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

AUD-IT-16-26 | Office of Audits | February 2016

Management Assistance Report: Department of State Incident Response and Reporting Program

MANAGEMENT ASSISTANCE REPORT

Summary of Review

The overall purpose of an IT incident response and reporting (IR&R) program is to allow an organization to detect cyber security incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations quickly. Acting on OIG's behalf, Williams, Adley & Company-DC, LLP (Williams, Adley), an independent public accounting firm, evaluated the effectiveness of the Department of State's (Department) IR&R program for the months of September and October 2014 in accordance with Department information security policies and procedures.

Overall, Williams, Adley determined that the Department's IR&R program was not operating effectively. Specifically, of the 25 cyber security incidents evaluated, Williams, Adley found that five were miscategorized, six were not remediated in a timely manner, one was not identified in a timely manner, one was missing incident information, four were not reported to the U.S. Computer Emergency Readiness Team (US-CERT) in a timely manner, and two were not reported to US-CERT as required.

The deficiencies in the IR&R program occurred primarily because of inadequate communication between the Bureau of Information Resource Management (IRM) and the Bureau of Diplomatic Security (DS) and inadequate management oversight that would ensure that personnel within the Department's incident response team fully complied with prescribed categorization guidelines, reporting requirements, and remediation timelines.

Without an effective IR&R program, the Department may be unable to properly identify weaknesses, restore IT operations in a timely manner, and identify and respond to cyber security incidents, which could potentially lead to interruptions of critical operations and hinder the Department's ability to achieve its core mission.

In its response (see Appendix D) to a draft of this report, DS concurred with the two recommendations. OIG considers both recommendations resolved, pending further action. DS's response to each recommendation and OIG's reply are presented after each recommendation.

OBJECTIVE

OIG's Office of Audits contracted with Williams, Adley, an independent public accounting firm, to evaluate the effectiveness of the Department's IR&R program for the months of September and October 2014 in accordance with Department information security policies and procedures.

BACKGROUND

The Department is the U.S. Government's principal agency for advancing freedom for the benefit of the American people and the international community by helping to build and sustain a more democratic, secure, and prosperous world composed of well-governed states. The Department's mission is carried out by geographic and functional bureaus that provide policy guidance, program management, administrative support, and in-depth expertise. The Department has an extensive overseas presence, with over 275 missions worldwide. The Department, as well as its contractors, depends on information systems and electronic data to carry out essential mission-related functions. The security of these systems and networks is vital to protecting national and economic security, public health and safety, and the flow of commerce. As such, these information systems are subject to serious threats that can have adverse effects on organizational operations (that is, missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.

Cyber Security Trends

In April 2014, the Government Accountability Office (GAO) reported[1] that cyber security incidents reported by Federal agencies increased almost 33 percent in FY 2013. According to another GAO report,[2] cyber security incidents reported to US-CERT by Federal agencies increased from 41,776 cyber security incidents in FY 2010 to 67,168 cyber security incidents in FY 2014. Reported attacks and unintentional cyber security incidents involving Federal systems, such as those involving data loss or theft, computer intrusions, and privacy breaches, underscore the importance for agencies to have an effective IR&R program.

Incident Response and Reporting

The overall purpose of an IR&R program is to determine the kinds of attacks that have been successful and to allow agencies to make risk-based decisions as to where it is most cost effective to focus security resources. A well-defined incident response capability helps an agency detect cyber security incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations quickly. Proactive monitoring of networks and computing infrastructure, along with effective incident response policies, management processes, and operational practices, is paramount to having an effective IR&R program.

U.S. Computer Emergency Readiness Team

US-CERT is the Federal information security incident center mandated by the Federal Information Security Management Act of 2002. US-CERT's purpose is to help Federal agencies detect, report, and respond to cyber security incidents. Specifically, US-CERT consults with agencies on cyber security incidents and provides technical information in order to assist agencies in their incident response efforts. In addition, US-CERT compiles cyber security information, publishes the information on its website, and disseminates timely notifications to

[1] GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices* (GAO-14-354, April 2014).
[2] GAO, *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems* (GAO-15-573T, April 2015).

agencies regarding current and potential security threats and vulnerabilities. US-CERT does not replace existing agency response teams; rather, it augments the efforts of Federal agencies by serving as a focal point for dealing with cyber security incidents. US-CERT analyzes the agency-provided information to identify trends and indicators of attacks; these are easier to discern when reviewing data from many organizations than when reviewing the data of a single organization. Furthermore, US-CERT defines seven categories[3] of cyber security incidents that Federal agencies use when reporting a cyber security incident. Agencies are required to report cyber security incidents to US-CERT within specified timeframes (for example, within one hour, one week, or one month) depending on the category of the incident. Details regarding these seven categories and associated reporting timeframes are presented in Appendix B.

