United States Government Accountability Office

Report to Congressional Requesters

April 2014

INFORMATION SECURITY

Agencies Need to Improve Cyber Incident Response Practices

GAO Highlights

Highlights of GAO-14-354, a report to congressional requesters

April 2014

INFORMATION SECURITY

Agencies Need to Improve Cyber Incident Response Practices

Why GAO Did This Study

The number of cyber incidents reported by federal agencies increased in fiscal year 2013 significantly over the prior 3 years (see figure). An effective response to a cyber incident is essential to minimize any damage that might be caused. DHS and US-CERT have a role in helping agencies detect, report, and respond to cyber incidents.

GAO was asked to review federal agencies' ability to respond to cyber incidents. To do this, GAO reviewed the extent to which (1) federal agencies are effectively responding to cyber incidents and (2) DHS is providing cybersecurity incident assistance to agencies. To do this, GAO used a statistical sample of cyber incidents reported in fiscal year 2012 to project whether 24 major federal agencies demonstrated effective response activities. In addition, GAO evaluated incident response policies, plans, and procedures at 6 randomly-selected federal agencies to determine adherence to federal guidance. GAO also examined DHS and US-CERT policies, procedures, and practices, and surveyed officials from the 24 federal agencies on their experience receiving incident assistance from DHS.

What GAO Recommends

GAO is making recommendations to OMB and DHS to address incident response practices governmentwide, particularly in CyberStat meetings with agencies; to the heads of six agencies to strengthen their incident response policies, plans, and procedures; and to DHS to establish measures of effectiveness for the assistance US-CERT provides to agencies. The agencies generally concurred with GAO's recommendations.

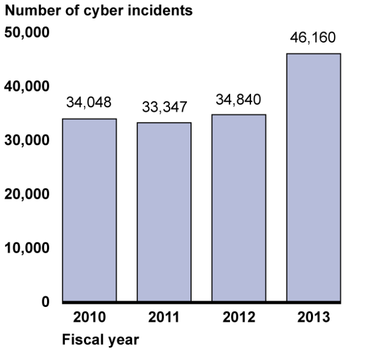
View GAO-14-354. For more information, contact Gregory C.Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Twenty-four major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information). Based on a statistical sample of cyber incidents reported in fiscal year 2012, GAO projects that these agencies did not completely document actions taken in response to detected incidents in about 65 percent of cases (with 95 percent confidence that the estimate falls between 58 and 72 percent). For example, agencies identified the scope of an incident in the majority of cases, but frequently did not demonstrate that they had determined the impact of an incident. In addition, agencies did not consistently demonstrate how they had handled other key activities, such as whether preventive actions to prevent the reoccurrence of an incident were taken. Although all 6 selected agencies that GAO reviewed in depth had developed parts of policies, plans, and procedures to guide their incident response activities, their efforts were not comprehensive or fully consistent with federal requirements. In addition, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) conduct CyberStat reviews, which are intended to help federal agencies improve their information security posture, but the reviews have not addressed agencies' cyber incident response practices. Without complete policies, plans, and procedures, along with appropriate oversight of response activities, agencies face reduced assurance that they can effectively respond to cyber incidents.

DHS and a component, the United States Computer Emergency Readiness Team (US-CERT), offer services that assist agencies in preparing to handle cyber incidents, maintain awareness of the current threat environment, and deal with ongoing incidents. Officials from the 24 agencies GAO surveyed said that they were generally satisfied with the assistance provided, and made suggestions to make the services more useful, such as improving reporting requirements. Although US-CERT receives feedback from agencies to improve its services, it has not yet developed performance measures for evaluating the effectiveness of the assistance it provides to agencies. Without results-oriented performance measures, US-CERT will face challenges in ensuring it is effectively assisting federal agencies with preparing for and responding to cyber incidents.

Cyber Incidents Reported by All Federal Agencies to US-CERT, Fiscal Years 2010-2013



Source: GAO analysis of US-CERT data for fiscal years 2010-2013.

Contents

Tables

Figures

Abbreviations

DHS	Department of Homeland Security
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
FISMA	Federal Information Security Management Act of 2002
FNR	Federal Network Resilience
HUD	Housing and Urban Development
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
SP	special publication
US-CERT	United States Computer Emergency Readiness Team
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 30 2014

The Honorable Thomas R. Carper
Chairman
The Honorable Tom Coburn, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan M. Collins
United States Senate

Cyber-based attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive. Protecting the information systems and the information that resides on them and effectively responding to a cyber incident[1] is important to federal agencies because the unauthorized disclosure, alteration, and destruction of the information on those systems can result in great harm to those involved.

According to the National Institute of Standards and Technology (NIST),[2] preventive activities developed from the results of a risk assessment can help federal agencies and other entities to deter known cybersecurity[3] threats and to respond to them quickly. Having policies, plans, and procedures in place to guide agencies in responding to a cyber incident is critically important to minimizing loss and destruction, mitigating the weaknesses that have been exploited, and restoring IT services.

[1] A cyber incident is a security breach of a computerized system and information and, for the purposes of this report, has the same meaning as a computer security incident, which the National Institute of Standards and Technology defines as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. The terms information security and information security incident apply more broadly to any forms of information and systems.

[2] NIST provides technical leadership for the nation's measurement and standards infrastructure, including the development of management, administrative, technical, and physical standards for the security of information in federal information systems. NIST's 800-series of Special Publications focuses on research, guidelines, and outreach efforts in information system security.

[3] As used in this report, cybersecurity refers to the security of computerized information systems and the information maintained in them.

The *Federal Information Security Management Act of 2002* (FISMA)[4] requires agencies to develop, document, and implement an information security program. FISMA also authorizes the establishment of a federal information security incident center to assist agencies in handling a cyber incident. The Office of Management and Budget (OMB) has transferred certain information security responsibilities to the Department of Homeland Security (DHS).[5] Further, one of DHS's components, the United States Computer Emergency Readiness Team (US-CERT) operates the federal information security incident center required under FISMA.

You asked us to review federal agencies' ability to respond to cyber incidents. Our objectives were to evaluate the extent to which (1) federal agencies are effectively responding to cyber incidents and (2) the Department of Homeland Security provides cyber incident assistance to agencies.

To evaluate the extent to which federal agencies are effectively responding to cyber incidents, we randomly selected 40 incidents from each of 6 randomly selected[6] agencies: the Departments of Energy (DOE), Justice (DOJ), Housing and Urban Development (HUD), Transportation (DOT), Veterans Affairs (VA), and the National Aeronautics and Space Administration (NASA). We reviewed documentation related to the 240 incidents to determine the extent to which the agencies had performed cyber incident response activities in accordance with federal requirements and guidance and their own policies and procedures. This statistical sample allowed us to project the

[4] Pub. L. No. 107-347, Title III (Dec. 17, 2002).

[5] Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-10-15 (Washington, D.C.: Apr. 21, 2010) and *Memorandum for the Heads of Executive Departments and Agencies*, OMB M-10-28 (Washington, D.C.: July 6, 2010).

[6] We selected 6 agencies from the population of 24 of the major federal agencies covered by the *Chief Financial Officers Act*, used probability proportionate to the number of cyber incidents the agencies had reported to US-CERT in fiscal year 2012, and selected without replacing the agency into the original population.

results, with 95 percent confidence, to the 24 major agencies[7] covered by the *Chief Financial Officers Act*.[8] We also reviewed the 6 selected agencies' incident response policies, plans, and procedures in depth and compared them to federal requirements and guidelines and interviewed officials from the selected agencies regarding their practices for responding to cyber incidents. We also administered a web-based survey to officials at the 24 major federal agencies to gather information about their incident response practices.

To evaluate the extent to which DHS provides cyber incident assistance to agencies, we examined DHS's policies, procedures, and practices. We reviewed agencies' survey responses for information about the type, quality, and usefulness of incident response guidance and services provided by DHS and US-CERT. We also interviewed DHS officials regarding their roles, responsibilities, and actions in assisting agencies in responding to cyber incidents.

We conducted this performance audit from February 2013 to April 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See appendix I for additional details on our scope and methodology.

Background

A cyber incident can occur under many circumstances and for many reasons. It can be inadvertent, such as from the loss of an electronic device, or deliberate, such as from the theft of a device, or a cyber-based attack by a malicious individual or group, agency insiders, foreign nation,

[7] The 24 major departments and agencies covered by the *Chief Financial Officers Act* are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[8] 31 U.S.C. § 901.

terrorist, or other adversary. Incidents have been reported at a wide range of public- and private-sector institutions, including federal, state, and local government agencies; educational institutions; hospitals and medical facilities; financial institutions; information resellers; retailers; and other types of businesses.

Protecting federal systems and the information on them is essential because the loss or unauthorized disclosure or alteration of the information can lead to serious consequences and can result in substantial harm to individuals and the federal government. Specifically, ineffective protection of IT systems and information can result in

- threats to national security, economic well-being, and public health and safety;
- loss or theft of resources, including money and intellectual property;
- inappropriate access to and disclosure, modification, or destruction of sensitive information;
- use of computer resources for unauthorized purposes or to launch an attack on other computer systems;
- damage to networks and equipment;
- loss of public confidence; and
- high costs for remediation.

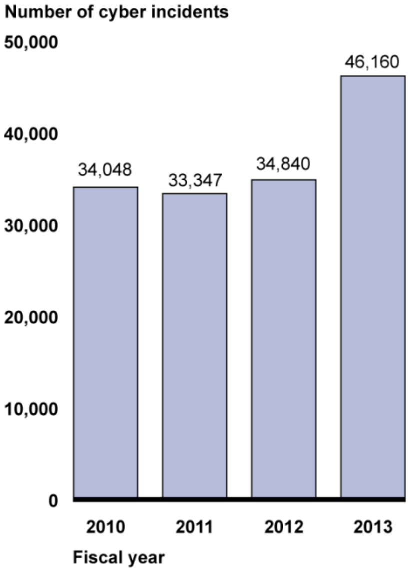
While some cyber incidents can be resolved quickly and at minimal cost, others may go unresolved and incur exorbitant costs.

Thousands of Cyber Incidents Occur at Agencies Each Year

Reported attacks and unintentional incidents involving federal systems such as those involving data loss or theft, computer intrusions, and privacy breaches underscore the importance of having strong security practices in place. In fiscal year 2013, US-CERT received notifications of 46,160 cyber incidents at all agencies and 43,931 incidents at the 24 major agencies.[9] Cyber incidents reported by federal agencies increased in fiscal year 2013 significantly over the prior 3 years (see fig. 1), increasing almost 33 percent in the last 2 fiscal years.

[9] During fiscal year 2013, agencies reported a total of 61,214 incidents to US-CERT, which were comprised of 46,160 cyber incidents and 15,054 non-cyber incidents. According to US-CERT, a “non-cyber” incident is one that involves the mishandling of sensitive information without a cybersecurity component, such as the loss of a hard copy record containing personally identifiable information. Cyber incidents are the focus of this report.

Figure 1: Cyber Incidents Reported to US-CERT by All Federal Agencies: Fiscal Years 2010-2013



Source: GAO analysis of US-CERT data for fiscal years 2010-2013.

The following examples reported in 2013 illustrate that information and assets remain at risk.

- July 2013: Hackers stole a variety of personally identifiable information on more than 104,000 individuals from a Department of Energy system. Types of data stolen included Social Security numbers, birth dates and locations, bank account numbers, and security questions and answers. According to the department's Inspector General, the combined costs of assisting affected individuals and lost productivity—due to federal employees being granted administrative leave to correct issues stemming from the breach—could be more than $3.7 million.[10]
- June 2013: Edward Snowden, an employee of a contractor of the National Security Agency, disclosed classified documents through the media. In January 2014, the Director of National Intelligence testified, in his annual worldwide threat assessment, that insider threats will

[10] Department of Energy, Office of the Inspector General, *The Department of Energy's July 2013 Cyber Security Breach*, DOE/IG-0900 (Washington, D.C.: Dec. 6, 2013).

continue to pose a persistent challenge, as trusted insiders with the intent to do harm can exploit their access to compromise vast amounts of sensitive and classified information as part of a personal ideology or at the direction of a foreign government.[11]

- June 2013: The Office of the Inspector General at the Department of Commerce reported that the department's Economic Development Administration inaccurately identified a common malware infection as a sophisticated cyber attack by another country. To remedy the situation, according to the Office of Inspector General, the Economic Development Administration spent more than $2.7 million—more than half its fiscal year 2012 IT budget—on unnecessary incident response activities and destroyed more than $170,000 worth of IT components officials incorrectly thought to have been irrecoverably infected. The Office of Inspector General reported that a failure to adhere to the department's incident handling procedures, a lack of experienced and qualified incident handlers, and a failure to coordinate incident handling activities all contributed to the mishandling of the incident.[12]
- January 2013: A Romanian national was indicted in U.S. District Court for the Southern District of New York for allegedly running a "bulletproof hosting" service that enabled cyber criminals to distribute malicious software (malware) and conduct other sophisticated cybercrimes. Malware distributed by this hosting service had infected more than 1 million computers worldwide, including computers belonging to the National Aeronautics and Space Administration (NASA), causing tens of millions of dollars in losses to the affected individuals, businesses, and government entities. NASA's Office of Inspector General and the Federal Bureau of Investigation are investigating this incident.[13]

[11] James R. Clapper, Director of National Intelligence, *Statement for the Record - Worldwide Threat Assessment of the US Intelligence Community*, before the Senate Armed Services Committee (Feb. 11, 2014).

[12] Department of Commerce, Office of the Inspector General, *Economic Development Administration: Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted*, OIG-13-027-A (Washington, D.C.: June 26, 2013).

[13] National Aeronautics and Space Administration, Office of Inspector General, *Semiannual Report, October 1, 2012-March 31, 2013* (Washington, D.C.: Apr. 29, 2013).

Federal Law and Policy Establish a Framework for Managing Cyber Risks

FISMA sets up a layered framework for managing cyber risks and assigns specific responsibilities to (1) OMB, including to develop and oversee the implementation of policies, principles, standards, and guidelines for information security; to report, at least annually, on agency compliance with the act; and to approve or disapprove agency information security programs; (2) agency heads, including to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; (3) agency heads and chief information officers, including to develop, document, and implement an agencywide information security program; (4) inspectors general, to conduct annual independent evaluations of agency efforts to effectively implement information security; and (5) NIST, to provide standards and guidance to agencies on information security. Organized, planned cyber incident response activities are essential in defending an information system and the information that resides on it from an accidental or malicious cyber incident.

In addition, FISMA requires the establishment of a federal information security incident center to, among other things, provide timely technical assistance to agencies regarding cyber incidents. Each federal agency must also report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of its information security policies, procedures, practices, and compliance with requirements.

OMB and DHS Provide Oversight and Assistance to Agencies

In 2010, OMB transferred the operational aspects of its FISMA-mandated responsibilities for overseeing and assisting the cybersecurity efforts of federal agencies to DHS. Specifically, according to OMB, DHS activities are to include, but are not limited to:

- overseeing agencies’ cybersecurity operations and incident response and providing appropriate assistance;
- overseeing the governmentwide and agency-specific implementation of and reporting on cybersecurity policies and guidance;
- overseeing and assisting governmentwide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity;
- overseeing agencies’ compliance with FISMA and developing analyses for OMB to assist in the development of the FISMA annual report; and
- annually reviewing agencies’ cybersecurity programs.

Under presidential directive, DHS is also responsible for assisting public- and private-sector critical infrastructure owners and operators in preparing for, preventing, protecting against, mitigating from, responding to, and recovering from a cyber incident.

NIST Has Issued Federal Guidelines for Responding to Incidents

NIST has responsibility for developing standards and guidelines for securing the information systems used or operated by a federal agency or contractor on behalf of an agency. NIST has issued three special publications (SP) that provide guidance to agencies for detecting and handling cyber incidents.

NIST SP 800-61 specifies procedures for implementing FISMA incident handling requirements, and includes guidelines on establishing an effective incident response program and detecting, analyzing, prioritizing, and handling an incident.[14] The specific steps outlined for a formal, focused, and coordinated response to a cyber incident include a plan that should be tailored to meet the unique requirements of the agency and lay out the necessary resources and management support.

