U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

OFFICE OF THE CHIEF INFORMATION OFFICER

Management Attention Is Needed To Assure Adequate Computer Incident Response Capability

Final Inspection Report No. OSE-16522/September 2004
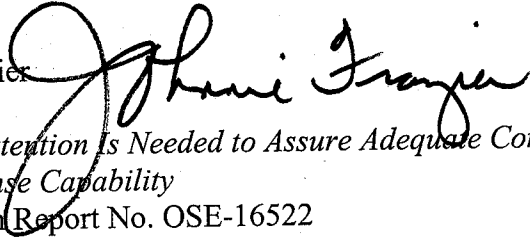
PUBLIC RELEASE

Office of Systems Evaluation

SEP 28 2004

MEMORANDUM FOR: Thomas N. Pyke, Jr.
Department of Commerce Chief Information Officer

FROM: Johnnie E. Frazier

SUBJECT: *Management Attention Is Needed to Assure Adequate Computer Incident Response Capability*
Final Inspection Report No. OSE-16522

This memorandum transmits our final report evaluating the Department's computer incident response capability. Agencies are required by the Federal Information Security Management Act (FISMA) to implement procedures for detecting, responding to, and reporting computer security incidents. Our report identifies improvements needed for better computer incident detection, response, and reporting throughout Commerce. Your written response to our draft report indicates that you agree with our findings and recommendations, and provides an action plan for addressing the recommendations.

Please ensure that your action plan is included in a plan of action and milestones (POA&M) to facilitate tracking of corrective actions in accordance with the Office of Management and Budget's FISMA guidance. If you have any questions regarding the report or the requested action plan, please contact me on (202) 482-4661 or Judith Gordon, Assistant Inspector General for Systems Evaluation, on (202) 482-5643.

We appreciate the cooperation and courtesies extended to us by your staff and by CIO office staff throughout the Department during our review.

Attachment

cc: Theodore W. Kassinger, Deputy Secretary, U. S. Department of Commerce
Otto Wolff, Chief Financial Officer and Assistant Secretary for Administration,
U. S. Department of Commerce

CONTENTS

Attachment: Department CIO's Response

EXECUTIVE SUMMARY

The Federal Information Security Management Act (FISMA)[1] requires agencies to review their information security program annually and Offices of Inspector General (OIGs) to conduct independent evaluations of those programs annually as well. Agencies are required by FISMA to implement procedures for detecting, responding to, and reporting computer security incidents.[2] Pursuant to FISMA, we evaluated the Department's computer incident response capability with a focus on the organizational structure, roles and responsibilities, and operating unit procedures for incident identification, analysis, response, and reporting.

The Department's information security policy establishes requirements for computer incident response as part of the overall information security program administered by the Department's Office of the Chief Information Officer (CIO). The policy requires all operating units to have a computer incident response capability (CIRC), defined as a set of formal mechanisms and procedures that allows an organization to react quickly, decisively, and consistently when an incident occurs. Any operating unit personnel may perform CIRC duties on an as-needed basis. An operating unit may also establish its own computer incident response team (CIRT), a formal group that performs intrusion monitoring and incident handling and reporting on a full-time basis. An operating unit that does not have its own CIRT receives support from the Department of Commerce CIRT (DOC CIRT), which resides in the Office of the Secretary.

Our evaluation found that the Department's distributed incident response structure is appropriate for the decentralized organization of the Department. However, improvements are needed to allow the Department CIO to obtain a Commerce-wide view of vulnerabilities and threats and ensure efficient and effective incident response throughout Commerce. Issues we identified include (1) the lack of a centralized entity to promote information sharing and consistency in response processes across the decentralized structure, (2) the absence of adequate incident response procedures in several units, (3) incomplete and inconsistent reporting of incidents by the operating units, and (4) the need for system administrators and IT security officers to improve their intrusion detection approaches and obtain additional specialized tools and training. Our specific findings are as follows.