Federal Laws, Standards, and Guidelines

The Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014, requires that Federal agencies create, provision, and operate a formal incident response program. The National Institute of Standards and Technology (NIST)[4] provides guidance to aid Federal agencies in meeting this requirement.

According to NIST,[5] organizing an effective cyber security incident response program involves several major decisions and actions. One of the first considerations is creating an organization-specific definition of the terms "event" and "incident" to ensure a clear IR&R scope. NIST defines an event as any occurrence observed on a network and/or system. Examples of events that may become cyber security incidents include system crashes, unauthorized use of privileges, and execution of malware. Events are recognized as cyber security incidents only after evidence indicates a violation, or imminent threat of violation, of computer security policies and procedures or standard security practices. User analysis of an event is necessary in order to determine whether an event can be identified as a cyber security incident.

Department Policy and Procedures

Department policies and procedures for identifying, handling, responding to, and reporting cyber security incidents are included in Volumes 5 and 12 of the Foreign Affairs Manual and the Foreign Affairs Handbook (Information Management and Diplomatic Security series, respectively).

According to Department guidance,[6] IRM and DS both have responsibilities for information security. In order to secure and protect the confidentiality, integrity, and availability of the Department's networks, information systems, and data, DS and IRM must coordinate and integrate their diverse sets of IR&R responsibilities and capabilities. Appendix A provides a detailed description of the specific-incident response governance roles, management processes, and operational practices.

[3] US-CERT, <https://www.us-cert.gov/government-users/reporting-requirements>, accessed on October 12, 2015.
[4] NIST SP 800-61, rev. 2, Computer Security Incident Handling Guide, August 2012.
[5] Ibid.
[6] IRM and DS Cyber Security Roles, October 2003.

In addition, IRM and DS have developed separate internal standard operating procedures (SOP) and incident-specific instructions. These SOPs describe specific security-incident monitoring, response, and reporting processes and activities applicable to the incident response functions, processes, and activities within IRM and DS. Within DS, the Computer Incident Response Team (CIRT) acts as a central reporting point for computer security events on all Department automated information systems. According to the CIRT SOP,[7] the incident handling process begins when CIRT identifies an incident; creates a ticket; and, based on the potential severity and impact of the incident, assigns an initial category based on US-CERT's incident-type classifications (see Appendix B). CIRT then performs a more in-depth analysis of the incident based on the assigned category and makes a determination of how the incident is reported thereafter. In some instances, CIRT management may determine that incidents were initially miscategorized based on the actual level of severity and impact on the network. CIRT management will recategorize the incident prior to closing the ticket.

RESULTS

Williams, Adley determined that the Department's IR&R program was not operating effectively for the months of September and October 2014. Specifically, Williams, Adley reviewed the Department's handling of 25 cyber security incidents out of 303 incidents (CAT 1 to CAT 6) reported during the scope period[8] to determine whether the Department complied with its information security policies and procedures. Williams, Adley identified deficiencies in 14 of the 25 cyber security incidents tested, as shown in Table 1.

Table 1: Incidents Reviewed With Deficiencies

Incident Category	Event Type	Incident Details	Deficiencies Identified
CAT 1	Unauthorized Access	Defaced Department website User Logon ID and password posted to public website	-Event type and incident details miscategorized by CIRT analyst
CAT 1	Unauthorized Access	Connection to remote system	-Event type and incident details miscategorized by CIRT analyst
CAT 2	Denial of Service	Distributed attack	-Event type and incident details miscategorized by CIRT analyst -Untimely remediation (more than 8 days)
CAT 2	Denial of Service	Distributed attack	-Untimely identification of incident -Incomplete incident information
CAT 3	Malicious Code	Email – malicious payload	-Untimely reporting to US-CERT (2 hours)
CAT 3	Malicious	Malicious code confirmed on	-Incident not reported to US-CERT

[7] DS, Cyber Security Operations Support, CIRT SOP, August 2014.
[8] Williams, Adley's sampling methodology is in Appendix C.

Incident Category	Event Type	Incident Details	Deficiencies Identified
	Code	internal machine	as required
CAT 3	Malicious Code	Email - malicious payload	-Untimely remediation (more than 7 days) -Untimely reporting to US-CERT (reported to US-CERT after remediation)
CAT 3	Malicious Code	Malicious email payload confirmed on internal machine	-Untimely remediation (more than 12 days) -Untimely reporting to US-CERT (20 hours)
CAT 3	Malicious Code	Malicious code confirmed on internal machine	-Untimely remediation (more than 6 days)
CAT 3	Malicious Code	Malicious email payload confirmed on internal machine	-Untimely remediation (more than 11 days) -Untimely reporting to US-CERT (4 hours after remediation)
CAT 4	Improper Usage	Classified Spillage	-Incident not reported to US-CERT
CAT 5	Scans/Probes/ Attempted Access	Attempted access	-Event type and incident details miscategorized by CIRT analyst
CAT 5	Scans/Probes/ Attempted Access	Scan	-Event type and incident details miscategorized by CIRT analyst
CAT 5	Scans/Probes/ Attempted Access	Probe	-Untimely remediation (more than 7 days)

Source: Prepared by Williams, Adley based on results of testing.