The incident response process that NIST outlines has four phases: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. In preparing to respond to incidents, agencies should (1) develop and document policies, plans and procedures for appropriate incident handling guidance; (2) create and train an incident response team; (3) acquire the necessary tools and resources, such as those needed for analyzing incidents; and (4) periodically test their response capability to ensure it is working as intended.

Upon detection of an incident, analysis is needed to determine the incident's scope, such as affected systems, and potential impact to agency operations. These factors assist agencies in prioritizing response activities. In keeping with the severity of the incident, the agency can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts have been infected by malware while eradicating a malware incident. After the

[14] NIST, *Computer Security Incident Handling Guide*, Special Publication 800-61, revision 2 (Gaithersburg, Md.: August 2012).

incident has been managed, the agency may issue a report that details the cause and costs and the steps it should take to prevent a future incident. Policies, plans, procedures, as well as testing and training practices may require updates as lessons are learned throughout the various phases of response.

In addition, NIST SP 800-53 identifies specific incident response control activities that parallel those in NIST SP 800-61 and that agencies should address in order to effectively respond to a cyber incident.[15] These controls include, among others, (1) monitoring incident-handling activities (e.g., tracking and documenting incidents), (2) developing incident response policies and plans, (3) developing incident response procedures, (4) testing an agency's incident response capability, and (5) training incident responders.

NIST also provides guidelines on preventing malware[16] incidents and how agencies should respond to such an incident in an effective and efficient manner.[17]

US-CERT Provides Guidance for Reporting Incidents

Established in 2003, US-CERT is the federal information security incident center mandated by FISMA. US-CERT consults with agencies on cyber incidents, provides technical information about threats and incidents, compiles the information, and publishes it on its website, https://www.us-cert.gov/.

[15] NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 3 with updates as of June 1, 2010 (Gaithersburg, MD.: August 2009). Although NIST released an updated version of SP800-53—NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* in April 2013, we used SP 800-53 revision 3 for this audit. We relied on the previous guidance based on (1) our analysis showing that, while NIST added optional incident response controls and control enhancements in SP 800-53 revision 4, the eight core incident response controls did not change between the two versions and (2) OMB granted agencies a 1-year grace period after publication of new NIST guidance before they must be in compliance with the updated guidance, so the requirements from revision 4 were not yet in effect.

[16] Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim's system.

[17] NIST, *Guide to Malware Incident Prevention and Handling*, Special Publication 800-83 (Gaithersburg, Md.: November 2005).

In addition, US-CERT defines seven categories of incidents for federal agencies to use in reporting an incident. Agencies are required to report incidents to US-CERT within specified time frames, such as within an hour or weekly or monthly, depending on the category of the incident. The categories and their time frames for reporting are listed in table 1.

Table 1: Incident Categories for Federal Agencies and their Reporting Time Frames to US-CERT

Category	Name	Description	Reporting time frame
CAT 0	Exercise/network defense testing	Used during state, federal, national, and international exercises and approved activity testing of internal/external network defenses or responses.	Not applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized access	An individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.	Within one hour of discovery/detection.
CAT 2	Denial of service	An attack that successfully prevents or impairs the normal authorized functionality of a network, system, or application by exhausting resources. Includes being the victim or participating in the denial of service.	Within two hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity.
CAT 3	Malicious code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.	Daily. Note: Within one hour of discovery/detection if widespread across agency.
CAT 4	Improper usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/probes/attempted access	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one hour of discovery.
CAT 6	Investigation	Unconfirmed incident that is potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

Source: US-CERT.

Agencies Did Not Consistently Demonstrate Effective Cyber Incident Response Practices

Based on our statistical sample of cyber incidents reported in fiscal year 2012, we estimate that the 24 agencies did not effectively or consistently demonstrate actions taken in response to a detected incident in about 65 percent of reported incidents.[18] Agencies frequently documented their incident response actions for containing and eradicating incidents, but did not consistently demonstrate how they had handled incident response activities for the analysis, recovery, and post-incident phases. Further, although the 6 selected agencies we reviewed had developed policies, plans, and procedures to guide their incident response activities, such efforts were not comprehensive or consistent with federal requirements.

Agencies Did Not Effectively Demonstrate Some Incident Response Activities

NIST specifies that agencies should document incident response activities, including analysis, containment, eradication, and recovery, as well as post-incident activities.[19] Although we found that agencies documented some required actions, they did not effectively demonstrate others.

Agencies' Demonstrated Aspects of Incident Analyses, but Did Not Complete Others

NIST SP 800-61 specifies that an initial analysis be performed to determine the type, nature, and scope of an incident, such as which networks, systems, or applications have been affected; who or what originated the incident; and what is taking place regarding the incident (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited).

According to NIST SP 800-61, agencies are to consider impact for prioritizing incident response activities, such as the functional impact of the incident—the current and likely future negative impact to business functions. Resource limitations at agencies are one of the factors emphasizing the need for them to prioritize their incident response activities. Further, by prioritizing the handling of incidents, agencies could identify situations of greater severity that demand immediate attention.

[18] Based on our sample, we are 95 percent confident that the estimate falls between 58 percent and 72 percent. This estimate represents the percentage of incident cases where the agency did not complete and/or document incident response activities completed for each of the phases—analysis, containment, eradication, and recovery—where required to do so.

[19] NIST, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-61, Revision 2 (Gaithersburg, Md.: August 2012).

The initial analysis of an incident should identify enough information for the team to prioritize subsequent activities, such as containment of the incident and a deeper analysis of the effects of the incident.

Agencies determined and documented the scope of an incident—a key part of the analysis—for about 91 percent[20] of incidents governmentwide.[21] Examples below illustrate both effective and ineffective scoping practices, such as:

- In a malware incident, the affected agency involved determined that after infecting a computer with malware, an attacker compromised the computer's local administrator account and used those credentials to successfully access another agency computer, which incident handlers then contained and remediated.
- In another incident, an agency received a report from US-CERT indicating that login credentials at two of the agency's components may have been compromised. When contacting the impacted components, agency incident handlers mistyped the potentially compromised credentials for one component and did not respond to an e-mail from the component requesting clarification, and failed to follow up with the second component when it did not respond to the initial alert. Despite these errors, the incident handlers closed the incident without taking further action.

In addition, most agencies did not consistently consider potential impact of incidents. Although the variance in our statistical sample was too great for us to project a percentage, 2 of the 6 selected agencies demonstrated that they had considered impact; the other 4 did not. In addition, 11 of the 24 agencies responding to our survey reported that they did not categorize the functional impact (e.g., low, moderate, and high) to their agency. Agencies risk ineffective and more costly incident response if they do not account for an incident's impact.

[20] Based on our sample, we are 95 percent confident that the estimate falls between 85 and 95 percent.

[21] For purposes of projecting our sample, we are using the term "governmentwide" to refer to the 24 major *Chief Financial Officers Act* agencies. Small agencies were not included in our sampling population.

Agencies Demonstrated That They Contained the Majority of Incidents

NIST SP 800-61 states that an agency can minimize the impact of an incident by containing it, and emphasizes the importance of containing an incident before it overwhelms resources or increases damages. Containment strategies vary according to the type of incident. For example, an incident involving a lost mobile device could involve sending the device commands that will delete its data and permanently disable it, and then cancelling its access to mobile phone networks. A malware incident could be contained by physically or logically quarantining infected computers, preventing the malware from spreading over the network or communicating with the attacker who initially placed the malware.

Our sample indicates that agencies demonstrated that they had contained the majority of their cyber incidents. Specifically, our analysis shows that agencies had recorded actions to halt the spread of, or otherwise limit, the damage caused by an incident in about 75 percent of incidents governmentwide.[22] However, agencies did not demonstrate such actions for about 25 percent of incidents governmentwide.[23] For example:

- In an incident involving a lost iPhone, the device's mobile service was disabled before a "kill" command could be sent to the device, meaning incident handlers were unable to remotely delete e-mails and other data in its memory, potentially leaving the data exposed to anyone who found the device.
- In a malware incident, sensors on an agency's network recorded an agency computer contacting an external domain known to host malicious files, and downloading a suspicious file. Incident handlers closed the ticket without recording any actions taken to contain or otherwise remediate the potential malware infection.

Although agencies demonstrated that they had contained most of the incidents, those that were not effectively contained could increase the risk of the incident spreading and causing greater damage to their operating environments.

[22] Based on our sample, we are 95 percent confident that the estimate falls between 65 and 84 percent.

[23] Based on our sample, we are 95 percent confident that the estimate falls between 16 and 35 percent.

Agencies Demonstrated That They Eradicated Most Incidents

According to NIST SP 800-61, after an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, and identifying and mitigating all vulnerabilities that have been exploited. During eradication, it is important to identify all affected hosts within the agency so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery. For example, after a lost mobile device has been remotely disabled and had its data deleted and network connectivity severed, incident handlers cannot take further actions regarding that mobile device. In the case of a minor malware incident, the malware could be removed from the system when the infected host has been removed from service or has had its hard drive wiped and its operating system and applications reinstalled.

Our sample indicates that agencies demonstrated that they completed their eradication steps for the majority of cyber incidents. Specifically, our analysis shows that for about 77 percent of incidents governmentwide, the agencies had identified and eliminated the remaining elements of the incident.[24] However, agencies did not demonstrate that they had effectively eradicated incidents in about 23 percent of incidents.[25] For example:

- In a malware incident, incident handlers noted that they had requested the creation of network blocks to isolate the infected computer and the collection of its hard drive for analysis, but the ticket had not been updated to indicate whether the incident handlers had performed the requested actions or any subsequent actions.
- After an administrative password was exposed to one facility’s user population, incident handlers removed the password from the location where it had been posted, but did not indicate that they had changed the password to prevent users who had already seen it from using it.

Although agencies demonstrated that they had eradicated most of the incidents, those that were not effectively eradicated could increase the

[24] Based on our sample, we are 95 percent confident that the estimate falls between 66 and 86 percent.

[25] Based on our sample, we are 95 percent confident that the estimate falls between 14 and 34 percent.

risk that components of an incident might still remain in the operating environment and cause damage.

Agencies Demonstrated Steps to Recover Systems, but Did Not Consistently Demonstrate Remedial Actions to Prevent Reoccurrence

According to NIST SP 800-61, in recovering from an incident, system administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent a similar incident. Recovery may involve actions such as restoring systems from clean backups, rebuilding systems from scratch, and replacing compromised files with clean versions. NIST states that, during recovery, the agency should remediate vulnerabilities to prevent a similar incident from reoccurring (this could include, but is not limited to, installing patches, changing passwords, tightening network perimeter security, user education, adding or enhancing security controls, changing system configurations, etc.).

Agencies generally demonstrated the steps they took in restoring systems to normal operations. Specifically, our analysis shows that agencies returned their systems to an operationally ready state for about 81 percent of incidents governmentwide.[26] However, they had not consistently documented remedial actions on whether they had taken steps to prevent an incident from reoccurring. Specifically, agencies did not demonstrate that they had acted to prevent an incident from reoccurring in about 49 percent of incidents governmentwide.[27] For example:

- In a malware incident, incident handlers determined that a laptop belonging to an agency employee on travel was infected with malware, and was targeting other agency employees. While incident handlers contained the incident by quarantining the machine and blocking the remote sites it was communicating with, they noted that further actions could not be taken until the user had returned from travel. Incident handlers did not document what, if any, action, they took when the employee returned.
- In an incident involving the leak of personally identifiable information, the information of seven agency employees was posted on a third-party website. The data included name, addresses, phone numbers,

[26] Based on our sample, we are 95 percent confident that the estimate falls between 68 and 91 percent.

[27] Based on our sample, we are 95 percent confident that the estimate falls between 41 and 57 percent.

> partial credit card information, mother’s name, e-mail addresses, and password. However, the agency did not document actions it took to determine how the leak had occurred, or how to prevent similar leaks from reoccurring. Incident handlers sent e-mails to the responsible component 31 times over a period exceeding 4 months, requesting status updates and confirmation that the component had taken remedial actions before the incident was eventually closed in the department’s tracking system.

If incident recovery steps are not completed, agencies cannot be assured that they have taken all steps necessary to reduce the risk of similar incidents reoccurring and ensure that their systems will operate optimally.

Agencies Updated Policies or Procedures Post-Incident, but Did Not Generally Capture Cost Information

In its incident response guide, NIST states certain post-incident data can be used to improve the handling of future incidents. Lessons learned and reports from post-incident meetings can be used to update policies and procedures, such as when post-incident analysis reveals a missing step or inaccuracy in a procedure. Data such as the total hours of involvement and the cost may be used to justify additional funding of the incident response team. After handling an incident, an agency should also issue a report that details the cost of the incident, among other information.

Agencies generally updated policies or procedures but did not consistently capture the costs of responding to an incident. Officials at 19 of the 24 agencies surveyed reported that their agency had amended policies or procedures as the result of a cyber incident. However, collection of cost data by agencies varied. Specifically, such information was recorded by only 1 of the selected 6 agencies we reviewed.[28] In addition, 12 of 24 agencies surveyed reported that they had captured the costs of responding to an incident. Without this information, agencies may be unaware of the costs of responding to an incident and lack the information necessary for improving their response in a cost-effective manner.

[28] The variance in our statistical sample was too great for us to project a percentage.

Selected Agencies' Policies, Plans, and Procedures for Cyber Incident Response Did Not Always Include Key Information

NIST states that, to facilitate effective and efficient incident response, agencies should develop corresponding policies, plans, procedures, and practices. However, selected agencies' policies, plans, and procedures did not always include key information.

Selected Agencies' Policies Did Not Include Key Information

NIST SP 800-61 states that policies are necessary for the effective implementation of a response to a cyber incident. Policies should identify the roles, responsibilities, and levels of authority[29] for those implementing incident response activities. In addition, policies should address the prioritization of incidents, an activity that NIST deems to be a critical decision point in the process of handling an incident, and that handling should be prioritized based on factors such as the incident's impact to the organization. Agencies' policies should also address performance measures,[30] which can help evaluate the effectiveness of the incident response.

As shown in table 2, the six selected agencies' policies did not always address each of three key elements defined by NIST.

[29] NIST states that the policy should also include levels of authority; the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity; the requirements for reporting certain types of incidents; the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels); and the handoff and escalation points in the incident management process.

[30] For this report, the term "measures" and "metrics" are used synonymously.

Table 2: Elements Key to Incident Response Policies at Selected Agencies

	Elements		
Agency	Define roles, responsibilities, and levels of authority	Prioritize severity ratings of incidents.	Establish performance measures
DOE	partial	no	no
DOJ[a]	partial	partial	yes
DOT	yes	no	no
HUD	partial	no	no
NASA	yes	yes	no
VA	partial	yes	no

Source: GAO analysis of agencies' incident response policies.

[a] DOJ's incident response policies are included within its incident response plan.

- **Roles, responsibilities, and levels of authority.** Policies for two of the six selected agencies addressed roles, responsibilities, and levels of authority for incident response. Specifically, DOT's cybersecurity policy tasked its Computer Security Incident Response Center with responsibility for implementing and monitoring incident handling for the agency and assigned roles for leading components' incident response planning to individual coordinators. Similarly, NASA's information security handbook specified the authorities of the incident response manager, who may, for example, decide to eradicate an incident without shutting down the system.

  Policies for DOE, DOJ, HUD, and VA partially defined the roles, responsibilities, and levels of authority for responding to cyber incidents. For example, while DOJ's policy defines roles and responsibilities, the agency did not include information on who had authority to confiscate equipment and did not describe when an incident should be escalated. In addition, VA's policies defined roles and responsibilities, but did not include authorities for the incident response team. HUD's policy addressed roles, responsibilities, and levels of authority, but the policy was still in draft at the time of our review. If levels of authority are not clearly defined, agencies risk ineffective incident response, since personnel may be unsure of their responsibilities in responding to an incident.
- **Prioritize severity ratings of incidents.** Policies for two of the six selected agencies fully addressed the prioritization of incidents. For example, NASA's handbook specified that, as part of prioritizing the

handling of an incident, the following should be considered: the incident's categorization, information sensitivity, the system's categorization, and the impact to the system or mission. Conversely, policies for DOE, DOT, and HUD did not address the prioritizing of incidents and DOJ partially addressed it. For example, DOJ's policy addressed the prioritizing of incidents affecting classified systems but not for unclassified systems. Agencies risk an ineffective response if they do not consider an incident's impact, since incidents having the most effect on an agency or its mission may not be addressed in a timely manner.

