OIG selected IT contingency planning as an area of emphasis for 2010 and 2011. (b) (5)

[REDACTED]

(b) (5)

Posts are required to provide for an off-site storage location in a U.S. Government approved and controlled facility, to minimize the potential for complete loss of programs and data in an emergency. In a catastrophic event, it is imperative that posts have their backup media stored in another location, preferably one that is not subject to the same environmental concerns as the primary location.

(b) (5)

According to 12 FAM 622.3-2 d., domestically, the system manager—in coordination with the information systems security officer and the data center manager—will coordinate the IT contingency plan with the emergency action plan, to ensure that any emergency response procedures specified in the contingency plan are consistent with the emergency action plan. Abroad, the information management officer and the regional security officer will coordinate both plans in conjunction with the data center manager and the system manager to ensure consistency.

SENSITIVE BUT UNCLASSIFIED

-3-

In accordance with 12 FAM 613.11 and 5 FAM 121.1, the information management officer is responsible for the overall management of contingency planning at overseas posts, including ensuring that the IT contingency plan is fully coordinated with the post's emergency action plan. Domestically, the system owner is responsible for ensuring that contingency plans are developed and maintained for each system and application, per 5 FAM 825 b.(3). However, in accordance with 5 FAM 822 (2), the responsibility for contingency planning ultimately lies with IRM to ensure the availability of IT systems and operations that support the Department's diplomatic, consular, and management operations.

The lack of a properly developed and tested IT contingency plan that is linked with overall emergency preparedness processes could be detrimental to a post's or bureau's recovery efforts following an unforeseen incident. During the IT contingency planning process—including drafting, testing, and updating—information management personnel are able to identify and address deficiencies. The planning process also provides a sound training environment, enabling emergency personnel to become familiar with potential emergency situations. Without such a process, bureaus and posts are vulnerable to the loss of availability of network systems, data, and communications capabilities.

Available Resources

The Department has several resources for employees seeking information on IT contingency planning. These include an online Foreign Service Institute (FSI) course on developing, maintaining, and implementing an IT contingency plan. Contingency planning also is included in the FSI IRM Tradecraft course, which focuses on the basic responsibilities of information management officers. Additionally, IRM's Office of Information Assurance Intranet site has templates, frequently asked questions, and basic guidance on contingency planning.

Even though these resources are readily available, the Department has not held assigned personnel within bureaus and posts accountable for complying with the requirements for IT contingency planning. IRM has no definitive means of ensuring that employees complete IT contingency plans and address all elements identified in Department regulations. As mentioned in IRM's Office of Information Assurance Web site, system owners are currently required to provide IT contingency planning test results for reportable systems and applications as part their Federal Information Security Management Act of 2002 compliance. However, this requirement does not apply to all bureaus and posts for their IT contingency planning components.

If IRM were to implement and enforce a tracking mechanism, it could help the Department ensure that all responsible parties are developing, updating, and testing IT contingency plans. Including IT contingency planning requirements as a rating factor in the performance appraisals for responsible system owners and information management personnel also would motivate responsible individuals to fulfill this critical element in protecting the Department's networks and systems.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

-4-

Including IT contingency planning requirements as a rating factor in the performance appraisals for responsible system owners and information management personnel also would motivate responsible individuals to fulfill this critical element in protecting the Department's networks and systems.

Further, the Department should include the completion and testing of IT contingency plans as factors in the methodology for determining risk scores for bureaus and posts, in applications such as iPost (a tool that allows authorized users to access enterprise network performance and system security monitoring data). Currently, the risk scores are calculated using elements such as patch management, antivirus, and cyber security awareness training statistics. If the Department were to include IT contingency planning as part of the risk scoring in iPost or another application, the information management personnel at bureaus and posts would have an additional incentive to comply with contingency planning requirements.