According to NIST,[9] an event may become a cyber security incident when a violation (or imminent threat of violation) of computer security policies, acceptable user policies, or standard security practices occurs. The Department escalates an event to incident status when any of the following actions occur: unauthorized access to the Department network, website defacement, unauthorized software that incurs a security threat to the Department network, loss of Department personally identifiable information, or when a senior-level executive is affected.[10] In addition, the CIRT SOP[11] states that the CIRT shift supervisor ensures proper updates are applied to cyber security event and incident tickets on a daily basis. Williams, Adley found that five cyber security incidents were miscategorized and therefore determined that CIRT analysts did not review and re-categorize the incidents as necessary prior to closing the cyber security incident tickets.

[9] NIST 800-61, rev. 2.
[10] DS, Cyber Security Operations Support, CIRT SOP.
[11] Ibid.

According to the CIRT SOP,[12] the CIRT technical lead ensures that Tier 2[13] projects are properly handled in a timely manner. Williams, Adley found that six cyber security incidents were not remediated timely.[14] Specifically, remediation of one denial of service attack took over 200 hours, remediation of four malicious code attacks took between 174 hours and 312 hours, and remediation of one probe attack took over 175 hours.

According to the Foreign Affairs Manual,[15] all employees are responsible for reporting cyber security incidents to their information system security officer upon detection so that their information system security officer can report the incidents to CIRT. However, Williams, Adley found that one cyber security incident involving a denial of service attack was not reported to CIRT upon detection. Specifically, CIRT did not create an incident ticket until 2 hours and 45 minutes after the event was identified.

According to the CIRT SOP,[16] all communication emails and telephone conversation summaries should be recorded in each incident ticket's work log. However, Williams, Adley found that one cyber security incident involving a denial of service attack was missing required information concerning a forwarded email.

According to the CIRT SOP,[17] cyber security incidents involving malicious code should be reported to US-CERT daily or within one hour of discovery or detection if widespread across the agency. Williams, Adley found that four cyber security incidents with the malicious code-related category were not reported to US-CERT in a timely manner. Specifically, Williams, Adley found that one cyber security incident, which affected four users, was reported to US-CERT 2 hours and 24 minutes after identification. Williams, Adley found that a second cyber security incident affected four users, including one senior-level executive, and was reported to US-CERT more than 180 minutes after identification. Williams, Adley found that a third cyber security incident, which possibly affected 10 or more users, was reported to US-CERT almost 20 hours after identification. Finally, Williams, Adley found that a fourth cyber security incident affecting one user was reported to US-CERT almost 223 hours after identification.

According to the CIRT SOP,[18] incidents are required to be reported to US-CERT within specified timeframes depending on the category of the incidents. Williams, Adley found that two cyber security incidents were not reported to US-CERT as required by both incidents' category levels. Specifically, one cyber security incident involved malicious code on an internal Department machine, which should have been reported to US-CERT within one day. The second cyber-security incident

[12] Ibid.
[13] According to the DS, Cyber Security Operations Support, CIRT SOP, Tier 2 responsibilities include, among other things, conducting advanced analysis and recommending remediation steps for computer security events and incidents.
[14] While the US-CERT reporting requirements for these types of incidents are within 2 hours of discovery or detection, Williams, Adley determined that remediation efforts for these types of incidents should not exceed 72 hours.
[15] 12 FAM 590, "Cyber Security Incident Program," March 2011.
[16] DS, Cyber Security Operations Support, CIRT SOP.
[17] Ibid.
[18] Ibid.

involved classified spillage, which should have been reported to US-CERT after CIRT notified the Program Applications Division within DS and within one week.

Williams, Adley determined that the Department's IR&R program was not operating effectively because there was insufficient communication between IRM and DS officials throughout the IR&R process and there was a lack of DS management oversight ensuring that responsible personnel fully complied with prescribed categorization guidelines, reporting requirements, and remediation timelines. As IRM and DS both have statutory responsibilities for information security, both bureaus must coordinate and integrate their diverse IR&R responsibilities and capabilities.

DS and IRM officials acknowledged that improvements were needed to strengthen the effectiveness and responsiveness of communications between both bureaus when responding to, analyzing, and remediating cyber security incidents. DS officials stated that a proposed solution was currently being developed that would improve the responsiveness of and communications between DS and IRM. Specifically, the Department would create a Joint Concept of Operations, via a Memorandum of Understanding, that would enhance the current capabilities of the DS Foreign Affairs Cybersecurity Center. Although the Memorandum of Understanding was in the initial drafting phase as of the date of this report, it is a proposed solution that, when fully implemented, will allow the Department to approve a Joint Security Operations Center concept that will potentially consolidate core IRM and DS cyber security functions and thus strengthen the responsiveness of and communications between IRM and DS. This effort will serve as the first step in improving communications between IRM and DS.