- **Establish performance measures.** One of the six selected agencies addressed the establishment of performance measures. DOJ listed several objectives for measuring incident response, such as limiting an incident's duration, minimizing impact to the department's operations, and requiring annual tests of the department's incident response capability. Policies for DOE, DOT, HUD, NASA, and VA did not address any measures of performance. Without such measures, agencies may lack the information needed to evaluate the effectiveness of their incident response.

Selected Agencies' Plans Did Not Address All Key Elements

NIST SP 800-61 states that incident response plans should be developed to provide guidance for implementing incident response practices based on the agency's policies. Further, NIST states the plan should be approved by senior management to indicate their support for the plan. The plan should also include and define metrics for measuring and evaluating the effectiveness of incident response. According to NIST, one such example would be "the total amount of labor spent working on the incident."

As shown in table 3, the six selected agencies' incident response plans did not consistently address two of the key elements defined by NIST. Following the table is a further discussion of those agencies' incident response plans.

Table 3: Elements Key to Incident Response Plans at Selected Agencies

	Elements	
Agency	Senior management approval	Metrics for measuring incident response capability and effectiveness
DOE	yes	no
DOJ	yes	partial
DOT	no	no
HUD	no	no
NASA	yes	no
VA	yes	no

Source: GAO analysis of agencies' incident response plans.

- **Senior management approval.** Senior managers approved incident response plans for four of the six selected agencies. For example, DOE's deputy secretary approved the department plan, and DOJ's Chief Information Officer signed and approved his agency's incident response plan. Similarly, NASA's Deputy Chief Information Officer for IT Security approved the agency's document and VA's Network Security Operations Center Director also approved his department's plan. However, DOT's plan did not indicate that its senior management had approved it and HUD had not yet developed a plan at the time of our review. Without senior management commitment, an agency may not have the support for resources necessary to implement an effective incident response.
- **Metrics for measuring effectiveness.** Only one of the six selected agencies included metrics for measuring their incident response capability and effectiveness. To illustrate, DOJ's plan included requirements for reporting incidents within established time frames, for example, that a data loss involving sensitive information should be reported within 1 hour. However, other metrics listed on the plan were not measurable. We have previously noted that it is important to develop metrics that are measurable.[31] The remaining five agencies (i.e., DOE, DOT, HUD, NASA, and VA) did not address metrics in their incident response plans. If agencies do not include metrics in their plans, they may not be able to establish clear goals needed for

[31] GAO-09-617, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures* (Washington, D.C.: Sept. 14, 2009).

measuring and determining whether their incident response is effective.

Selected Agencies Did Not Always Develop Procedures for Incident Response

FISMA requires agencies to develop procedures for responding to an incident. NIST SP 800-61 also states that, in addition to being based on incident response policies, such procedures should provide detailed steps for responding to an incident and cover all phases of the incident response process. According to NIST, following standardized responses as listed in procedures should minimize errors resulting from “stressful” incident handling situations. NIST lists several types of incident response procedures that agencies should develop. These include procedures for containing an incident that detail how incident handlers should contain specific types of incidents in a manner that meets the agency’s definition of acceptable risk and procedures for prioritizing incident handling, which allow incident handlers to more quickly determine how best to apply their resources based on risk.

As shown in table 4, selected agencies did not always develop procedures for responding to incidents, as NIST suggests.

Table 4: Incident Response Procedures at Selected Agencies

Agency	Procedures for containing incidents	Procedures that address the prioritization of handling incidents
DOE	partial	partial
DOJ	yes	no
DOT	yes	no
HUD	yes	partial
NASA	yes	yes
VA	yes	yes

Source: GAO analysis of agencies’ incident response procedures.

- **Procedures for containing incidents.** Five of the six selected agencies developed procedures for containing incidents. For example, DOJ developed procedures for handling e-mails with malicious content and procedures for blocking potential malicious IP addresses. Similarly, DOT’s incident response group’s standard operating procedures identify procedures for handling key logging software, which can record keystrokes and capture sensitive information such as usernames and passwords. However, DOE procedures partially addressed the containing of incidents. For example, while the department had not developed procedures for containing incidents, two DOE components had developed such procedures. Without procedures for containing incidents, incident response personnel may not have instructions necessary to prevent incidents from negatively affecting other parts of their operating environment.

- **Procedures for prioritizing incidents.** Two of the six selected agencies developed and documented procedures for prioritizing the handling of incidents. NASA listed eight factors for determining the priority of handling an incident. Each of the factors is to be assigned a rating, after which the ratings for each factor would be added together to determine a number that would then be mapped to a priority ranging from low to critical. In addition, VA developed procedures for prioritizing incidents where a matrix would be used to map the type of incident to a predefined priority, such as critical, high, medium, and low, for handling the incident. Procedures for HUD and DOE partially addressed this activity since their procedures did not specify whether risk or impact would determine incident handling priorities. The remaining two of the six agencies (i.e., DOJ and DOT) had not developed and documented procedures for prioritizing incidents. As a result, these agencies may not be addressing incidents affecting the agency in the most risk-effective manner.

Other Incident Response Practices Were Not Implemented

NIST SP 800-53 states that agencies are to test their incident response capability, at an agency-defined frequency, for their information systems to determine the effectiveness of procedures for responding to cyber incidents. Agencies should also train personnel in their incident response roles and responsibilities. According to NIST, the lack of a well-trained and capable staff could result in inefficient incident detection and analysis and costly mistakes.

As shown in table 5, agencies did not test their incident response capabilities or consistently train staff responsible for responding to incidents.

Table 5: Other Incident Response Practices at Selected Agencies

	Other incident response practices	
Agency	Tested incident response	Trained incident response personnel
DOE	partial	partial
DOJ	partial	yes
DOT	no	yes
HUD	no	yes
NASA	no	partial
VA	no	no

Source: GAO analysis of agencies' incident response practices.

- **Tested incident response capability.** Four of the six agencies had not tested their incident response capability and two—DOE and DOJ—partially tested their incident response capabilities. For example, DOE did not demonstrate that the department had conducted an entitywide test of its incident response capability and only provided information concerning a review of a key component's incident response activities. In addition, components at DOJ are responsible for testing their own incident response capability, with 10 of the 13 agency components completing testing of their capabilities. If an agency's incident response capability has not been tested, the agency will have limited assurance its controls have been effectively implemented.
- **Trained incident response personnel.** Three of the six agencies trained their incident response personnel. For example, both DOJ and HUD maintained a list of personnel who were responsible for responding to their department's incidents. These lists included the dates staff received training and the type of training received. DOT also trained their incident response personnel. However, VA did not demonstrate that their incident response personnel had received training, and DOE and NASA partially addressed this activity. For example, NASA provided a detailed listing of incident response personnel and the types of training they had taken, but did not define what qualified as acceptable training. If staff do not receive training on their incident response roles, they may not have the knowledge or skills to ensure they are prepared to effectively respond to cyber incidents affecting their agency.

OMB and DHS Have Not Used the CyberStat Review Process to Address Agencies' Incident Response Practices

Inconsistencies in agencies' performance of incident response activities and development of policies, plans, and procedures indicate that further oversight, such as that provided by OMB's and DHS's CyberStat review process, may be warranted. CyberStat reviews are in-depth sessions with

National Security Staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and discuss opportunities for collaboration. According to OMB, these reviews were face-to-face, evidence-based meetings to ensure agencies were accountable for their cybersecurity posture and to assist them in developing focused strategies for improving their information security posture in areas where they faced challenges. According to DHS, the goal for fiscal year 2013 was for all 24 major agencies to be reviewed. However, this goal was not met. DHS officials stated that the reviews were conducted with 7 federal agencies, and that interviews were conducted with chief information officers from the other 17 agencies.

In addition, the current CyberStat reviews have not generally covered agencies' cyber incident response practices, such as considering impact to aid in prioritizing incident response activities, recording key steps in responding to an incident, and documenting the costs for responding to an incident. DHS officials told us that, regarding incident response, the reviews discussed the status of agencies' closing of incidents and trends surrounding incident reporting; however, the reviews did not address evaluating the incident response practices of the agencies. Without addressing response practices in these reviews, OMB and DHS may be missing opportunities to help agencies improve their information security posture and more effectively respond to cyber incidents.

Agencies Were Generally Satisfied with Services Provided by DHS, but Reported That DHS Could Enhance Assistance to Agencies

While DHS provides various services to agencies to assist them in addressing cyber incidents, opportunities exist to improve the usefulness of these services, according to the 24 agencies we surveyed. DHS components, including US-CERT, offer services that assist agencies in preparing to handle incidents, maintain awareness of the current threat environment, and deal with ongoing incidents. Based on responses to our survey, officials at 24 major agencies were generally satisfied with DHS's service offerings, although they identified improvements they believe would make certain services more useful, such as improving reporting requirements. For its part, US-CERT does not evaluate the effectiveness of its incident services.

DHS Makes a Variety of Incident Services Available to Agencies

US-CERT serves as the central federal information security incident center mandated by FISMA. By law, the center is required to

- provide timely technical assistance to operators of agency information systems regarding security incidents,

- compile and analyze information about incidents that threaten information security,
- inform operators of agency information systems about current and potential information security threats and vulnerabilities, and
- consult with NIST and agencies operating national security systems regarding security incidents.

More broadly, OMB has transferred responsibility to DHS for the operational aspects of federal cybersecurity, including overseeing and assisting federal agencies' cybersecurity operations and incident response. Table 6 lists DHS cyber incident assistance services.

Table 6: Informational and Technical Assistance Services Provided by DHS to Federal Agencies

Service	Description
US-CERT portal	Provides a secure online forum for vetted incident responders to share information about cyber incidents, threats, and vulnerabilities.
US-CERT website	Provides alerts about new and ongoing attacks, links to information on newly identified vulnerabilities, contact information for US-CERT, and links and instructions for reporting incidents, phishing, malware, and software vulnerabilities.
Malware analysis	Analyzes agency-submitted malware samples to identify their functionality and behavioral characteristics, in support of improving detection and mitigation activities.
Digital forensics	Analyzes the current state of digital artifacts (e.g., computer systems, storage mediums such as hard drives, CD-ROM, and physical memory of computer systems using industry standard tools).
Einstein[a] alerts	Develops and deploys threat indicator signatures across Einstein 2 to improve detection capabilities. Monitors and correlates Einstein 1 and Einstein 2 sensor data to identify potentially malicious activity directed at agency networks and reports it to incident handlers.
Red team/Blue team	Provides services including assessments of agencies' technical cybersecurity capabilities, and operational readiness, vulnerability assessment and validation, testing of web applications, and testing of incident response capabilities.
On-site technical assistance	US-CERT analysts with specialized laptops and digital forensic data capture equipment provide on-site incident response to an agency.
Threat and vulnerability warnings	Review and correlate technical data from partners, constituents, and monitoring systems and use this information to develop periodical and event-driven alerts and warnings for US-CERT's partners and constituents.

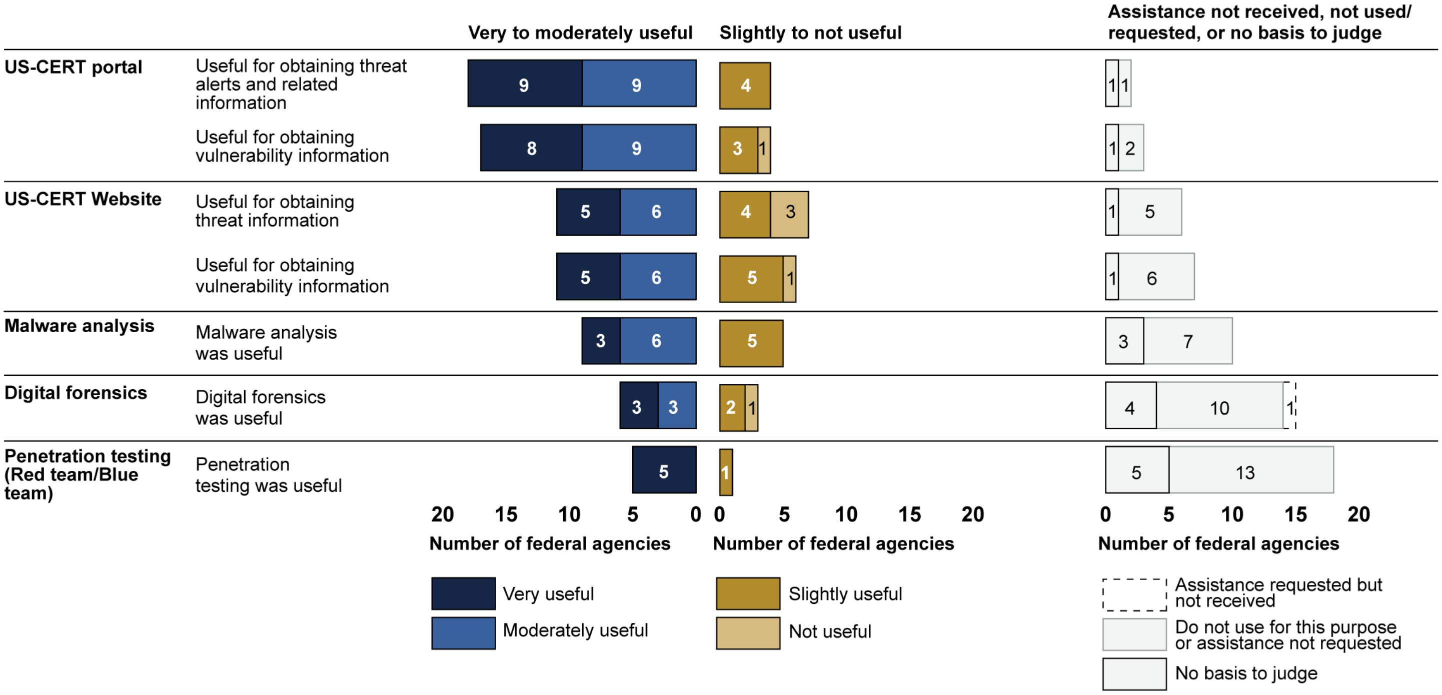
Source: GAO analysis of DHS documents

[a] Einstein is a set of systems that monitor federal agencies' connections to the Internet. Einstein 1 allows agencies to monitor network traffic between their network connections and the Internet, while Einstein 2 has intrusion detection capabilities that can identify potentially malicious network activity as it is occurring and alert incident handlers. Einstein 3, which DHS is currently deploying, will include the capability to automatically block malicious traffic upon detection.

Surveyed Agency Officials Identified Opportunities to Improve DHS Incident Services

The results of our survey indicate that agency officials were generally satisfied with the services provided to them by DHS, and they offered various opinions about DHS services or noted dissatisfaction with incident reporting requirements. Of the agency officials that used services provided to them by DHS, as illustrated in figure 2, the majority were generally satisfied, finding the service to be very or moderately useful.

Figure 2: Satisfaction with Services Provided by DHS, as Reported by Agencies



Source: GAO survey.

In addition, officials from 16 of the 24 agencies reported that they were generally satisfied with DHS's outreach efforts to inform them of cyber incident services and assistance, while 4 of the 24 officials reported that they were generally dissatisfied.[32]

[32] The remaining four agencies did not provide an opinion.

However, surveyed officials at 11 of the 24 agencies noted dissatisfaction with incident reporting requirements. Agency officials made the following comments:

- Time frames are difficult to meet.
- The incident categories are no longer practical. Attributes that contribute to classification are not unique between the categories and it allows for too much discretion and interpretation. The categories are long overdue for updates.
- A category that separates data loss from unauthorized access would be beneficial.
- A category specific to phishing and advanced persistent threats would be helpful.
- Add a category for non-incident. Additionally, each category should have sub-categories to further identify the incident and how it happened.