The Department's Distributed Incident Response Structure Is Appropriate, but the Planned Coordination Mechanism Has Not Been Implemented. To support Commerce's decentralized and diverse organization, many of its computer incident response teams are organizationally part of the operating units as opposed to being centralized in the Department. While this permits these teams to have valuable technical and organizational knowledge of the units they serve, it also requires effective communication and coordination among the teams.

---

[1] Title III, E-Government Act of 2002 (P.L. 107-347).
[2] An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. The Department's definition of a reportable incident is presented on page 14.

Indeed, NIST guidance[3] on computer security incident handling points out that distributed teams should be part of a single centralized entity so that the incident response process is consistent across the organization and information is shared among teams. The Department CIO intended to establish what he termed a "CIRT federation" to achieve coordination and communication by July 2002. To date, however, the federation has not been implemented. Thus, coordination and communication regarding incident prevention and response do not occur systematically, and the Department CIO's ability to have an accurate Commerce-wide view of incidents and capabilities is hampered. (See page 5.)

Some Operating Units Lack Adequate Incident Response Procedures and Most Lack the Required Approvals. Having written incident response procedures is one of the most important tools for successfully handling incidents. The Department's policy requires all operating units to have formal response procedures and to submit them to the operating unit's CIO and the Department for review and approval. Despite the importance of procedures, 4 of the 10 operating units we reviewed, including the Office of the Secretary which houses DOC CIRT, do not have procedures that are detailed and complete enough to support effective incident response, 6 of the 10 units did not receive operating unit CIO approval for their procedures, and only 1 of the 10 units received approval by the Department CIO's office. The lack of adequate procedures is particularly troubling for DOC CIRT since it is the incident handling organization for the operating units without a formal CIRT. (See page 9.)

Operating Units' Incident Reporting Is Incomplete and Inconsistent. Reporting of incidents to the Federal Computer Incident Response Capability (FedCIRC) is required both by FISMA and Department policy, and analysis of reported incident data is an important way for the Department to gain a better understanding of its threats and vulnerabilities. However, few detected incidents are currently being reported. We found that one reason for inadequate reporting is that some operating units are unfamiliar with the Department's reporting requirements, and the Department has not enforced them. (See page 12.)

System Administrators and IT Security Officers Must Improve Their Intrusion Detection Approaches and Obtain Additional Specialized Tools and Training. Although incident detection can help prevent incidents or mitigate their effects, the necessary detection steps frequently are not taken. Incident prevention and detection can be facilitated by installing intrusion detection systems and reviewing log information on a regular basis. Our review identified weaknesses in the frequency and approach used to review log information from network devices. We found instances where log information was not reviewed, infrequently reviewed, or reviewed only on a monthly basis. We also found instances where large quantities of information were examined using visual inspection as opposed to automated tools. Furthermore, we found that most operating units identify few incidents, a consequence, in part, of poor incident detection techniques. Although some specialized security training is provided to system administrators, network administrators, IT security officers, and IT security staff who are responsible for responding to incidents and reviewing audit log information from network

---

[3] NIST's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems.

devices, this training is not systematic and does not ensure that staff members have the requisite knowledge and skills. (See page 16.)

We made numerous recommendations to the Department CIO including to define and implement an approach for achieving coordination and communication among the distributed incident response teams either through a CIRT federation or some other means, as well as for improving incident response procedures, reporting, and detection. (See pages 8, 11, 15, and 17.)

...

In his response to our draft report, the Department CIO concurred with our findings and recommendations, and described the corrective actions planned or underway. The response states that an approach for achieving coordination and communication among the Department's distributed incident response teams will be implemented by June 2005. It also states that model incident response procedures will be developed and the IT security policy and procedures will be revised to ensure prompt notification of the DOC CIRT and FedCIRC when incidents occur. The response further states that the policy will be revised and model procedures developed to address handling of network device log information, and appropriate tools to support this activity will be acquired. Training on the new policy and procedures will be provided for IT security officers and CIRT personnel, as appropriate. The implementation of these actions will be completed in FY 2005, and the Department's annual IT security compliance review program will be used to monitor compliance throughout Commerce. These actions are responsive to our recommendations and, when implemented, should improve incident detection and response. The CIO's complete response is included as an attachment to this report.