DS officials also acknowledged that improvements were needed for effective IR&R process implementation. Specifically, DS management oversight was needed to ensure that CIRT analysts reviewed and re-categorized cyber security incidents prior to closing incident tickets. DS management oversight was also needed to ensure timely identification, reporting, and remediation of cyber security incidents.

Impact

Over the past year, the Department reported multiple network intrusions that caused unscheduled downtimes; loss of productivity; and, in some cases, loss of data.[19] Without effective communication between IRM and DS and improvements in DS management oversight throughout the IR&R process, the Department may be unable to properly identify and respond to unauthorized breaches while minimizing loss and destruction and restoring IT operations quickly, which could adversely impact the Department's overall business mission. For example, as reported in the media,[20] a breach in August 2015 led to months-long email attacks against the Department.

[19] U.S. Department of State Cybersecurity Strategy, August 2015.

[20] Nextgov, <http://www.nextgov.com/cybersecurity/2015/08/common-malware-jimmied-open-white-house-and-anthem-systems-say-researchers/119085/?oref=dropdown#>, accessed on August 17, 2015.

Ineffective communication between DS and IRM throughout the IR&R process hinders both bureaus' abilities to coordinate and integrate their diverse sets of IR&R responsibilities. Furthermore, ineffective communication could delay cyber security incident response times and remediation, which could potentially lead to interruptions of critical operations and potentially cause breaches in other agencies.

In addition, without effective DS management oversight for the IR&R process, CIRT personnel may not be able to consistently follow established cyber security incident reporting requirements. These requirements are established to allow the Department to determine the kinds of attacks that have been successful and to enable the Department to make risk-based decisions about where it is most cost effective to focus its security resources. Furthermore, without following these requirements, US-CERT would be unable to assist the Department in responding to cyber security incidents and unable to disseminate timely notifications to other Federal agencies regarding current and potential security threats and vulnerabilities.

CONCLUSION

Williams, Adley determined that the Department's IR&R program was not operating effectively. Specifically, for 14 of the 25 cyber security incidents evaluated, CIRT personnel did not fully comply with categorization guidelines, reporting requirements, and remediation timelines as defined in the Department's information security policies and procedures. Specifically, Williams, Adley found that five incidents were miscategorized, six were not remediated in a timely manner, one was not identified in a timely manner, one was missing incident information, four were not reported to US-CERT in a timely manner, and two were not reported to US-CERT as required. These deficiencies occurred primarily because of insufficient communication between IRM and DS officials during the IR&R process and a lack of DS management oversight. An effective IR&R program is critical for ensuring that the Department's networks, information systems, and data are secured and protected.

Recommendation 1: OIG recommends that the Bureau of Diplomatic Security, in conjunction with the Bureau of Information Resource Management, finalize and implement the Joint Cyber Security Concept of Operations Memorandum of Understanding.

Management Response: DS and IRM concurred with the recommendation and requested that it be closed as IRM and DS have finalized and signed a Memorandum of Understanding establishing the Department's Joint Security Operations Center.

OIG Reply: OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM and DS have executed and implemented a Memorandum of Understanding to facilitate communication between IRM and DS officials during the IR&R process.

Recommendation 2: OIG recommends that the Bureau of Diplomatic Security (DS) amend the Computer Incident Response Team Standard Operating Procedures to provide management oversight responsibility to the Office of Cybersecurity. Specifically, DS should ensure that responsible supervisory personnel follow established categorization guidelines, reporting requirements, and remediation timelines in accordance with the Department of State's cyber security incident response and reporting policies and procedures.

Management Response: DS and IRM concurred with the recommendation and requested that it be closed based on recent enhancements to the Department's cyber incident response program capabilities. Specifically, DS stated that the Department has taken the following actions:

- Established the Joint Security Operations Center.
- Hired and placed additional Senior Watch Officers, which will ensure the constant presence of supervisory personnel to direct and manage incident response program activities.

DS also stated that it already performs an annual review of its standard operating procedures to ensure that cyber security events are properly identified, reviewed, reported, and resolved on time.

OIG Reply: OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that DS has amended the Computer Incident Response Team Standard Operating Procedures to provide management oversight responsibility to the Office of Cybersecurity and specifies that responsible supervisory personnel must follow established categorization guidelines, reporting requirements, and remediation timelines in accordance with the Department's cyber security incident response and reporting policies and procedures.

RECOMMENDATIONS

Recommendation 1: OIG recommends that the Bureau of Diplomatic Security, in conjunction with the Bureau of Information Resource Management, finalize and implement the Joint Cyber Security Concept of Operations Memorandum of Understanding.