These comments are consistent with the results of a review we conducted in 2013.[33] Based on that review, we made recommendations to OMB to revise reporting requirements to DHS for personally identifiable information-related data breaches, including time frames that would better reflect the needs of individual agencies and the government as a whole. DHS officials provided information about actions the agency plans to take to help address our recommendations and stated that it has interacted with OMB regarding requirements specific to these recommendations and is preparing new incident reporting guidance for agencies.

[33] GAO-14-34, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent* (Washington, D.C.: Dec. 9, 2013).

US-CERT Receives Feedback to Improve Services, but Has Not Yet Developed Performance Measures for Evaluating the Effectiveness of Assistance Provided to Agencies

We and others[34] have noted the value of having clear performance measures that demonstrate results. Such measures support an agency's efforts to plan, reinforce accountability, and advance the agency's mission.

However, US-CERT has not established measures to evaluate the effectiveness of the cyber incident assistance it provides to agencies. US-CERT gathers usage statistics and feedback on its public website and portal and uses those data to identify opportunities for improving those services, but it only performs these reviews on an ad-hoc basis. For its other activities, a US-CERT official stated that the agency gathers monthly statistics on activities such as the number of on-site or remote technical assistance engagements it performs each month, or the number of pieces of malware analyzed by staff.

The official noted, however, that these numbers are driven by factors outside of US-CERT's control, and as such, indicate activity levels rather than performance measures and that the agency is still trying to identify meaningful performance measures. However, without results-oriented performance measures, US-CERT will face challenges in ensuring it is effectively assisting federal agencies with preparing for and responding to cyber incidents.

Conclusions

With federal agencies facing increasing and more threatening cyber incidents, it is essential for them to be able to effectively manage their response activities. However, agencies did not consistently demonstrate that they responded to cyber incidents in an effective manner. Although agencies often demonstrated that they carried out various aspects of incident response activities, documenting all of the steps taken to analyze, contain, eradicate, and recover from incidents are important actions for agencies to take to ensure that incidents are being appropriately addressed. Having comprehensive policies, plans, and procedures that include measures of performance and guidance on impact assessment provide key elements necessary for agencies to effectively respond to cyber incidents. Testing the incident response

[34] See, for example, GAO, *Effectively Implementing the Government Performance and Results Act,* GAO/GGD-96-118 (Washington, D.C.: June 1, 1996) and CMMI Product Team, *CMMI for Services, Version 1.3* (Pittsburgh, Pa.: Carnegie Mellon University, 2010).

program and ensuring employees are appropriately trained increases the assurance that controls are in place to prevent, detect, or respond to incidents. Further, capturing related costs could help agencies more efficiently manage their incident response activities. OMB and DHS have established CyberStat reviews to improve information security at federal agencies, but the reviews have not focused on agencies' incident response practices.

Although DHS and US-CERT offer numerous services to agencies to assist with cyber incidents, US-CERT does not have a process in place to evaluate the effectiveness of the assistance that it provides agencies. Without results-oriented performance measures, US-CERT will face challenges in ensuring that it is effectively assisting federal agencies with preparing for and responding to cyber incidents.

Recommendations for Executive Action

To improve the effectiveness of governmentwide cyber incident response activities, we recommend that the Director of OMB and Secretary of Homeland Security address agency incident response practices governmentwide, in particular through CyberStat meetings, such as emphasizing the recording of key steps in responding to an incident.

To improve the effectiveness of cyber incident response activities, we are making 25 recommendations to six selected agencies to improve their cyber incident response programs.

We recommend that the Secretary of Energy:

- revise policies for incident response to include requirements for defining the incident response team's level of authority, prioritizing the severity ratings of incidents based on impact and establishing measures of performance;
- revise the department's incident response plan to include metrics for measuring the incident response capability and its effectiveness;
- develop incident response procedures that provide instructions for containing incidents and revise procedures for incident response to prioritize the handling of incidents by impact;
- fully test the department's incident response capability; and
- establish clear requirements to ensure the department's incident response personnel are trained.

We recommend that the Attorney General of the United States:

- revise policies for incident response by including requirements for defining the incident response team's level of authority, and prioritizing the severity ratings of incidents for unclassified systems, based on impact;
- revise the department's incident response plan to include quantifiable metrics for measuring the incident response capability and its effectiveness;
- develop incident response procedures that provide instructions for prioritizing the handling of incidents by impact; and
- ensure that all components test their incident response capability.

We recommend that the Secretary of Transportation:

- revise policies for incident response by including requirements for prioritizing the severity ratings of incidents based on impact and establishing measures of performance;
- revise the department's incident response plan to include senior management's approval, and metrics for measuring the incident response capability and its effectiveness;
- develop incident response procedures that provide instructions for prioritizing the handling of incidents by impact; and
- test the department's incident response capability.

We recommend that the Secretary of Housing and Urban Development:

- finalize policies for incident response and include in those policies requirements for prioritizing the severity ratings of incidents and establishing measures of performance;
- develop a departmentwide incident response plan that includes, among other elements, senior management's approval, and metrics for measuring the incident response capability and its effectiveness;
- revise procedures for incident response to prioritize the handling of incidents by impact; and
- test the department's incident response capability.

We recommend that Administrator of the National Aeronautics and Space Administration:

- revise policies for incident response by including requirements for establishing measures of performance;
- revise the agency's incident response plan to include metrics for measuring the incident response capability and its effectiveness;
- test the agency's incident response capability; and

- establish clear requirements for training the agency's incident response personnel.

We recommend that the Secretary of Veterans Affairs:

- revise policies for incident response by including requirements for defining the incident response team's level of authority, and establishing measures of performance;
- revise the department's incident response plan to include metrics for measuring the incident response capability and its effectiveness;
- test the department's incident response capability; and
- train the department's incident response personnel per the agency's requirements.

To improve the cyber incident response assistance provided to federal agencies, we recommend that the Secretary of Homeland Security:

- establish measures to evaluate the effectiveness of the cyber incident assistance it provides to agencies.

Agency Comments and Our Evaluation

We sent draft copies of this report to the six agencies selected for our sample, as well as to DHS and OMB. We received written responses from DOE, DHS, HUD, NASA and VA. These comments are reprinted in appendices II through VI. The audit liaisons for DOJ and DOT responded via e-mail. However, OMB did not provide comments to our draft report.

Six of the eight agencies generally concurred with our recommendations. Five agencies (DOE, DHS, DOJ, HUD, and VA) concurred with all of our recommendations. NASA agreed with three of four draft recommendations and partially agreed with the fourth recommendation. DOT responded that the department had no comments. In cases where these agencies also provided technical comments, we have addressed them in the final report as appropriate. DOE, DHS, NASA, and VA also provided information regarding specific actions they have taken or plan on taking that address portions of our recommendations. Further, DHS, NASA, and VA provided estimated timelines for completion of actions that would address our recommendations.

NASA agreed with our three recommendations to revise its incident response policy, revise its incident response plan, and test the agency's incident response capability. In addition, it partially concurred with our recommendation that the agency establish clear requirements for training its incident response personnel. The Chief Information Officer stated that agency personnel were being trained in their response roles and responsibilities. He added that his office would define what qualified as acceptable training for incident response personnel and that his office would then update policy to reflect the need for focused incident response training. We believe these actions, if effectively implemented, will satisfy our recommendation.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Departments of Energy, Homeland Security, Housing and Urban Development, Justice, Transportation, and Veterans Affairs, as well as the National Aeronautics and Space Administration and the Office of Management and Budget. In addition, the report is available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact Gregory C. Wilshusen at (202) 512-6244. I can also be reached by e-mail at wilshuseng@gao.gov. Key contributors to this report are listed in appendix VII.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to evaluate the extent to which (1) federal agencies are effectively responding to cyber incidents and (2) the Department of Homeland Security (DHS) provides cyber incident assistance to agencies.

To address our first objective, we reviewed the *Federal Information Security Management Act (FISMA)*, National Institute of Standards and Technology (NIST) *Special Publication 800-53 Revision 3, Special Publication 800-61 Revision 2*, Office of Management and Budget (OMB) OMB-06-19,[1] and United States Computer Emergency Readiness Team (US-CERT) guidance to determine the key steps agencies should address when responding to a cyber incident. We then used a two-stage cluster sample to identify a generalizable sample of incidents to review for compliance with key steps. First, we selected 6 agencies from the population of 24 major agencies covered by the *Chief Financial Officers Act*,[2] using probability proportionate to the number of cyber incidents those agencies had reported to US-CERT in fiscal year 2012, divided by 32,442—the total number of cyber incidents reported to US-CERT in fiscal year 2012—sampling without replacement. The 6 agencies selected were the Departments of Energy (DOE), Justice (DOJ), Housing and Urban Development (HUD), Transportation (DOT), Veterans Affairs (VA), and the National Aeronautics and Space Administration (NASA). After selecting the 6 agencies in the first stage of sampling, we then obtained for each agency the list of individual cyber incidents for fiscal year 2012. From those lists, we then randomly selected 40 cyber incidents within each agency, for a total sample size of 240 cyber incidents. This statistical sample allowed us to project the results, with 95 percent confidence, to the 24 major agencies. Table 7 lists the number of incidents in our sample in each of the six US-CERT-defined incident categories.

[1] Office of Management and Budget, *Memorandum for Chief Information Officers: Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, M-06-19 (Washington, D.C.: July 12, 2006).

[2] The 24 major departments and agencies covered by the Chief Financial Officers Act are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

Table 7: Sample Cyber incidents by US-CERT Incident Category

US-CERT category	Sample incidents by category
Category 1 —Unauthorized access	69
Category 2 —Denial of service	0
Category 3 —Malicious code	66
Category 4 —Improper usage	45
Category 5 —Scans/probes/attempted access	32
Category 6 —Investigation	28
Total	**240**

Source: GAO analysis of US-CERT data.

Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our particular sample's results as a 95 percent confidence interval (e.g., plus or minus 7 percentage points). This is the interval that would contain the actual population value for 95 percent of the samples we could have drawn.

To determine the reliability and accuracy of the data we used to develop our sample, we interviewed knowledgeable agency officials and reviewed related documentation on internal controls for US-CERT's database of incident tickets and reviewed the data for duplicates and outliers. For the incident data in our sample, we interviewed officials at the six agencies in our sample, reviewed each agency's incident management system to gain an understanding of the data, reviewed related documentation on internal controls for each agency's incident management system, and traced a random sample of records back to source agency documents and tested the fields for accuracy. Our sample results capture estimates for the extent of duplicate records, false positives, and inaccurately recorded data fields. Based on this assessment, we determined that the data were sufficiently reliable for our work.

To address the effectiveness with which agencies responded to a cyber incident, we reviewed documents (extracted from agencies' incident tracking systems) covering the incidents in our sample to determine the extent to which the agencies had performed analysis, containment, eradication, recovery, reporting, and post-incident procedures in accordance with federal requirements and guidance and their own policies and procedures. In addition, we reviewed and analyzed the six selected agencies' cyber incident response policies, plans, procedures, and practices and compared them to key elements in NIST guidance; and interviewed agency officials to discuss their incident response practices.

We also conducted a web-based survey of officials responsible for cyber incident response at the 24 major federal agencies.

After we drafted the questionnaire, we asked for comments from independent GAO survey professionals, and we conducted two in-person pretests to check that (1) the questions were clear and unambiguous, (2) terminology was used correctly, (3) the questionnaire did not place an undue burden on agency officials, (4) the information could be obtained, and (5) the survey was comprehensive and unbiased. We chose the pretest participants to include one member of our survey population, and one official from a federal agency not in our population, but who had a similar role and responsibilities with regard to incident response.

We made changes to the content and format of the questionnaire after the review and both pretests, based on the feedback we received.

We received completed questionnaires from all 24 agencies surveyed. Because this was not a sample survey, it has no sampling errors. However, the practical difficulties of conducting any survey may introduce errors, commonly referred to as nonsampling errors. For example, difficulties in interpreting a particular question, sources of information available to respondents, or entering data into a database or analyzing them can introduce unwanted variability into the survey results.

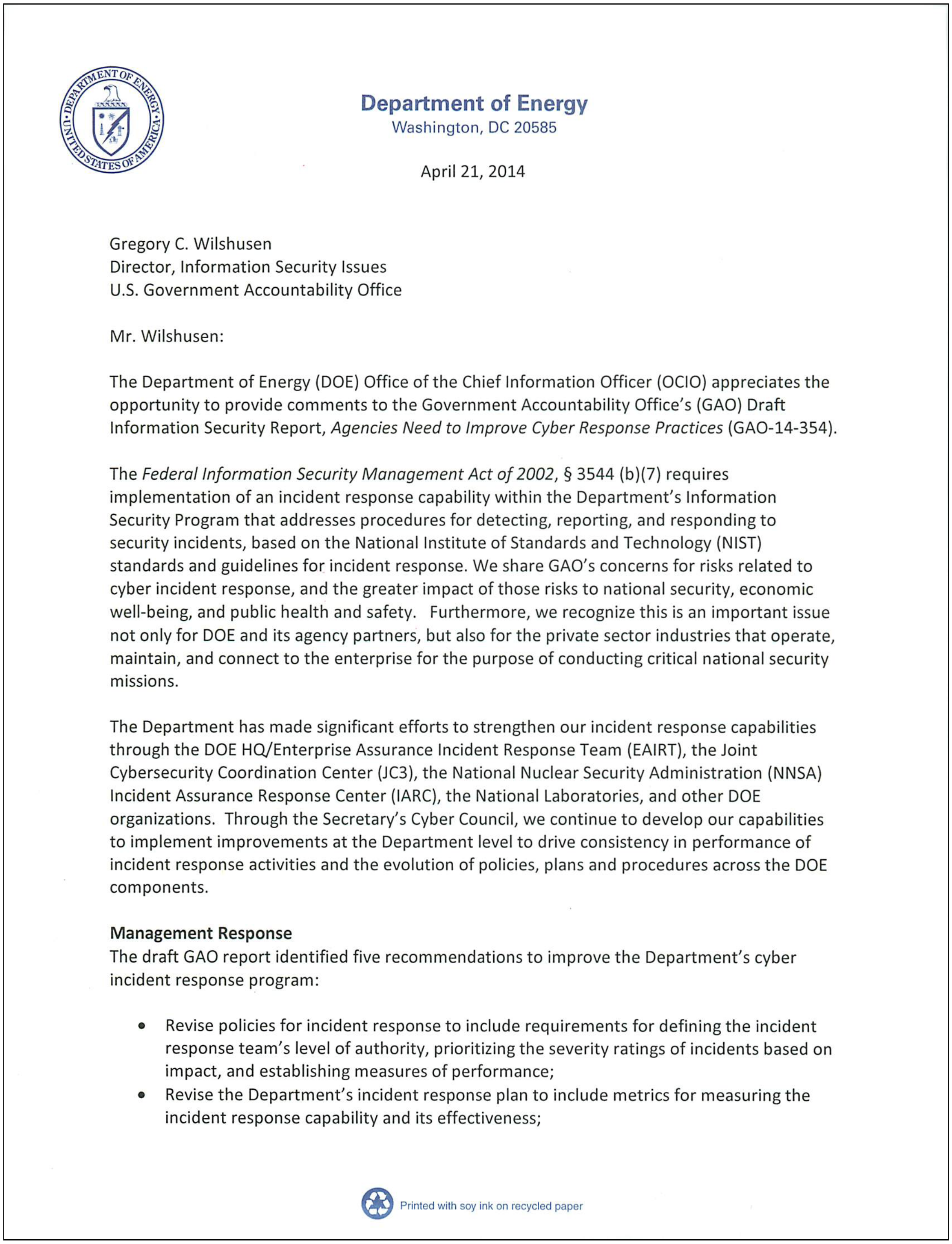
We took steps in developing the questionnaire, collecting the data, and analyzing them to minimize such nonsampling errors. For example, social science survey specialists designed the questionnaire in collaboration with GAO staff who had subject matter expertise. Then, we pretested the draft questionnaire with a number of officials to ensure that the questions were relevant, clearly stated, and easy to understand. When we analyzed the data, an independent analyst checked all computer programs. Since this was a web-based survey, respondents entered their answers directly into the electronic questionnaire, eliminating the need to key data into a database.