Recommendation 1: The Bureau of Information Resource Management should implement and enforce a tracking mechanism to document whether or not bureaus and posts have complied with information technology contingency planning requirements. (Action: IRM)

Recommendation 2: The Bureau of Information Resource Management should include the development and testing of contingency plans as criteria in its risk scoring methodology for site health of posts and bureaus. (Action: IRM)

I would be happy to meet with you to discuss this matter further, or your staff may contact

(b) (6)

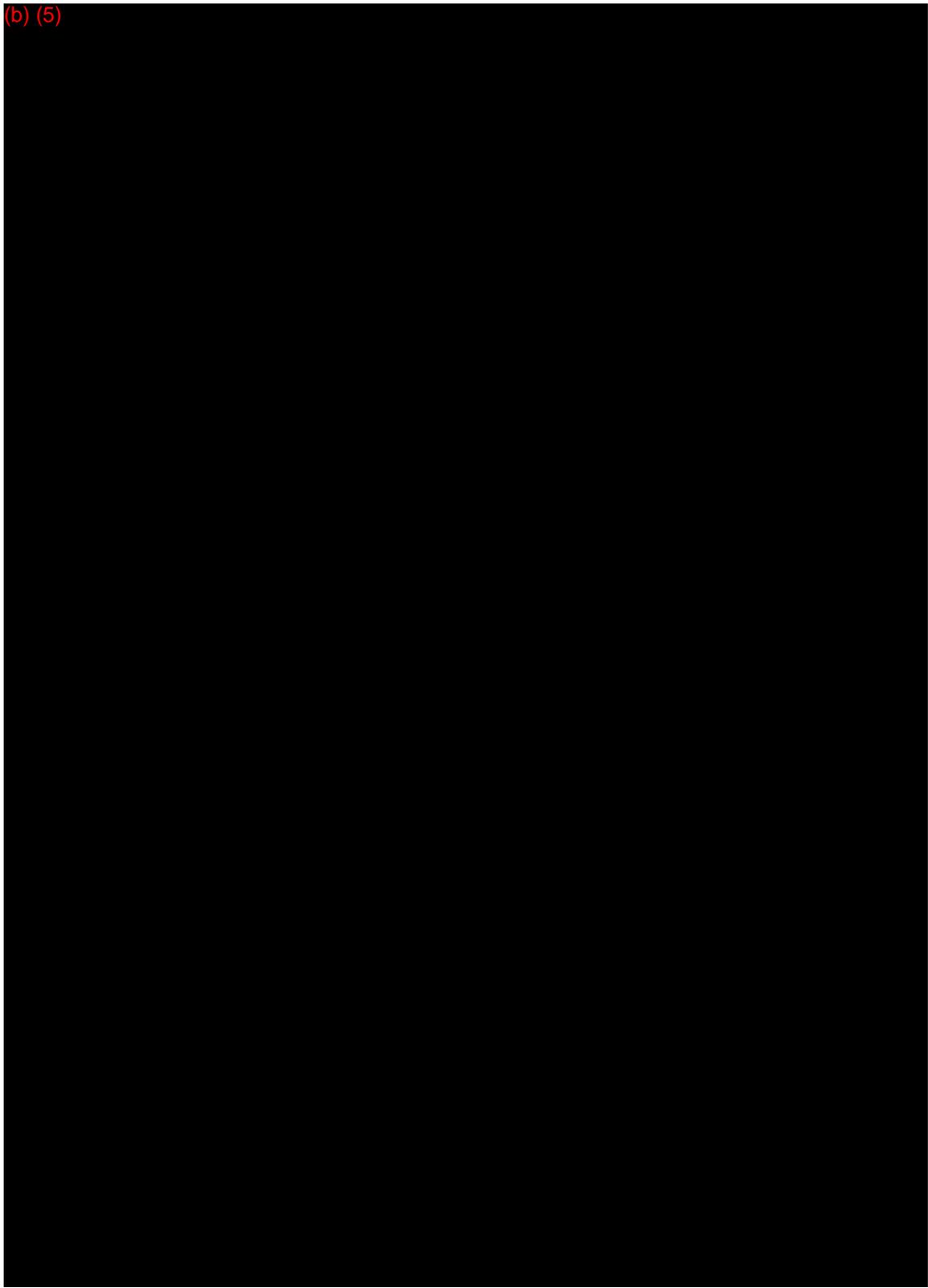
A large black rectangular redaction box covers the majority of the text in this section, starting below the word 'contact' and extending down to the 'Enclosures' section.

Enclosures:

Compliance Information and Instruction Sheet

SENSITIVE BUT UNCLASSIFIED

(b) (5)



(b) (5)