Recommendation 2: OIG recommends that the Bureau of Diplomatic Security (DS) amend the Computer Incident Response Team Standard Operating Procedures to provide management oversight responsibility to the Office of Cybersecurity. Specifically, DS should ensure that responsible supervisory personnel follow established categorization guidelines, reporting requirements, and remediation timelines in accordance with the Department of State's cyber security incident response and reporting policies and procedures.

APPENDIX A: DEPARTMENT OF STATE RESPONSIBILITIES AND FUNCTIONS FOR INCIDENT RESPONSE AND REPORTING

To secure and protect the confidentiality, integrity, and availability of the Department of State's (Department) networks, information systems, and data, the Department's incident response mission requires effective coordination between the Bureau of Diplomatic Security (DS) and the Bureau of Information Resource Management (IRM).

Table A.1 provides a high-level view of the Department's incident response responsibilities that are dispersed between DS's and IRM's offices and divisions.

Table A.1: Department Responsibilities for Incident Response and Reporting

Department of State Bureau/Directorate/ Office	Incident Response Governance and Strategy	Incident Response Management and Processes	Incident Response Operational Practices
DS	X		
DS/DSS	X		
DS/SI	X		
DS/SI/IS		X	X
DS/SI/CS		X	X
DS/CS/MIR		X	X
DS/CS/CTA		X	X
DS/CS/ESS		X	X
CIO	X		
IRM/IA/CISO	X	X	X
IRM/OPS	X	X	X
IRM/OPS/ITI/SI/IIB		X	X
IRM/OPS/ENM		X	X
IRM/OPS/ENM/NED		X	X
IRM/OPS/ENM/OPS		X	X

Source: Foreign Affairs Manual, Vol. 1, "Organization and Functions"; Foreign Affairs Manual, Vol. 5, "Information Management"; and Foreign Affairs Manual, Vol. 12, "Diplomatic Security."

Bureau of Diplomatic Security

The Department assigned DS responsibility for administering the Cyber Security Incident Program in order to comply with the Federal Information Security Management Act of 2002 as amended. Specifically, DS provides the following:

- Network Monitoring
- Cyber Incident Handling
- Cyber Threat Analysis
- Compliance Verification and Vulnerability Analysis
- Cyber Security Policy and Configuration Development
- Cyber Security Awareness and Training

- Regional Computer Security Officer program

The Principal Deputy Assistant Secretary for DS and the Director of the Diplomatic Security Service provide direct management oversight of the DS Security Infrastructure (DS/SI) directorate. The Senior Coordinator for DS/SI manages all matters relating to security infrastructure in the DS functional areas of information security and cyber security. The Office of Information Security is responsible for the Department's information protection programs. The Office of Information Security administers the Department's Cyber Security Incident Program and the Security Incident Program.

The Office of Cybersecurity

The Office of Cybersecurity comprises the Monitoring and Incident Response Division, the Cyber Threat Analysis Division, the Enterprise Security Services Division, and the Cybersecurity Policy and Awareness Program. The responsibilities of the Office of Cybersecurity are as follows:

- Direct, manage, and maintain the Department's overall capacity for network intrusion detection, monitoring, incident handling and response, and cyber threat analysis relating to the Department's secret collateral and below systems.
- Research, develop, and maintain security configuration standards and principles for Departmental implementation of IT hardware and applications.
- Develop and maintain a cyber-threat analysis and reporting capability to support Department-level threat determinations and subsequent vulnerability mitigation.
- Develop, in conjunction with IRM's Office of the Deputy Chief Information Officer (Deputy CIO) for Operations (IRM/OPS), cyber security procedures for operational elements.
- Maintain and operate, in coordination with IRM, key components of the Department's Situational Awareness Program, including input from continuous scanning, advanced threat monitoring and analysis, site scoring, and the Regional Cybersecurity Officers.
- Ensure compliance with the Department's information security program requirements in coordination with the CIO, the Chief Information Security Officer (CISO), and IRM/OPS.

The Monitoring and Incident Response Division

The Monitoring and Incident Response Division is to maintain a comprehensive layered defense-in-depth cyber security program to do the following:

- Monitor and audit information systems.
- Detect inappropriate, malicious, or anomalous activity.
- Warn and alert of possible unauthorized access.
- Monitor Department host information systems and networks to detect vulnerabilities and inappropriate, incorrect, malicious, unauthorized, or anomalous activity and respond to security-related incidents.
- Monitor continuously for vulnerabilities and configuration compliance of hardware and software.

The Cyber Threat Analysis Division

The Cyber Threat Analysis Division is to do the following:

- Conduct malware analysis and network intrusion forensics on Department hardware drives and mobile computing devices.
- Identify network vulnerabilities through advanced analyses addressing system assets.