To address our second objective, we reviewed DHS documents, reviewed US-CERT's public-facing website and limited-access portal, and interviewed officials at DHS about the services it offers to agencies to support their incident response capabilities and activities. In addition, as part of our web-based survey, we asked officials at the agencies what incident response-related services or assistance they had sought from DHS, and their opinion of those services and the utility of US-CERT's public website and limited-access portal. In addition, we interviewed agency officials from the six agencies selected as part of our random sample regarding their interactions with DHS in receiving cyber incident assistance. We compared the assistance provided by DHS, including US-CERT, to the requirements specified in FISMA. Further, we met with officials to determine whether the department had measures—such as those described by us and others[3]—to evaluate the effectiveness of the assistance they provided to agencies.

We conducted this performance audit from February 2013 to April 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[3] See, for example, GAO, *Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1, 1996) and CMMI Product Team, *CMMI for Services*, Version 1.3 (Pittsburgh, Pa.: Carnegie Mellon University, 2010).

Appendix II: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

April 21, 2014

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office

Mr. Wilshusen:

The Department of Energy (DOE) Office of the Chief Information Officer (OCIO) appreciates the opportunity to provide comments to the Government Accountability Office's (GAO) Draft Information Security Report, *Agencies Need to Improve Cyber Response Practices* (GAO-14-354).

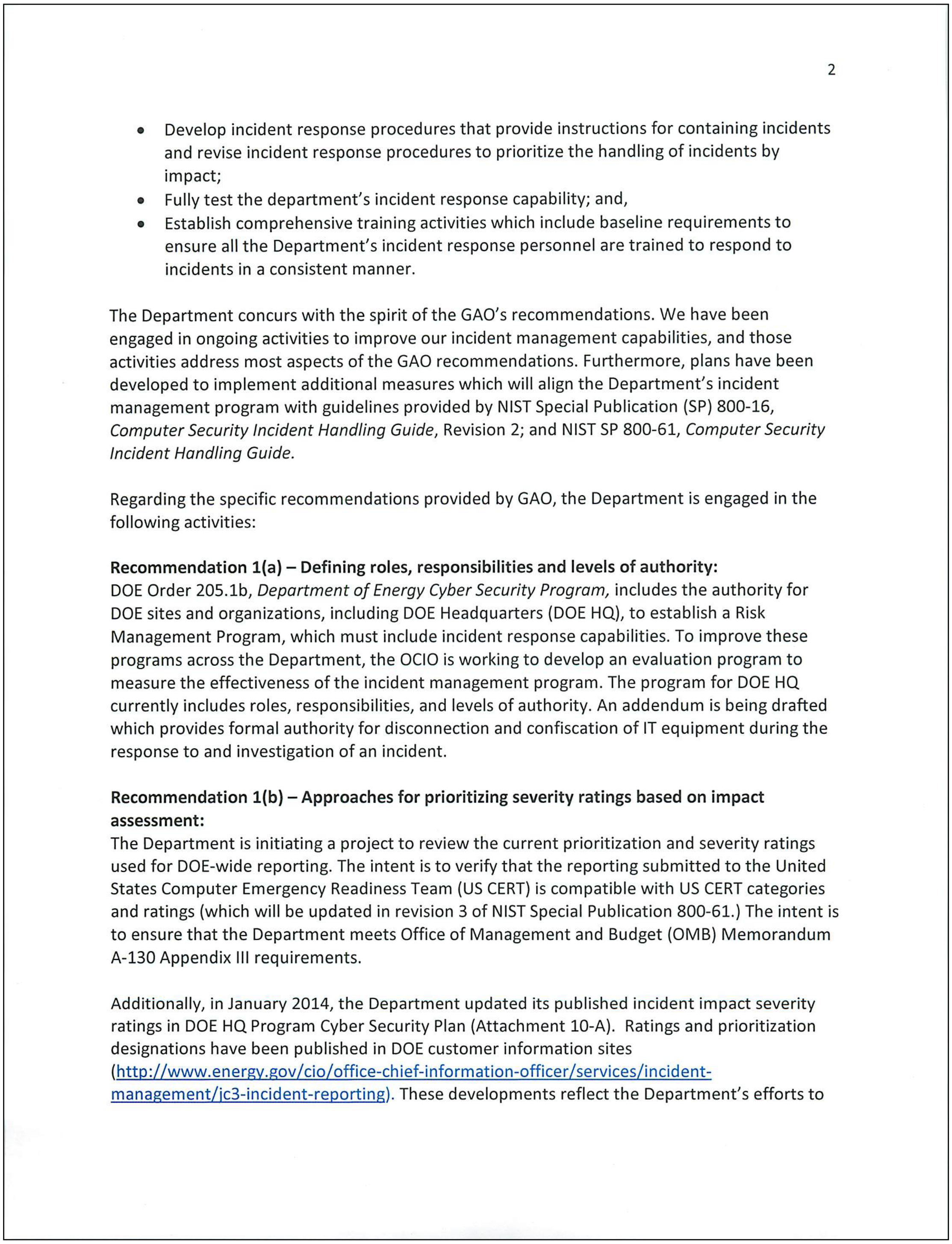
The *Federal Information Security Management Act of 2002*, § 3544 (b)(7) requires implementation of an incident response capability within the Department's Information Security Program that addresses procedures for detecting, reporting, and responding to security incidents, based on the National Institute of Standards and Technology (NIST) standards and guidelines for incident response. We share GAO's concerns for risks related to cyber incident response, and the greater impact of those risks to national security, economic well-being, and public health and safety. Furthermore, we recognize this is an important issue not only for DOE and its agency partners, but also for the private sector industries that operate, maintain, and connect to the enterprise for the purpose of conducting critical national security missions.

The Department has made significant efforts to strengthen our incident response capabilities through the DOE HQ/Enterprise Assurance Incident Response Team (EAIRT), the Joint Cybersecurity Coordination Center (JC3), the National Nuclear Security Administration (NNSA) Incident Assurance Response Center (IARC), the National Laboratories, and other DOE organizations. Through the Secretary's Cyber Council, we continue to develop our capabilities to implement improvements at the Department level to drive consistency in performance of incident response activities and the evolution of policies, plans and procedures across the DOE components.

Management Response
The draft GAO report identified five recommendations to improve the Department's cyber incident response program:

- Revise policies for incident response to include requirements for defining the incident response team's level of authority, prioritizing the severity ratings of incidents based on impact, and establishing measures of performance;
- Revise the Department's incident response plan to include metrics for measuring the incident response capability and its effectiveness;

Printed with soy ink on recycled paper



- Develop incident response procedures that provide instructions for containing incidents and revise incident response procedures to prioritize the handling of incidents by impact;
- Fully test the department's incident response capability; and,
- Establish comprehensive training activities which include baseline requirements to ensure all the Department's incident response personnel are trained to respond to incidents in a consistent manner.

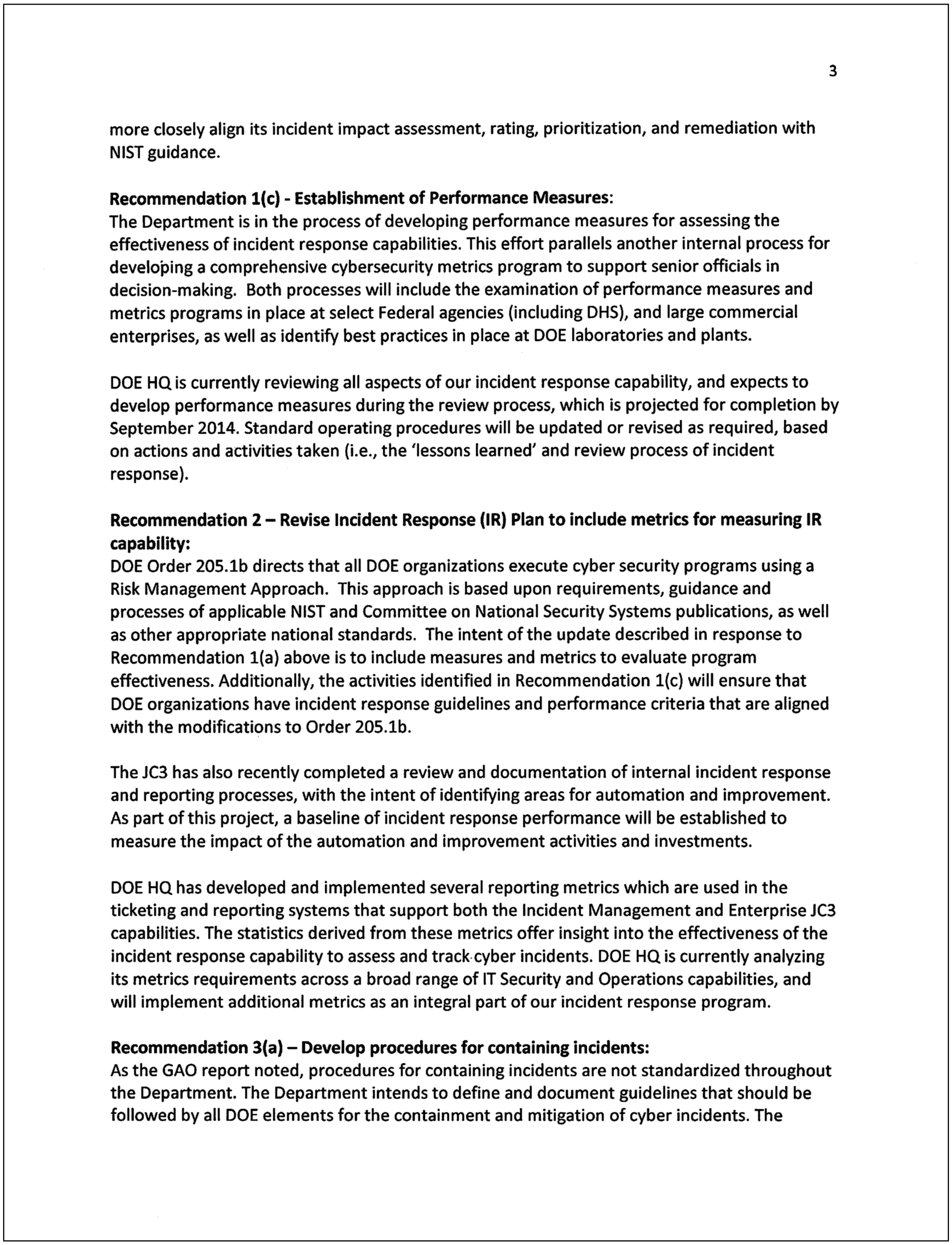
The Department concurs with the spirit of the GAO's recommendations. We have been engaged in ongoing activities to improve our incident management capabilities, and those activities address most aspects of the GAO recommendations. Furthermore, plans have been developed to implement additional measures which will align the Department's incident management program with guidelines provided by NIST Special Publication (SP) 800-16, *Computer Security Incident Handling Guide*, Revision 2; and NIST SP 800-61, *Computer Security Incident Handling Guide*.

Regarding the specific recommendations provided by GAO, the Department is engaged in the following activities:

Recommendation 1(a) – Defining roles, responsibilities and levels of authority:
DOE Order 205.1b, *Department of Energy Cyber Security Program,* includes the authority for DOE sites and organizations, including DOE Headquarters (DOE HQ), to establish a Risk Management Program, which must include incident response capabilities. To improve these programs across the Department, the OCIO is working to develop an evaluation program to measure the effectiveness of the incident management program. The program for DOE HQ currently includes roles, responsibilities, and levels of authority. An addendum is being drafted which provides formal authority for disconnection and confiscation of IT equipment during the response to and investigation of an incident.

Recommendation 1(b) – Approaches for prioritizing severity ratings based on impact assessment:
The Department is initiating a project to review the current prioritization and severity ratings used for DOE-wide reporting. The intent is to verify that the reporting submitted to the United States Computer Emergency Readiness Team (US CERT) is compatible with US CERT categories and ratings (which will be updated in revision 3 of NIST Special Publication 800-61.) The intent is to ensure that the Department meets Office of Management and Budget (OMB) Memorandum A-130 Appendix III requirements.

Additionally, in January 2014, the Department updated its published incident impact severity ratings in DOE HQ Program Cyber Security Plan (Attachment 10-A). Ratings and prioritization designations have been published in DOE customer information sites (http://www.energy.gov/cio/office-chief-information-officer/services/incident-management/jc3-incident-reporting). These developments reflect the Department's efforts to



more closely align its incident impact assessment, rating, prioritization, and remediation with NIST guidance.

Recommendation 1(c) - Establishment of Performance Measures:
The Department is in the process of developing performance measures for assessing the effectiveness of incident response capabilities. This effort parallels another internal process for developing a comprehensive cybersecurity metrics program to support senior officials in decision-making. Both processes will include the examination of performance measures and metrics programs in place at select Federal agencies (including DHS), and large commercial enterprises, as well as identify best practices in place at DOE laboratories and plants.

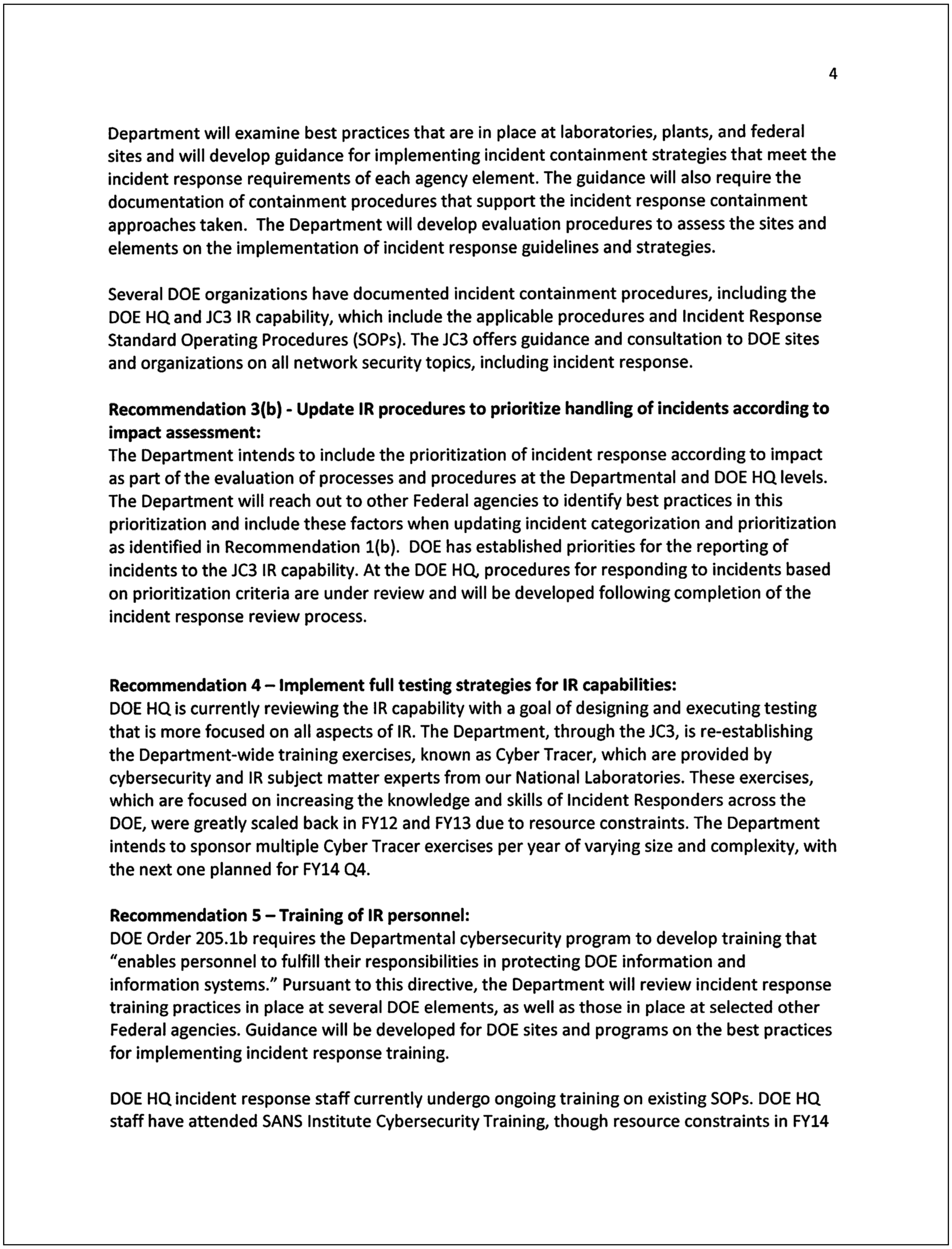
DOE HQ is currently reviewing all aspects of our incident response capability, and expects to develop performance measures during the review process, which is projected for completion by September 2014. Standard operating procedures will be updated or revised as required, based on actions and activities taken (i.e., the 'lessons learned' and review process of incident response).

