



OIG

Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

AUD-IT-IB-16-25

Office of Audits

January 2016

Management Assistance Report: Broadcasting Board of Governors Incident Response and Reporting

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

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 (hereinafter referred to as Williams, Adley), an independent public accounting firm, evaluated the effectiveness of the Broadcasting Board of Governors (BBG) IR&R program for the period October 1, 2014, through May 26, 2015, in accordance with BBG information security policies and procedures, Federal law, and applicable standards and guidelines.

Overall, Williams, Adley determined that BBG's IR&R program was not operating effectively. Specifically, for all seven cyber security incidents reported to BBG's incident response team, the Computer Security Incident Response Team (CSIRT), during the scope period, BBG's incident response team did not fully comply with categorization guidelines, reporting requirements, and remediation timelines as required by the U.S. Computer Emergency Readiness Team (US-CERT). Williams, Adley determined that one cyber security event was not properly categorized as a cyber security incident. In addition, category levels were not assigned to any of the seven cyber security incidents tested. Furthermore, two cyber security incidents were not reported to US-CERT as required, and another cyber security incident was not reported to US-CERT in a timely manner.

These deficiencies may have occurred in the IR&R program because BBG's IR&R policy and procedures were not finalized until May 7, 2015. However, Williams, Adley found that even if the policy and procedures had been implemented during the evaluation period, the documents were ineffective in achieving the desired and Federally required results of an effective IR&R program. For example, BBG's policy and procedures lacked a defined process to correlate IT events and cyber security incidents.

Without an effective IR&R program, BBG may be unable to properly identify and respond to unauthorized breaches, identify weaknesses, and restore IT operations timely, which may impede BBG's ability to achieve its core mission.

In its response (see Appendix B) to a draft of this report, BBG concurred with OIG's recommendation to amend and implement BBG's IR&R policy and procedures. OIG considers the recommendation resolved, pending further action. BBG's response to the recommendation and OIG's reply are presented after the recommendation.

OBJECTIVE

OIG's Office of Audits (AUD) contracted with Williams, Adley, an independent public accounting firm, to evaluate the effectiveness of BBG's IR&R program for the period October 1, 2014, through May 26, 2015, in accordance with Federal requirements.

BACKGROUND

BBG is an independent Federal agency that supervises all U.S. civilian international broadcasting. BBG broadcasters distribute programming in 61 languages to an estimated weekly audience of 215 million people via radio, television, the Internet, and other news media. BBG works to serve as an example of a free and professional press, reaching a worldwide audience with news, information, and relevant discussions. The International Broadcasting Bureau, a significant component of BBG, maintains the global distribution network over which all BBG-funded news and information programming is distributed. The International Broadcasting Bureau also performs administrative functions such as financial management, human resources, and IT support. For example, BBG's Chief Information Officer is part of the International Broadcasting Bureau. The BBG Chief Information Officer has overall responsibility for managing the information security program.

Cyber Security Trends

In April 2014, the Government Accountability Office (GAO) reported¹ 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 cyber attacks that have been successful and to allow agencies to make risk-based decisions about where it is most cost effective to focus security resources. A well-defined incident response capability helps an agency to 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.

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).

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 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 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 categories³ 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 A.

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 are 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.

BBG's Computer Security Incident Response Policy and Procedures

In an attempt to comply with Federal requirements, BBG's Office of Technology, Services, and Innovation (TSI) developed the Computer Security Incident Response Policy⁶ and Computer Security Incident Response Procedure⁷ in May 2015. According to these documents, BBG's IR&R

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 TSI, Computer Security Incident Response Policy, May 7, 2015.

⁷ Ibid.

process begins when a BBG employee or contractor reports an event to the TSI Help Desk or when a computer security incident is detected via BBG's computer security monitoring tools. Personnel at the TSI Help Desk then review the reported event to determine whether it is a cyber security incident. When TSI Help Desk personnel determine that a cyber security incident occurred, they report the cyber security incident to BBG's incident response team, CSIRT, which then determines the validity, scope, and severity of the cyber security incident. The cyber security incident is then prioritized, entered into BBG's cyber security incident tracking system (Redmine), assigned a category based on US-CERT's incident-type classifications (see Appendix A), and subsequently submitted to US-CERT within the designated timeframe based on the incident-type classification.