Enterprise Security Services Division

The Enterprise Security Services Division is to do the following:

- Develop and maintain security configuration standards and principles for IT hardware, operating systems, and applications.
- Conduct detailed security and safeguards analyses of software and IT systems and update related policy, standards, and guidelines as necessary.
- Provide collaborative, consultative assistance within the Office of Cybersecurity (DS/SI/CS) for inquiries regarding security of Department IT systems.
- Conduct risk assessments and identify mitigation strategies to safeguard the Department's IT infrastructure and systems.
- Provide specialized security tools to the Foreign Affairs Cybersecurity Center to detect, deter, and prevent cyber attacks against the Department's networks.

Bureau of Information Resource Management

IRM, under the direction of the CIO, is responsible for ensuring the availability of information technology systems and operations. Specifically, the CIO's incident response and reporting responsibilities are as follows:

- Establish information resource management policies, plans, and programs.
- Oversee specific operations to ensure that the Department's information resource management, information systems, and information technology are designed, acquired, operated, maintained, monitored, and evaluated for compliance with all applicable governance mandates and requirements.
- Coordinate with DS to support the efficient, cost-effective, and timely achievement of strategic Department missions for security and configuration management.

The key divisions and offices within IRM that are responsible for core processes and operational practices critical to the Department's incident response mission include the following:

- Office of Information Assurance/CISO (IRM/IA)
- Deputy CIO for Operations/Chief Technology Officer (IRM/OPS)
- Information Integrity Branch
- Enterprise Network Management Office (IRM/OPS/ENM)
- Network Engineering and Design Division
- Operations Division (IRM/OPS/ENM/OPS)

Office of Information Assurance/CISO (IRM/IA)

The Department's CISO is to do the following:

- Lead the Office of Information Assurance (IRM/IA) to ensure the Department's compliance with the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014, and other applicable national requirements and mandates.
- Serve as co-chair of the Department's Information Security Steering Committee.

The CISO is charged with developing and maintaining a Department-wide information security program as required by the United States Code, 44 U.S.C 3544(b), that includes procedures for detecting, reporting, and responding to security incidents. Security incident procedures developed by the CISO ensure the following:

- Risks associated with security incidents are mitigated before substantial damage is done.
- The U.S. Computer Emergency Readiness Team is notified and consulted.
- Law enforcement agencies and other offices, including the relevant OIG, are notified and consulted when national security systems are involved.

The Deputy CIO for Operations/Chief Technology Officer (IRM/OPS)

IRM/OPS is to do the following:

- Provide the overall liaison, interface, and outreach functions within the Department to supply the information resources management operations necessary to support the Department's mission and functions.
- Provide direction and policy guidance on substantive operational activities in IRM to ensure that the Department receives reliable, responsive, and secure data information management operating systems, networks, and programs.
- Provide enterprise-wide business systems, system integration, mainframes, and client/server operations.
- Account for the management and overall security of the classified and unclassified mainframe systems.

Information Integrity Branch

The Information Integrity Branch implements information systems security policies, standards, and procedures that conform to Department regulations. Specifically, the Information Integrity Branch is to do the following:

- Implement policies, standards, and procedures regarding information systems security that conform to Department regulations.
- Manage the Department's Mainframe Security Program to ensure compliance with Department security policies and industry best practices.
- Develop, implement, and administer policies, standards, and procedures regarding mainframe security including security event monitoring and auditing.

- Monitor and provide advice, as appropriate, on the installation and operation of mainframe interfaces with the OpenNet, Internet, or dedicated interagency communication links.
- Serve as a first-level Computer Incident Response Team for security incidents originating on any mainframe platform or at the mainframe's boundary interfaces.
- Conduct real-time security event monitoring and mainframe network intrusion detection.
- Manage and coordinate the mainframe application Information System Security Officer program in cooperation with CIO/IA and DS.
- Advise on all mainframe security relevant policies and coordinate intra-agency and inter-agency computer security issues.
- Implement anti-virus policies, standards, and procedures to conform to established Department of State architecture to ensure effective and efficient operations that protect critical automated information systems against the threat of malicious code virus infection.
- Manage a Virus Incident Response Team capable of responding to virus alerts Department-wide.
- Develop policy that mandates reporting virus discoveries to the Information Technology Branch.

Enterprise Network Management Office (IRM/OPS/ENM)

IRM/OPS/ENM is responsible for managing and overseeing the design, operation, and life-cycle management of the Department's worldwide networks. The Network Engineering and Design Division and the Operations Division have key roles in supporting the Department's incident response mission.

Network Engineering and Design Division

The Network Engineering and Design Division is to do the following:

- Validate applications to run on the Department's network.
- Support the IRM Customer Center in consolidating wide-area network and operating system requirements.
- Oversee the development, implementation, and maintenance of the Integrated Enterprise Management System, which includes proactive network monitoring, problem resolutions, escalation, troubleshooting, and trouble-ticketing.