BACKGROUND

Information security threats have become more numerous and diverse, as well as more damaging and disruptive. New types of incidents are continually emerging, and not all incidents can be prevented. An effective incident response capability is essential for rapidly detecting incidents, minimizing losses, and restoring services.

The Federal Information Security Management Act (FISMA)[1] requires agencies to review their information security program annually and Offices of Inspector General (OIGs) to conduct independent evaluations of those programs annually as well. Agencies are required by FISMA to implement procedures for detecting, responding to, and reporting computer security incidents. Pursuant to FISMA, we evaluated the Department's computer incident response capability.

National Institute of Standards and Technology (NIST) Special Publication 800-61, *Computer Security Incident Handling Guide*,[2] points out that a computer security incident was previously thought of as a security-related adverse event in which there was a loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability, but recently new types of computer security incidents have emerged, necessitating an expanded definition of an incident. The guide defines an incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. The guide notes that the definition of a computer security incident has evolved.

Examples of incidents include (1) denial of service attack, which prevents or impairs the authorized use of networks, systems, or applications by exhausting resources; (2) introduction of malicious code, which could be a virus, worm, Trojan horse, or other code-based entity that infects a host; (3) unauthorized access, in which logical or physical access is obtained without permission to a network, system, application, data, or other resource; and (4) inappropriate usage, which is a violation of acceptable computing use policies.

Since even strong security controls may not prevent all incidents, an effective incident response capability is imperative. NIST guidance identifies the benefits of having an incident response capability as providing the ability to:

- Respond to incidents systematically so that the appropriate steps are taken,

- Help personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services,

---

[1] Title III, E-Government Act of 2002 (P.L. 107-347).
[2] NIST's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, is intended to assist organizations in mitigating the risks from information security incidents by providing practical guidance on responding to incidents effectively and efficiently.

- Use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data, and

- Deal properly with legal issues that may arise during incidents.

Departmental Policy on Computer Incident Response

The Department's information security policy entitled, *IT Security Program Policy and Minimum Implementation Standards,* establishes requirements for computer incident response as part of the overall information security program, which is administered by the Department's Office of the Chief Information Officer (CIO). The incident response portion of the policy covers such topics as:

- Definition of a reportable incident,
- Responsibility for developing the computer incident response capability (CIRC),
- Responsibility for approving and updating operating unit CIRC policies and procedures,
- Information to be provided to the Department on CIRC operating procedures,
- Actions required for monitoring and detecting incidents, and
- Requirements for reporting incidents to the Federal Computer Incident Response Capability (FedCIRC)[3].

The policy requires *all* operating units to have a CIRC, defined as a set of formal mechanisms and procedures that allows an organization to react quickly, decisively, and consistently when an incident occurs. Any operating unit personnel may perform CIRC duties on an as-needed basis. In addition, an operating unit may establish its own computer incident response team (CIRT), a formal group that performs intrusion monitoring and incident handling and reporting on a full-time basis. An operating unit that does not have its own CIRT receives support from the Department of Commerce CIRT (DOC CIRT), which resides in the Office of the Secretary. Such units must report incidents to DOC CIRT, which then notifies FedCIRC. Formally established operating unit CIRTs must report incidents directly to FedCIRC and send an information copy of the report to DOC CIRT. According to the policy, the required interface and exchange of information among CIRTs is called the DOC federated CIRT structure.