Recommendation 2 – Revise Incident Response (IR) Plan to include metrics for measuring IR capability:
DOE Order 205.1b directs that all DOE organizations execute cyber security programs using a Risk Management Approach. This approach is based upon requirements, guidance and processes of applicable NIST and Committee on National Security Systems publications, as well as other appropriate national standards. The intent of the update described in response to Recommendation 1(a) above is to include measures and metrics to evaluate program effectiveness. Additionally, the activities identified in Recommendation 1(c) will ensure that DOE organizations have incident response guidelines and performance criteria that are aligned with the modifications to Order 205.1b.

The JC3 has also recently completed a review and documentation of internal incident response and reporting processes, with the intent of identifying areas for automation and improvement. As part of this project, a baseline of incident response performance will be established to measure the impact of the automation and improvement activities and investments.

DOE HQ has developed and implemented several reporting metrics which are used in the ticketing and reporting systems that support both the Incident Management and Enterprise JC3 capabilities. The statistics derived from these metrics offer insight into the effectiveness of the incident response capability to assess and track cyber incidents. DOE HQ is currently analyzing its metrics requirements across a broad range of IT Security and Operations capabilities, and will implement additional metrics as an integral part of our incident response program.

Recommendation 3(a) – Develop procedures for containing incidents:
As the GAO report noted, procedures for containing incidents are not standardized throughout the Department. The Department intends to define and document guidelines that should be followed by all DOE elements for the containment and mitigation of cyber incidents. The



Department will examine best practices that are in place at laboratories, plants, and federal sites and will develop guidance for implementing incident containment strategies that meet the incident response requirements of each agency element. The guidance will also require the documentation of containment procedures that support the incident response containment approaches taken. The Department will develop evaluation procedures to assess the sites and elements on the implementation of incident response guidelines and strategies.

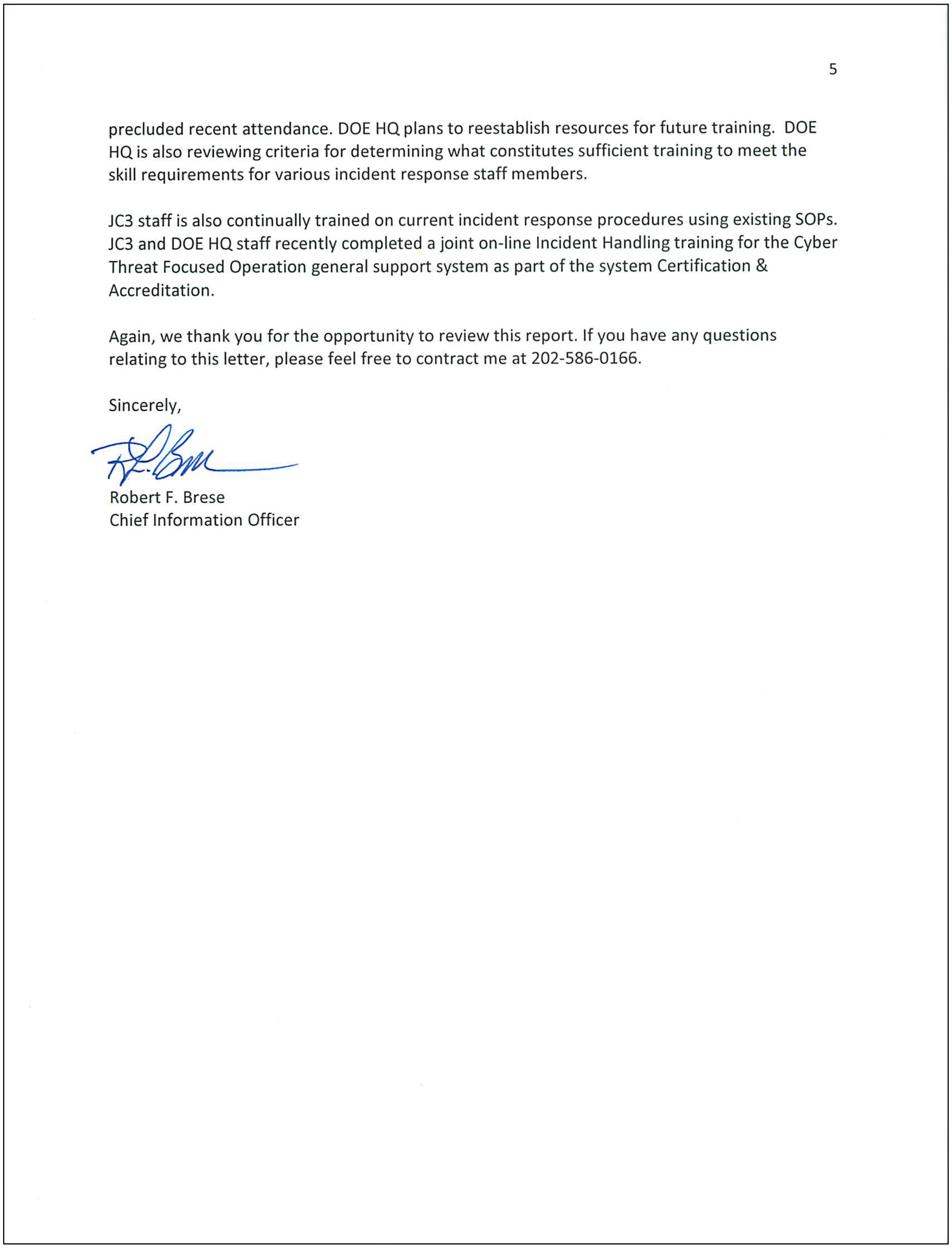
Several DOE organizations have documented incident containment procedures, including the DOE HQ and JC3 IR capability, which include the applicable procedures and Incident Response Standard Operating Procedures (SOPs). The JC3 offers guidance and consultation to DOE sites and organizations on all network security topics, including incident response.

Recommendation 3(b) - Update IR procedures to prioritize handling of incidents according to impact assessment:
The Department intends to include the prioritization of incident response according to impact as part of the evaluation of processes and procedures at the Departmental and DOE HQ levels. The Department will reach out to other Federal agencies to identify best practices in this prioritization and include these factors when updating incident categorization and prioritization as identified in Recommendation 1(b). DOE has established priorities for the reporting of incidents to the JC3 IR capability. At the DOE HQ, procedures for responding to incidents based on prioritization criteria are under review and will be developed following completion of the incident response review process.

Recommendation 4 – Implement full testing strategies for IR capabilities:
DOE HQ is currently reviewing the IR capability with a goal of designing and executing testing that is more focused on all aspects of IR. The Department, through the JC3, is re-establishing the Department-wide training exercises, known as Cyber Tracer, which are provided by cybersecurity and IR subject matter experts from our National Laboratories. These exercises, which are focused on increasing the knowledge and skills of Incident Responders across the DOE, were greatly scaled back in FY12 and FY13 due to resource constraints. The Department intends to sponsor multiple Cyber Tracer exercises per year of varying size and complexity, with the next one planned for FY14 Q4.

Recommendation 5 – Training of IR personnel:
DOE Order 205.1b requires the Departmental cybersecurity program to develop training that "enables personnel to fulfill their responsibilities in protecting DOE information and information systems." Pursuant to this directive, the Department will review incident response training practices in place at several DOE elements, as well as those in place at selected other Federal agencies. Guidance will be developed for DOE sites and programs on the best practices for implementing incident response training.

DOE HQ incident response staff currently undergo ongoing training on existing SOPs. DOE HQ staff have attended SANS Institute Cybersecurity Training, though resource constraints in FY14



precluded recent attendance. DOE HQ plans to reestablish resources for future training. DOE HQ is also reviewing criteria for determining what constitutes sufficient training to meet the skill requirements for various incident response staff members.

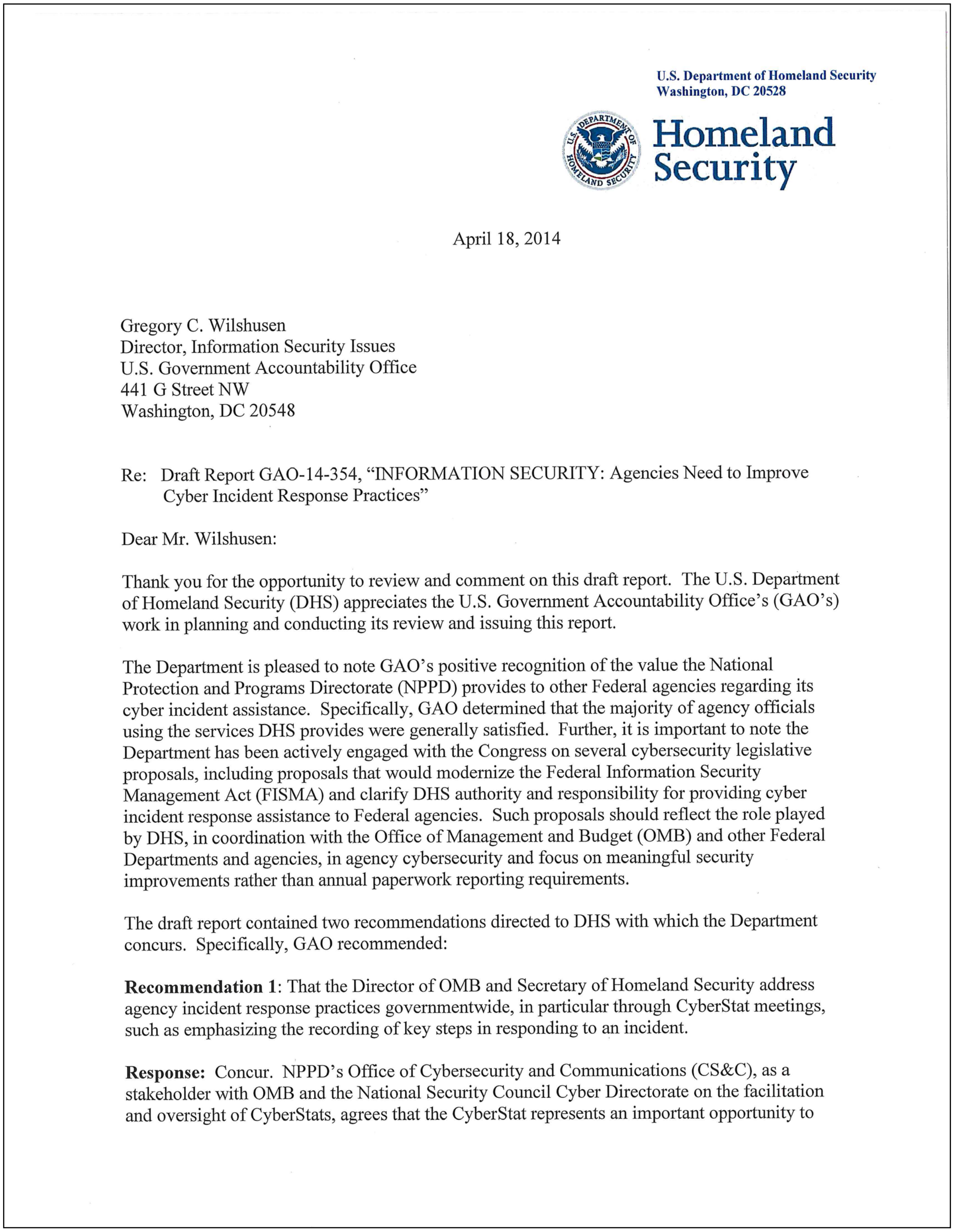
JC3 staff is also continually trained on current incident response procedures using existing SOPs. JC3 and DOE HQ staff recently completed a joint on-line Incident Handling training for the Cyber Threat Focused Operation general support system as part of the system Certification & Accreditation.

Again, we thank you for the opportunity to review this report. If you have any questions relating to this letter, please feel free to contract me at 202-586-0166.

Sincerely,

Robert F. Brese
Chief Information Officer

Appendix III: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

April 18, 2014

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Re: Draft Report GAO-14-354, "INFORMATION SECURITY: Agencies Need to Improve Cyber Incident Response Practices"

Dear Mr. Wilshusen:

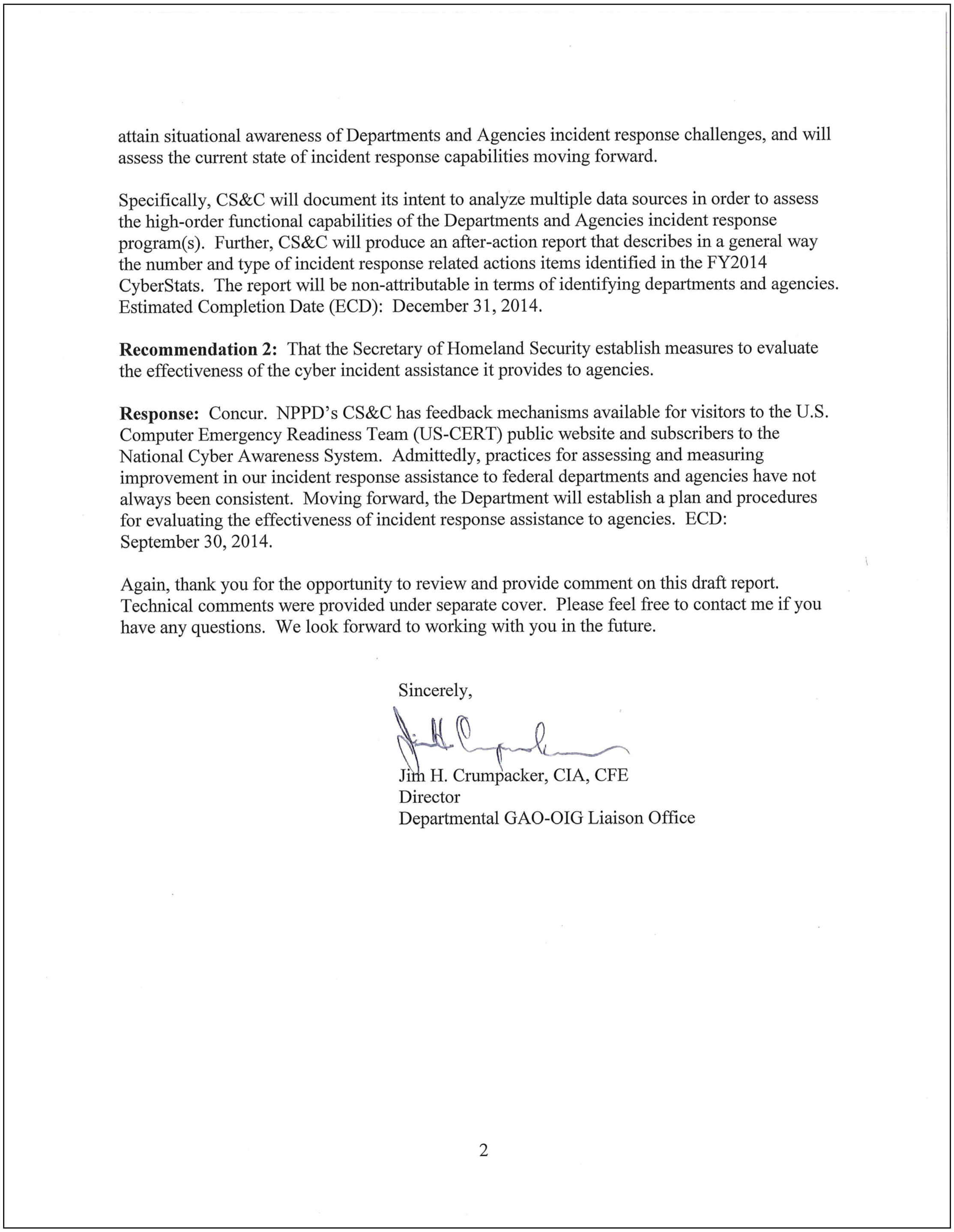
Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive recognition of the value the National Protection and Programs Directorate (NPPD) provides to other Federal agencies regarding its cyber incident assistance. Specifically, GAO determined that the majority of agency officials using the services DHS provides were generally satisfied. Further, it is important to note the Department has been actively engaged with the Congress on several cybersecurity legislative proposals, including proposals that would modernize the Federal Information Security Management Act (FISMA) and clarify DHS authority and responsibility for providing cyber incident response assistance to Federal agencies. Such proposals should reflect the role played by DHS, in coordination with the Office of Management and Budget (OMB) and other Federal Departments and agencies, in agency cybersecurity and focus on meaningful security improvements rather than annual paperwork reporting requirements.