Operations Division (IRM/OPS/ENM/OPS)

OPS is to do the following:

- Oversee and provide 24-hour management and administrative support for the Department's networks.
- Ensure the reliable operations and performance of classified/unclassified Internet-working systems and network services.
- Provide operational, administrative, and management support for the worldwide internet protocol network through the Department's Enterprise Network Management Operations Center.
- Provide operational support for the Department's server and client operating systems.
- Provide technical support and coordination for detecting and correcting IT security vulnerabilities.

APPENDIX B: U.S. COMPUTER EMERGENCY RESPONSE TEAM INCIDENT CATEGORIES, TYPES, AND REPORTING TIMES

Table B.1: U.S. Computer Emergency Readiness Team Incident Categories,* Types, and Reporting Items

Incident Category (CAT)	Incident Type	Examples of Incident Types	U.S. Computer Emergency Readiness Team Reporting Time
CAT 0	Exercise or Network Defense Testing	- Test incident response and reporting capabilities for a distributed attack	Not applicable; this category is for internal use during exercises.
CAT 1	Unauthorized Access	-Attempted access -Unauthorized hardware connected to network -Website defacement	Within one (1) hour of discovery or detection.
CAT 2	Denial of Service	-Distributed attack	Within two (2) hours of discovery or detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	-Malicious email payload. -Confirmed malicious code on machine	Daily or within one (1) hour of discovery/detection if widespread across agency.
CAT 4	Improper Usage	-Classified spillage -Policy violation	Weekly.
CAT 5	Scans, Probes, and Attempted Access	-Attempted access -Probe/Scan	Monthly or within one (1) hour of discovery if system is classified.
CAT 6	Investigation	-Personally Identifiable Information	Not applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

*U.S. Computer Emergency Readiness Team, <https://www.us-cert.gov/government-users/reporting-requirements>, accessed on October 12, 2015.

Source: U.S. Computer Emergency Readiness Team.

APPENDIX C: EVALUATION SCOPE AND METHODOLOGY

The Bureau of Diplomatic Security provided a total population of 3,731 Remedy[1] cyber security incident tickets for the period August 1 through December 31, 2014. Williams, Adley & Company, DC-LLP (Williams, Adley), reduced the total population by selecting cyber security incidents that occurred during the months of September and October 2014. A total of 1,395 cyber security incidents remained in the population. Of those 1,395 cyber security incident tickets, Williams, Adley determined that 1,092[2] cyber-security incidents were categorized as having a low priority and were removed from the population. From the remaining 303 cyber security incidents, Williams, Adley judgmentally selected 25 cyber security incident tickets from categories (CAT) 1 through 6, focusing mainly on incidents that had higher impact levels (CATs 1 and 2). Accordingly, Williams, Adley selected all CAT 1 and CAT 2 incidents. Williams, Adley then judgmentally sampled incidents for the remaining categories (CAT 3 to 6) in order to increase visibility for all types of incidents. Williams, Adley relied on information captured in the cyber security incident details by the Bureau of Diplomatic Security to determine associated impact levels beyond incident category. Additional details are provided in Table C.1.

Table C.1: Category and Incident Types Included in Judgmental Sample

Incident Category	Incident Type	Details Noted by the Computer Incident Response Team	Population Size	Sample Size
CAT 1	Unauthorized Access	-Attempted access -Unauthorized hardware connected to network -Website defacement	3	3
CAT 2	Denial of Service	-Distributed attack	2	2
CAT 3	Malicious Code	-Malicious email payload -Confirmed malicious code on machine	175	11
CAT 4	Improper Usage	-Classified spillage -Policy violation	73	2
CAT 5	Scans, Probes, and Attempted Access	-Attempted access -Probe/scan	18	3
CAT 6	Investigation	-Personally identifiable information -Social media reported to Office of Innovative Engagement	32	4
TOTAL			303	25

Source: Bureau of Diplomatic Security.

[1] **(U)** Remedy is the Department of State's cyber security incident tracking system.
[2] **(U)** Williams, Adley determined that 1,090 of the 1,092 incidents were "non-incidents." For example, one was a CAT 0 Exercise/Network Defense Testing incident, and one was canceled.

APPENDIX D: BUREAUS OF INFORMATION RESOURCE MANAGEMENT AND DIPLOMATIC SECURITY RESPONSES

United States Department of State

Washington, D.C. 20520

~~SENSITIVE BUT UNCLASSIFIED~~

January 15, 2016

INFORMATION MEMO FOR NORMAN P. BROWN, AIG FOR AUDITS (OIG)

FROM: IRM – Frontis B. Wiggins, Acting
DS – Gregory B. Starr /s/

SUBJECT: ~~(SBU)~~ Response to "Management Assistant Report: Department of State Incident and Response Reporting Program"

Thank you for the opportunity to review and comment on the aforementioned draft report. This joint memo includes DS responses for the two assigned recommendations and changes to the report that IRM recommends.