RESULTS

Williams, Adley determined that BBG's IR&R program was not operating effectively for the period October 1, 2014, through May 26, 2015. BBG's IR&R process did not comply with US-CERT requirements. Specifically, Williams, Adley reviewed BBG's handling of all seven cyber security incidents and one judgmentally selected cyber security event that were reported to CSIRT during the scope period to determine whether BBG complied with Federal requirements.

According to NIST,⁸ 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. BBG classifies cyber security incidents as "those adverse events in which automated intrusion detection systems fail to detect, contain, and eradicate the incident, and exhibit that the confidentiality, integrity, or availability of a Federal Government information system is compromised."⁹ Williams, Adley found that the one judgmentally selected cyber security event reported to CSIRT during the scope period was not properly categorized as a cyber security incident. Specifically, the event was a compromised workstation, which, according to US-CERT,¹⁰ should have been recorded as an incident.

US-CERT¹¹ requires that a category level (between zero and six) be designated for all cyber security incidents to determine the reporting timeframe to US-CERT. However, Williams, Adley found that BBG did not assign category levels for any of the seven cyber security incidents tested.

US-CERT¹² requires that agencies report incidents to US-CERT based on timeframes designated by an incident's specific category level. However, Williams, Adley found two cyber security incidents that were not reported to US-CERT and a third that was not reported to US-CERT in a timely manner. Specifically, one cyber security incident involved two unidentified hosts, while

⁸ NIST 800-61, rev. 2.

⁹ TSI, Computer Security Incident Response Policy.

¹⁰ US-CERT, <<https://www.us-cert.gov/government-users/reporting-requirements>>.

¹¹ Ibid.

¹² Ibid.

the second incident involved a compromised host. Both cyber security incidents involved unauthorized access and should have been reported to US-CERT. The third cyber security incident involved a compromised demilitarized zone,¹³ which should have been reported to US-CERT within one hour of discovery; however, CSIRT reported the incident to US-CERT the following day.

BBG's IR&R program was not operating effectively for the period October 1, 2014, through May 26, 2015, because BBG's official IR&R policy and procedures, which established and governed the IR&R program, were not finalized until May 7, 2015. However, even if the policies and procedures had been in place, the deficiencies would most likely have persisted. Williams, Adley reviewed the finalized policy and procedures and determined that they did not align with US-CERT and NIST guidance. Specifically, as required by NIST 800-61, Revision 2, when handling an incident, BBG should compile the following information to ensure appropriate preparation:

- Incident handler communication and facilities list.
- Incident analysis resources list.
- Information regarding mitigation software.

However, these requirements were not included in the policy and procedures. In addition, BBG did not include other essential processes in the policy and procedures, including risk assessment, host security, network security, malware prevention, and user awareness and training. Further, BBG did not include details on the following methods of attack in its incident handling procedures: external and removable media, attrition, web, email, impersonation, improper usage, and equipment loss/theft. In addition, BBG did not incorporate other vital information in its incident handling procedures regarding precursors and indicators such as a process for event correlation, evidence retention, and an incident handling checklist.

Impact

BBG depends on information systems and electronic data to carry out essential mission-related functions. Thus the security of these systems and networks is vital to allow broadcasters to distribute programming effectively to their worldwide audience. As an organization with international exposure, BBG's information systems are subject to serious threats that can have adverse effects on organizational operations, assets, and individuals. Exploiting both known and unknown vulnerabilities may compromise the confidentiality, integrity, or availability of information being processed, stored, and transmitted by BBG systems.

Without an effective IR&R program, BBG may be unable to properly identify and respond to unauthorized breaches while minimizing loss and destruction and restoring IT operations quickly,

¹³ NIST Interagency Report 7298, rev. 2, "Glossary of Key Information Security Terms," May 2013, states that a demilitarized zone is a host or network segment inserted as a neutral zone between an organization's private network and the Internet. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

which would adversely impact BBG's overall business mission. For example, according to a BBG press release,¹⁴ BBG websites were hacked in 2011, which resulted in the redirection of website traffic.

In addition, without effective IR&R policies, BBG personnel may not be able to implement cyber security incident handling and reporting requirements necessary to determine the kinds of attacks that have been successful or make risk-based decisions about where it is most cost effective to focus BBG's security resources. Furthermore, without following these requirements, US-CERT would not be able to assist BBG in responding to cyber security incidents or disseminate timely notifications to other Federal agencies regarding current and potential security threats and vulnerabilities.