The policy identifies two positions in the Department CIO's Office that have significant responsibilities for establishing and maintaining an agency-wide computer incident response program. The Department's IT security program manager is responsible for issuing the policy and guidance that establish the framework for the Department-wide information security program, overseeing the program, and approving associated policy. The Department's critical infrastructure program manager is responsible for acting as the central point of contact for incident handling in concert with the Office of Security and OIG, ensuring the reporting of incidents to FedCIRC, and developing the Department's federated computer incident response program. In the operating units, the IT security officers serve as their units' focal point for handling all incidents and reporting. The IT security officers are also responsible for

---

[3] FedCIRC is the federal civilian agencies' focal point for computer security incident reporting, prevention, and response. It is located in the Department of Homeland Security.

coordinating with the Department's IT security program manager, critical infrastructure program manager, Office of Security, and OIG, as appropriate, concerning incidents, potential threats, and other concerns.

The Department's information security policy requires each operating unit IT security officer to develop standard operating policies and procedures for computer incident response. These policies and procedures are to be approved by the operating unit CIO and then submitted to the DOC critical infrastructure program manager for review and approval for integration into policies and procedures for the DOC federated CIRT. The Department's critical infrastructure program manager, in consultation with the IT security program manager, is to develop and approve all policies and procedures for operation of DOC CIRT and the DOC federation of CIRTs.

As noted previously, DOC CIRT supports those operating units that have not established a formal CIRT. Currently the following units are supported: Office of the Secretary (OS), International Trade Administration (ITA), Minority Business Development Agency (MBDA), Bureau of Industry and Security (BIS), Economics and Statistics Administration (ESA), Economic Development Administration (EDA), Technology Administration (TA), and OIG.

Units that have established their own CIRTs include: National Institute of Standards and Technology (NIST), Bureau of the Census, Bureau of Economic Analysis (BEA), National Oceanic and Atmospheric Administration (NOAA), National Technical Information Service (NTIS), National Telecommunications and Information Administration (NTIA), and United States Patent and Trademark Office (USPTO).

OBJECTIVES, SCOPE, AND METHODOLOGY

The purpose of this review was to evaluate the Department's computer incident response capability with a focus on the organizational structure, roles and responsibilities of DOC CIRT and federated CIRT, and operating unit policies and procedures for incident identification, analysis, handling, and reporting.

To satisfy our objective, we reviewed security incident response policies and procedures and incident reports for 10 operating units, as well as reporting of incidents by the operating units to DOC CIRT and FedCIRC. From the Department CIO's office we interviewed the director of the Office of Information Technology Security, Infrastructure, and Technology; IT security program manager; critical infrastructure program manager; and staff of DOC CIRT. We also interviewed the IT security officers and CIRT staff in the following operating units: BIS, Census, EDA, ITA, MBDA, NIST, NTIS, NOAA, and USPTO.

Our criteria included FISMA; NIST Special Publication 800-61, *Computer Security Incident Handling Guide*; *DOC IT Security Program Policy and Minimum Implementation Standards*; and Carnegie Mellon University/Software Engineering Institute, *Handbook for Computer Security Incident Response Teams.*

We conducted this evaluation in accordance with the Inspector General Act of 1978, as amended, and the Quality Standards for Inspections, March 1993, issued by the President's Council on Integrity and Efficiency. We performed our fieldwork from November 2003 to March 2004.

FINDINGS AND RECOMMENDATIONS

I. The Department's Distributed Incident Response Structure Is Appropriate, but the Planned Coordination Mechanism Has Not Been Implemented

To support Commerce's decentralized and diverse organization, many of its computer incident response teams are organizationally part of the operating units. While this permits these teams to have valuable technical and organizational knowledge of the units they serve, it also requires effective communication and coordination among the teams. To achieve communication and coordination, the Department CIO intended to establish what he termed a "CIRT federation" by July 2002. To date, however, a CIRT federation has not been established. Thus, coordination and communication regarding security incident prevention and response do not occur on a systematic basis, and the Department CIO's ability to have an accurate Commerce-wide view of incidents is hampered.