The draft report contained two recommendations directed to DHS with which the Department concurs. Specifically, GAO recommended:

Recommendation 1: That the Director of OMB and Secretary of Homeland Security address agency incident response practices governmentwide, in particular through CyberStat meetings, such as emphasizing the recording of key steps in responding to an incident.

Response: Concur. NPPD's Office of Cybersecurity and Communications (CS&C), as a stakeholder with OMB and the National Security Council Cyber Directorate on the facilitation and oversight of CyberStats, agrees that the CyberStat represents an important opportunity to



attain situational awareness of Departments and Agencies incident response challenges, and will assess the current state of incident response capabilities moving forward.

Specifically, CS&C will document its intent to analyze multiple data sources in order to assess the high-order functional capabilities of the Departments and Agencies incident response program(s). Further, CS&C will produce an after-action report that describes in a general way the number and type of incident response related actions items identified in the FY2014 CyberStats. The report will be non-attributable in terms of identifying departments and agencies. Estimated Completion Date (ECD): December 31, 2014.

Recommendation 2: That the Secretary of Homeland Security establish measures to evaluate the effectiveness of the cyber incident assistance it provides to agencies.

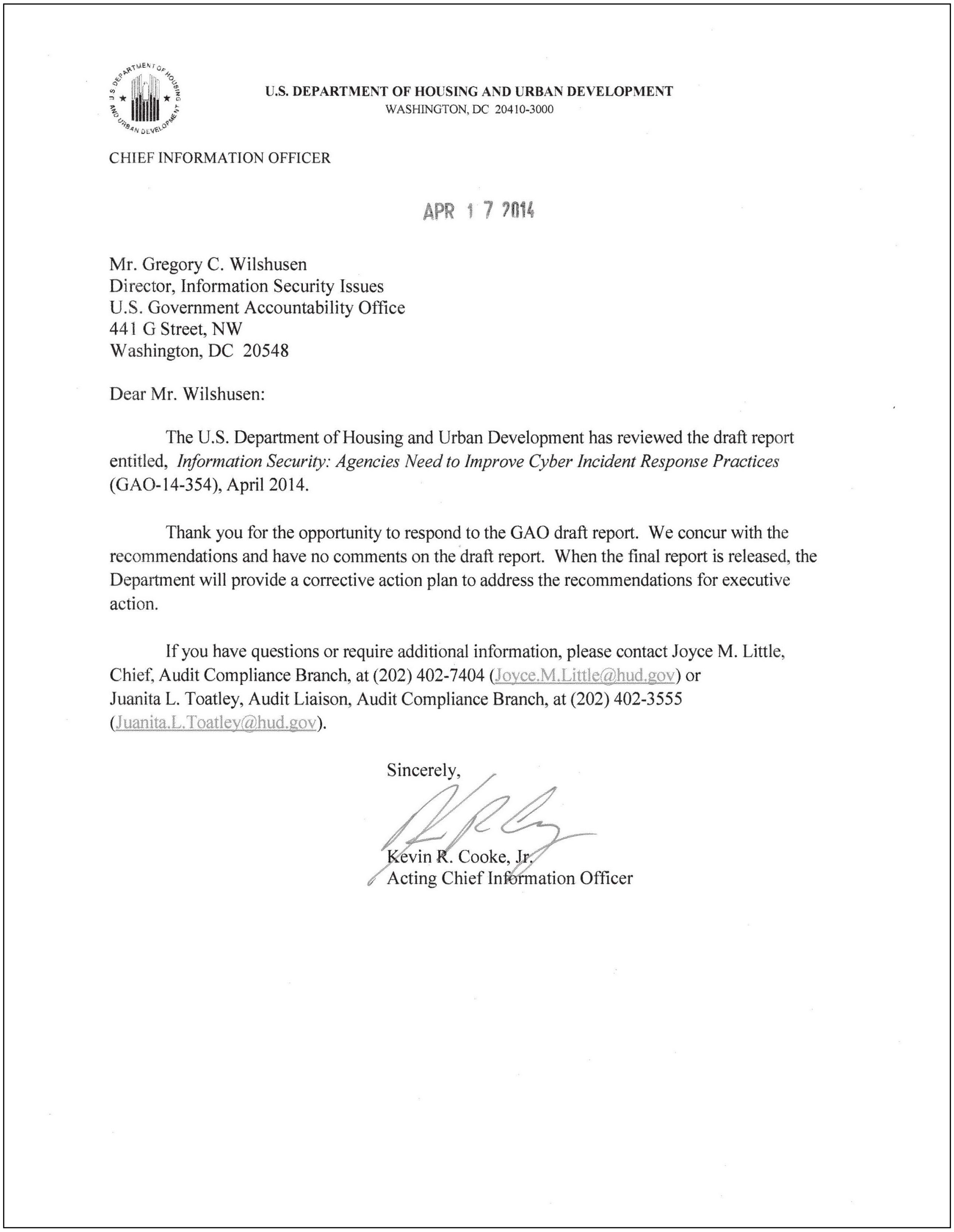
Response: Concur. NPPD's CS&C has feedback mechanisms available for visitors to the U.S. Computer Emergency Readiness Team (US-CERT) public website and subscribers to the National Cyber Awareness System. Admittedly, practices for assessing and measuring improvement in our incident response assistance to federal departments and agencies have not always been consistent. Moving forward, the Department will establish a plan and procedures for evaluating the effectiveness of incident response assistance to agencies. ECD: September 30, 2014.

Again, thank you for the opportunity to review and provide comment on this draft report. Technical comments were provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Appendix IV: Comments from the Department of Housing and Urban Development



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

APR 1 7 2014

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

The U.S. Department of Housing and Urban Development has reviewed the draft report entitled, *Information Security: Agencies Need to Improve Cyber Incident Response Practices* (GAO-14-354), April 2014.

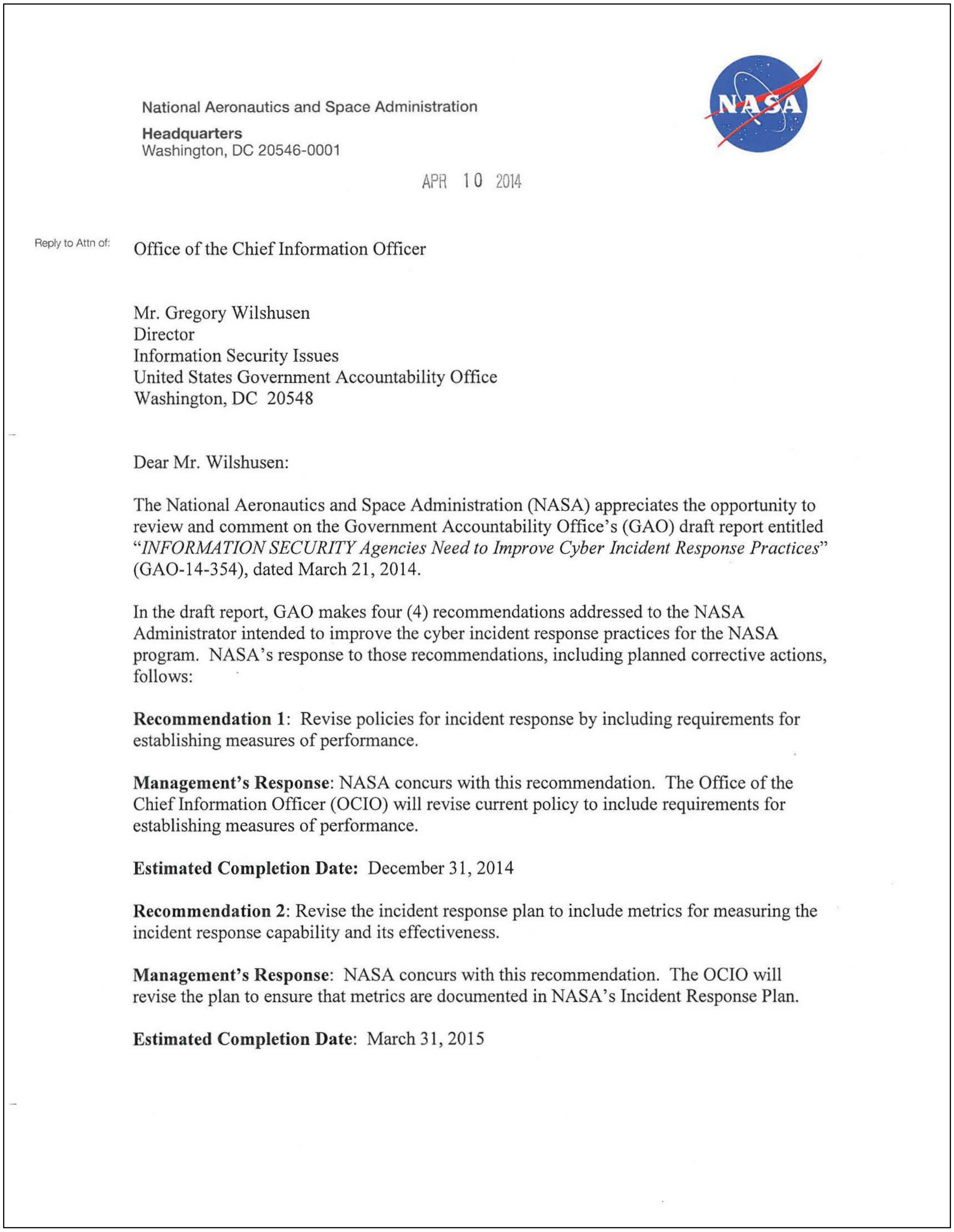
Thank you for the opportunity to respond to the GAO draft report. We concur with the recommendations and have no comments on the draft report. When the final report is released, the Department will provide a corrective action plan to address the recommendations for executive action.

If you have questions or require additional information, please contact Joyce M. Little, Chief, Audit Compliance Branch, at (202) 402-7404 (Joyce.M.Little@hud.gov) or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at (202) 402-3555 (Juanita.L.Toatley@hud.gov).

Sincerely,

Kevin R. Cooke, Jr.
Acting Chief Information Officer

Appendix V: Comments from the National Aeronautics and Space Administration



National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001

APR 10 2014

Reply to Attn of: Office of the Chief Information Officer

Mr. Gregory Wilshusen
Director
Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report entitled "*INFORMATION SECURITY Agencies Need to Improve Cyber Incident Response Practices*" (GAO-14-354), dated March 21, 2014.

In the draft report, GAO makes four (4) recommendations addressed to the NASA Administrator intended to improve the cyber incident response practices for the NASA program. NASA's response to those recommendations, including planned corrective actions, follows:

Recommendation 1: Revise policies for incident response by including requirements for establishing measures of performance.

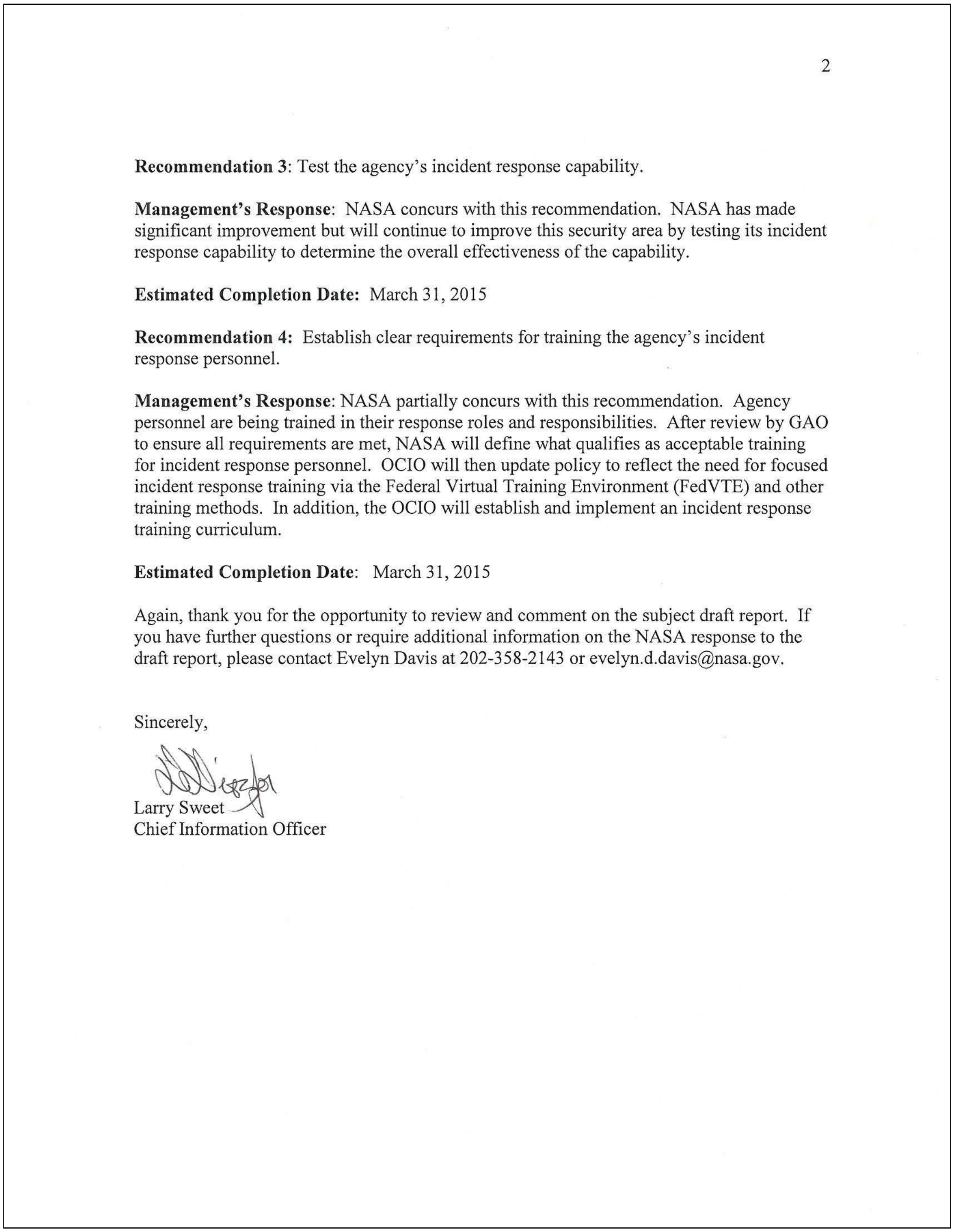
Management's Response: NASA concurs with this recommendation. The Office of the Chief Information Officer (OCIO) will revise current policy to include requirements for establishing measures of performance.