As noted in our November 6, 2015 response to the "Draft Report for Audit of the Department of State Information Security Program," we continue to have concern with the use of a press article on page seven to support a claim that the Department's November 2014 OpenNet outage was a result of a nation-state's actions. The article has broken links to the source material cited, uses the word "reportedly" often, and does not seem to meet the Government Auditing Standards (Yellow Book) for "Obtaining Sufficient, Appropriate Evidence" for supporting such a claim. The paragraph in question uses the article to support that the Department's OpenNet system was taken off-line due to a cyberincident. In lieu of the source used, IRM suggests citing from the attached Department Notice instead.

We appreciate your consideration of our concerns. Please contact Cristen L. Oehrig for questions regarding the recommendations or Jameela R. Akbari for questions related to the requested changes to the report text.

Attachment:
Tab 1 – DS responses to Recommendations 1 and 2
Tab 2 – Department Notice, Message from the CIO on the Recent Outage

~~SENSITIVE BUT UNCLASSIFIED~~

SENSITIVE BUT UNCLASSIFIED

Tab 1 -- Draft Management Assistance Report: Department of State Incident Response and Reporting Program, December 2015

Recommendation 1: (U) OIG recommends that the Bureau of Diplomatic Security, in conjunction with the Bureau of Information Resource Management, finalize and implement the Joint Cyber Security Concept of Operations Memorandum of Understanding.

DS Response: (SBU) DS requests this recommendation be closed as the Office of the Chief Information Officer (IRM) and the Bureau of Diplomatic Security (DS) have finalized and signed the Memorandum of Understanding, establishing the Department's Joint Security Operations Center (JSOC).

SENSITIVE BUT UNCLASSIFIED

~~SENSITIVE BUT UNCLASSIFIED~~

Recommendation 2: (U) OIG recommends that the Bureau of Diplomatic Security amend the Computer Incident Response Team Standard Operating Procedures to provide management oversight responsibility to the Office of Cybersecurity. Specifically, DS should ensure that responsible supervisory personnel follow established categorization guidelines, reporting requirements, and remediation timelines, in accordance with the Department of State's cyber security incident response and reporting policies and procedures.

DS Response: ~~(SBU)~~ DS requests this recommendation be closed as evidenced by these recent enhancements to the Department's cyber incident response program capabilities:

- The establishment of the Joint Security Operations Center (JSOC), which is designed to further mature the Department's ability to identify, react, respond to, and mitigate cyber threats and vulnerabilities.

- The hiring and placement of additional Senior Watch Officers (SWO's) to the DS CIRT, which will ensure the 24/7 presence of supervisory personnel to direct and manage incident response program activities, including proper identification, categorization, and reporting of security events in accordance with Department policies and the newly revised US-CERT reporting guidelines.

- Moreover, the DS CIRT currently performs an annual review of its standard operating procedures, under the direction of the Office of Cybersecurity (DS/SI/CS), to ensure that cyber security events are properly identified, reviewed, reported, and resolved on time.

~~SENSITIVE BUT UNCLASSIFIED~~

UNCLASSIFIED

Tab 2

United States Department of State Department Notice; http://mmsweb.a.state.gov/asp/notices/dn_temp.asp?Notice_Id=22564; Accessed on January 4, 2016

Office of Origin: IRM/CIO
Announcement Number: 2014_11_186
Date of Announcement: November 24, 2014

Message from the CIO on the Recent Outage

The news is filled with reports of cyber attacks and, like any large organization with a global presence, the Department of State is and will continue to be a target for malicious attacks. The Bureaus of Information Resource Management and Diplomatic Security closely monitor cyber activity on our networks, and our computer security teams respond to thousands of incidents each month.

The majority of these intrusion attempts are halted at the network perimeter. However, we have recently seen an uptick in the frequency and sophistication of the attacks. At the heart of the challenge is the need to balance the risk to collaborate with the need to secure critical data. Supporting this balance is most challenging on the unclassified network because of the numerous external connections, including the Internet. If our approach on security is too tight, collaboration comes to a halt, while the other end of the spectrum opens the door to intrusions.

The recent attack on OpenNet called for a carefully constructed response plan in coordination with cybersecurity experts from DHS and other agencies, as well as private sector experts. The outage that began last Friday was part of the Department's remediation strategy, and was executed after a thorough planning process. Any

UNCLASSIFIED

UNCLASSIFIED

earlier notification of the strategy would have alerted the adversary and sunk our remediation efforts.

It appears our efforts are successful, however we are still working to restore remote access via GO. The delays associated with GO stem from the requirement to replace the entire GO infrastructure. We are reviewing other technical restrictions put in place as a part of this strategy.

We cannot overemphasize the importance of following best practices when it comes to cybersecurity, including carefully scrutinizing hyperlinks in emails and reporting any suspicious activity immediately to your Information System Security Officer and Regional Security Officer.

We all have a role to play in protecting our systems. Thank you for your continued commitment.

◄ Return to Department Notices index

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