A. *A Distributed Structure Suits the Department's Decentralized Organization*

One of the initial steps in establishing an incident response capability is selecting the appropriate organizational structure. The Department has a distributed incident response structure. A distributed structure consists of multiple incident response teams located through out an organization, each being responsible for computer incidents within their area or physical/logical segment of the organization. Currently, all major Commerce operating units and some small units have their own incident response teams, as permitted by Department policy. Consistent with the policy, DOC CIRT has been established to support the Office of the Secretary, as well as the remainder of the units that do not have their own incident response teams. One of the activities performed by the DOC CIRT has been to communicate alerts on security issues and vulnerabilities received from FedCIRC and other sources to the operating units' IT security staff.

The Department is comprised of diverse operating units, each with different missions, network structures, system architectures, applications, intrusion monitoring technologies, and organizational issues. As NIST's *Computer Incident Handling Guide* observes, accurate analysis and prioritization of incidents are dependent on specific knowledge of the organization's environment. Because of the significant differences among Commerce's operating units, a distributed incident response structure positions each CIRT or CIRC to have specific technical and organizational knowledge of the unit it serves. According to NIST guidance, a distributed incident response structure is effective for large organizations and for organizations with major computing resources at distant locations, both of which are characteristics of Commerce. NIST guidance points out that distributed teams should be part of a single centralized entity so that the incident response process is consistent across the organization and information is shared among teams. This type of structure requires effective communication among the incident response teams and consistent practices for effective incident handling. Information sharing is particularly important because multiple teams may see components of the same incident or may handle similar incidents.

B. *The Federation of CIRTs Has Not Been Implemented*

To promote coordination and communication, the Department CIO made a commitment to establish a federated computer incident response capability by July 2002, and in a summary of accomplishments accompanying its FY 2003 FISMA report stated, "The Department's computer incident response capability was extended by the establishment of a Federated Computer Incident Response Capability to ensure integration, innovation, and cooperation in Department-wide incident prevention, response, and handling activities." The establishment of a federated capability was similarly reported in the Department's FY 2003 Performance and Accountability Report. However, to date, a federated capability has not been implemented. Thus, coordination and communication regarding security incident prevention and response do not occur on a systematic basis, and the Department CIO's ability to have an accurate Commerce-wide view of incidents is hampered.

A timeline depicting the events related to implementation of a CIRT federation is presented in table 1. In our March 2001 review of the Department's information security program, we noted the lack of an incident response capability at some operating units and recommended that all units have this capability. In its August 2001 review of information security within the Department, the Government Accountability Office[4] (GAO) made a similar recommendation. The Department CIO agreed to implement these recommendations and in an April 2002 memorandum to heads of operating units and CIOs, established a target date of July 2002 for the federation of CIRTs to be working together.

Table 1. Timeline of Events Related to CIRT Federation

Date	Event
March 2001	OIG report recommending ensuring all operating units have an incident response capability.[a]
August 2001	GAO report recommending establishment of Department-wide incident response capability.[b]
April 2002	Department CIO memorandum establishing target date of July 2002 for the CIRT federation to be working together and interconnected.
January 2003	Department's new information security policy issued defining at a high-level DOC CIRT and federated CIRT concept.
June 2003	Federation focus group formed to define a framework, mission, goals, and objectives for CIRT federation.
August 2003	Focus group white paper submitted to Department CIO.
November 2003	Focus group activities suspended by Department CIO.
[a]Office of Inspector General, *Additional Focus Needed on Information Technology Security Policy and Oversight,* OSE-13573, March 2001, U.S. Department of Commerce. [b]United States General Accounting Office, Information Security Weaknesses Place Commerce Data and Operations at Serious Risk, August 2001.	

---

[4] The Government Accountability Office was formerly called the General Accounting Office.