Estimated Completion Date: December 31, 2014

Recommendation 2: Revise the incident response plan to include metrics for measuring the incident response capability and its effectiveness.

Management's Response: NASA concurs with this recommendation. The OCIO will revise the plan to ensure that metrics are documented in NASA's Incident Response Plan.

Estimated Completion Date: March 31, 2015



Recommendation 3: Test the agency's incident response capability.

Management's Response: NASA concurs with this recommendation. NASA has made significant improvement but will continue to improve this security area by testing its incident response capability to determine the overall effectiveness of the capability.

Estimated Completion Date: March 31, 2015

Recommendation 4: Establish clear requirements for training the agency's incident response personnel.

Management's Response: NASA partially concurs with this recommendation. Agency personnel are being trained in their response roles and responsibilities. After review by GAO to ensure all requirements are met, NASA will define what qualifies as acceptable training for incident response personnel. OCIO will then update policy to reflect the need for focused incident response training via the Federal Virtual Training Environment (FedVTE) and other training methods. In addition, the OCIO will establish and implement an incident response training curriculum.

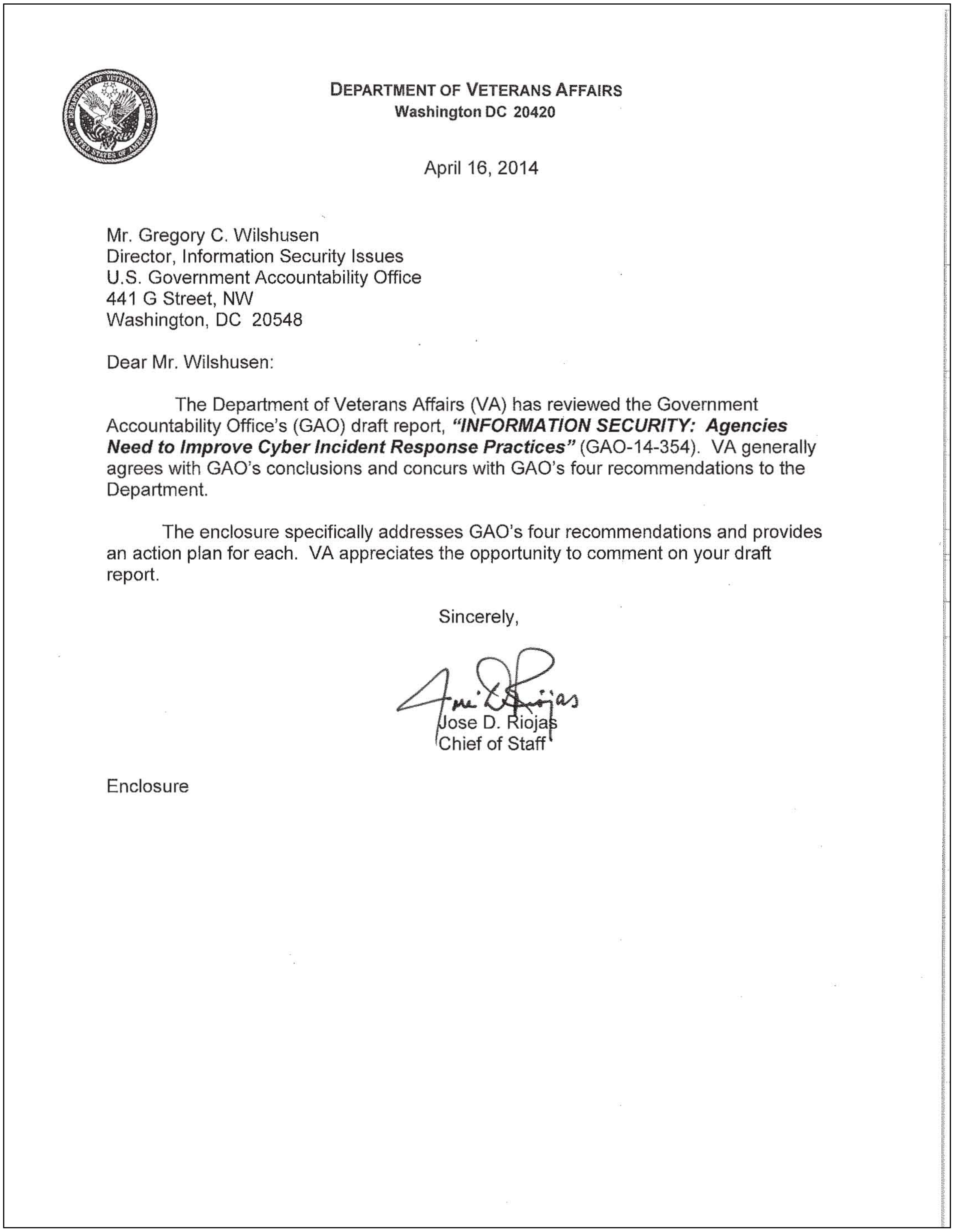
Estimated Completion Date: March 31, 2015

Again, thank you for the opportunity to review and comment on the subject draft report. If you have further questions or require additional information on the NASA response to the draft report, please contact Evelyn Davis at 202-358-2143 or evelyn.d.davis@nasa.gov.

Sincerely,

Larry Sweet
Chief Information Officer

Appendix VI: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
Washington DC 20420

April 16, 2014

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

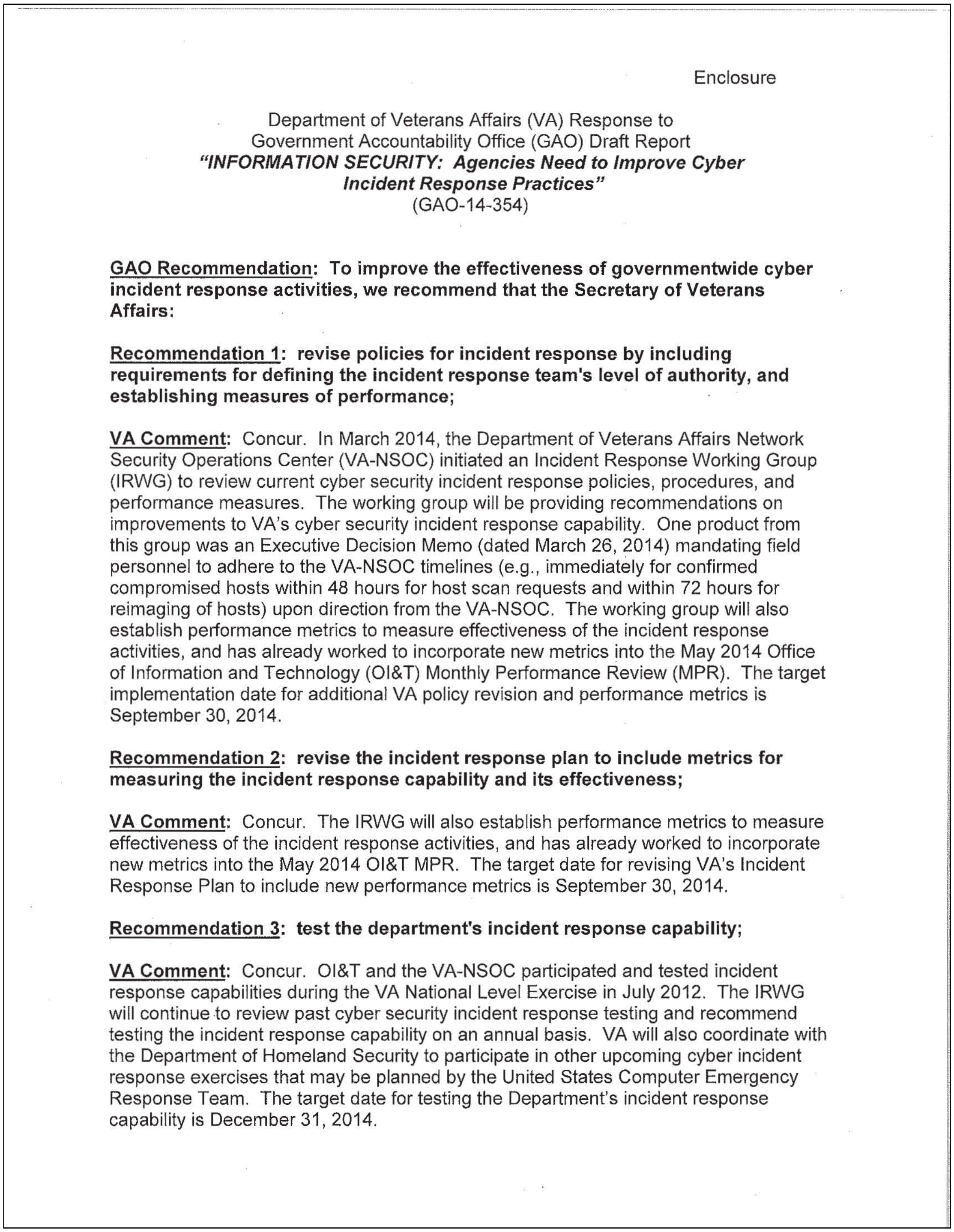
The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***"INFORMATION SECURITY: Agencies Need to Improve Cyber Incident Response Practices"*** (GAO-14-354). VA generally agrees with GAO's conclusions and concurs with GAO's four recommendations to the Department.

The enclosure specifically addresses GAO's four recommendations and provides an action plan for each. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Jose D. Riojas
Chief of Staff

Enclosure



Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
"INFORMATION SECURITY: Agencies Need to Improve Cyber Incident Response Practices"
(GAO-14-354)

GAO Recommendation: To improve the effectiveness of governmentwide cyber incident response activities, we recommend that the Secretary of Veterans Affairs:

Recommendation 1: revise policies for incident response by including requirements for defining the incident response team's level of authority, and establishing measures of performance;

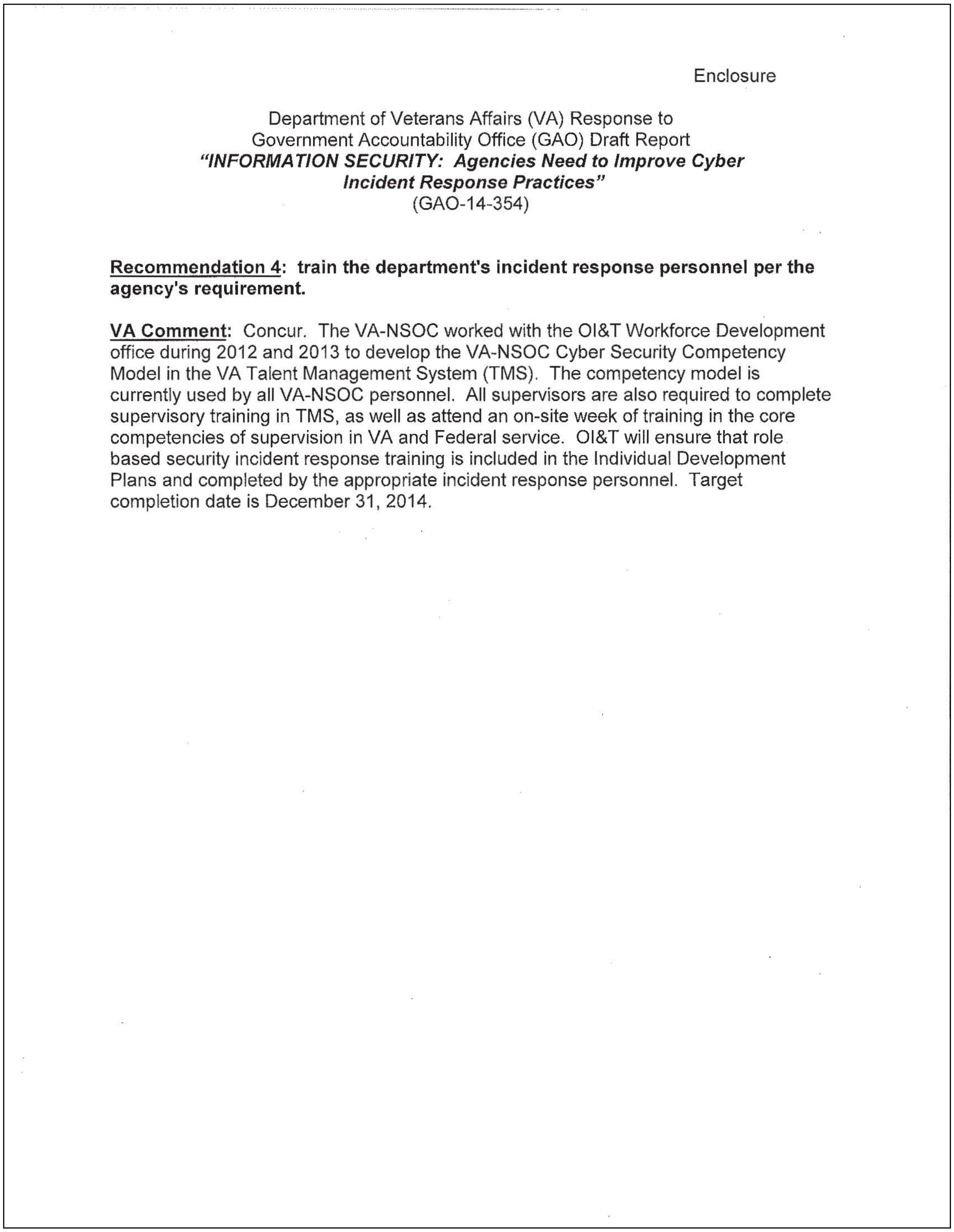
VA Comment: Concur. In March 2014, the Department of Veterans Affairs Network Security Operations Center (VA-NSOC) initiated an Incident Response Working Group (IRWG) to review current cyber security incident response policies, procedures, and performance measures. The working group will be providing recommendations on improvements to VA's cyber security incident response capability. One product from this group was an Executive Decision Memo (dated March 26, 2014) mandating field personnel to adhere to the VA-NSOC timelines (e.g., immediately for confirmed compromised hosts within 48 hours for host scan requests and within 72 hours for reimaging of hosts) upon direction from the VA-NSOC. The working group will also establish performance metrics to measure effectiveness of the incident response activities, and has already worked to incorporate new metrics into the May 2014 Office of Information and Technology (OI&T) Monthly Performance Review (MPR). The target implementation date for additional VA policy revision and performance metrics is September 30, 2014.

Recommendation 2: revise the incident response plan to include metrics for measuring the incident response capability and its effectiveness;

VA Comment: Concur. The IRWG will also establish performance metrics to measure effectiveness of the incident response activities, and has already worked to incorporate new metrics into the May 2014 OI&T MPR. The target date for revising VA's Incident Response Plan to include new performance metrics is September 30, 2014.

Recommendation 3: test the department's incident response capability;

VA Comment: Concur. OI&T and the VA-NSOC participated and tested incident response capabilities during the VA National Level Exercise in July 2012. The IRWG will continue to review past cyber security incident response testing and recommend testing the incident response capability on an annual basis. VA will also coordinate with the Department of Homeland Security to participate in other upcoming cyber incident response exercises that may be planned by the United States Computer Emergency Response Team. The target date for testing the Department's incident response capability is December 31, 2014.



Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
"INFORMATION SECURITY: Agencies Need to Improve Cyber Incident Response Practices"
(GAO-14-354)

Recommendation 4: train the department's incident response personnel per the agency's requirement.

VA Comment: Concur. The VA-NSOC worked with the OI&T Workforce Development office during 2012 and 2013 to develop the VA-NSOC Cyber Security Competency Model in the VA Talent Management System (TMS). The competency model is currently used by all VA-NSOC personnel. All supervisors are also required to complete supervisory training in TMS, as well as attend an on-site week of training in the core competencies of supervision in VA and Federal service. OI&T will ensure that role based security incident response training is included in the Individual Development Plans and completed by the appropriate incident response personnel. Target completion date is December 31, 2014.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jeffrey Knott (assistant director), Carl Barden, Larry Crosland, Kristi Dorsey, Nancy Glover, Wilfred Holloway, Kendrick Johnson, Stuart Kaufman, Tyler Mountjoy, Justin Palk, and Minette Richardson made key contributions to this report.

311304

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.