CONCLUSION

Williams, Adley determined that BBG's IR&R program was not operating effectively. Specifically, for the seven cyber security incidents evaluated, CSIRT personnel did not fully comply with categorization guidelines, reporting requirements, and remediation timelines as required by US-CERT. This occurred primarily because BBG's IR&R policy and procedures were not finalized until May 7, 2015. Williams, Adley reviewed the finalized policy and procedures and determined that even if implemented during the evaluation period, the IR&R policy and procedures were not aligned with US-CERT and NIST guidance and therefore would not be effective in achieving the desired and Federally required functions of an effective IR&R program. An effective IR&R program is critical for ensuring the security and protection of BBG's networks, information systems, and data.

Recommendation 1: OIG recommends that the Broadcasting Board of Governors Office of Technology, Services, and Innovation amend and implement the Computer Security Incident Response Policy and the Computer Security Incident Response Procedure to reflect all elements of an effective incident response and reporting program in accordance with National Institute of Standards and Technology Special Publication 800-61, Revision 2.

Management Response: BBG concurred with OIG's recommendation, stating that it will "review NIST's incident response guidance for additional elements." BBG further stated that it will "update its policy and procedures to comply with the current US-CERT Incident Notification Guidelines . . . that emphasize the consideration of the impact of an event on [BBG's] mission and information confidentiality, integrity, and availability."

OIG Reply: Because BBG agreed to implement the recommendation, OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the Office of Technology,

¹⁴ BBG, <<http://www.bbg.gov/blog/2011/02/22/hacking-and-signal-interference-of-u-s-international-broadcasting/>>, accessed on November 20, 2015.

Services, and Innovation has amended and implemented the Computer Security Incident Response Policy and the Computer Security Incident Response Procedure to reflect all elements of an effective incident response and reporting program in accordance with NIST SP 800-61, Revision 2.

RECOMMENDATIONS

Recommendation 1: OIG recommends that the Broadcasting Board of Governors Office of Technology, Services, and Innovation amend and implement the Computer Security Incident Response Policy and the Computer Security Incident Response Procedure to reflect all elements of an effective incident response and reporting program in accordance with National Institute of Standards and Technology Special Publication 800-61, Revision 2.

APPENDIX A: U.S. COMPUTER EMERGENCY READINESS TEAM INCIDENT CATEGORIES, TYPES, AND REPORTING TIMES

Table A.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 -Social media reported to the Office of Innovative Engagement	Not applicable; this category is for use to categorize a potential incident that is currently being investigated.

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

APPENDIX B: BROADCASTING BOARD OF GOVERNORS RESPONSE



BROADCASTING BOARD OF GOVERNORS
UNITED STATES OF AMERICA

January 7, 2016

Mr. Norman P. Brown
Assistant Inspector General for Audits
Office of Inspector General
U.S. Department of State

Dear Mr. Brown:

Thank you for the opportunity to comment on the draft report management *Assistance Report: Broadcasting Board of Governors Incident Response and Reporting*.

The Agency concurs with the report's recommendation that the Office of Technology, Services, and Innovation amend and implement the Computer Security Incident Response Policy and the Computer Security Incident Response Procedure to reflect all elements of an effective incident response and reporting program in accordance with National Institute of Standards and Technology Special Publication 800-61, Revision 2.

The Agency will review NIST's incident response guidance for additional elements which, if incorporated, would improve the Agency's Computer Security Incident Response Policy and Procedures. In addition, the Agency will update its policy and procedures to comply with the current US-CERT Incident Notification Guidelines (<https://www.us-cert.gov/incident-notification-guidelines>) that emphasize the consideration of the impact of an event on the Agency mission and information confidentiality, integrity, and availability.

Please do not hesitate to contact us should you have any questions.

Sincerely,

A handwritten signature in blue ink that reads "John F. Lansing".

John F. Lansing
Chief Executive Officer and Director

UNCLASSIFIED



HELP FIGHT
FRAUD. WASTE. ABUSE.

1-800-409-9926
[OIG.state.gov/HOTLINE](https://oig.state.gov/HOTLINE)

If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:

OIGWPEAOmbuds@state.gov

oig.state.gov

Office of Inspector General • U.S. Department of State • P.O. Box 9778 • Arlington, VA 22219

UNCLASSIFIED