Following the Department CIO's memorandum, IT security staff from the Department and operating units worked together to define the federated incident response capability. Despite their efforts, minimal progress was made due to significant differences among the operating units and the Department in defining the roles, responsibilities, and operating structure for the federated CIRT. In an effort to resolve these differences, the Department CIO created a federation of CIRTs focus group.[5] In August 2003, this group completed a white paper containing preliminary recommendations entitled, "Framework for the Commerce Federation of Computer Incident Services," and submitted it to the Department CIO. The recommendations addressed the federation's operating framework, capabilities, services, and functions and were designed to achieve the following goals:[6]

- Create and maintain a Commerce-wide perspective of threats against the Department,

- Improve operating unit incident response capability by enhancing communications concerning attacks and compromises,

- Share information to more efficiently and effectively respond to computer security related incidents,

- Make resources available that would otherwise not be available to separately functioning CIRCs, and

- Continually enhance CIRCs' expertise to better support their constituencies.

The white paper stated that a "final draft" report was targeted for September 30, 2003. However, due to operating unit concerns with the recommendations, the Department CIO did not issue the report and suspended further focus group activities.

We believe the goals presented in the white paper are sound, and a CIRT federation having roles and responsibilities designed to achieve them would help the Department CIO attain a Department-wide view of threats and incident response capabilities and promote high quality and consistent incident response services throughout Commerce. However, a CIRT federation is not the only means to achieve these goals. For example, DOC CIRT could be given the responsibility and resources to become the coordinator and focal point for all the CIRTs, with responsibility for such functions as obtaining and providing to the CIO the Department-wide perspective, coordinating the sharing of information and resources, providing guidance and advice, and promulgating best practices to operating units.

The Department CIO needs to work with the operating unit CIOs to determine how best to achieve the goals presented in the white paper—be it through the CIRT federation or some other

---

[5] The Federation of CIRTs Focus Group includes security staff from the following: Census, EDA, MBDA, NIST, NOAA, USPTO, and the Departments CIO's office.

[6] White Paper, *Framework for the Computer Federation of Computer Incident Services (FOCIS), Preliminary Recommendations of the DOC Federation of Computer Incident Response Teams Focus Group,* August 31, 2003.

means—and ensure that the preferred approach is implemented and functioning effectively in a timely manner.

Recommendation

The Department CIO should develop a plan and schedule for defining and implementing an approach for achieving the goals presented in the CIRT focus group white paper.

II.   Some Commerce Operating Units Lack Adequate Incident Response Procedures and Most Lack the Required Reviews and Approvals

The Department's policy requires all operating units to have formal incident response procedures, whether or not they have a CIRT, and to submit these procedures to their operating unit CIO and then to the Department CIO's office for review and approval. The DOC critical infrastructure program manager, in consultation with the DOC IT security program manager, is to develop and approve all policies and procedures for operation of DOC CIRT and the CIRT federation. Procedures are needed to aid in the detection of incidents and to guide operating unit incident response personnel—system and network administrators and IT security officers—during security incidents. According to Carnegie Mellon University's Software Engineering Institute, having written incident response procedures is one of the most important tools for successfully handling incidents.[7]

Table 3 summarizes each operating unit's status for establishing procedures that are detailed and complete enough to support effective incident response, obtaining the approval of the unit's CIO, and obtaining Department approval. Four of the 10 operating units we reviewed, including the Office of the Secretary which houses DOC CIRT, lacked procedures that would support effective incident response; 6 of the 10 units did not receive operating unit CIO approval for their procedures; and only 1 of the 10 units received approval by the Department CIO's office.

The DOC CIRT's lack of adequate procedures is particularly troubling since it is the incident handling organization for the operating units without a formal CIRT. Although DOC CIRT gave us a document entitled, *Computer Incident Response Guidelines,* it provides policy but contains only minimal procedures. Moreover, developed in 1999, the document has not been updated or validated against the current information security policy of the Department, which has changed considerably over the past five years. In addition to DOC CIRT, Census, EDA, and MBDA either lacked documented procedures or had inadequate procedures. Census, which operates a CIRT, indicated it is developing formalized procedures, but could not provide a date for their completion. EDA's directive on incident response purports to provide policies and procedures for incident handling but contains only high-level steps for establishing a capability to do so. MBDA provided a draft document entitled, *IT Security Emergency Mobilization Plan,* dated March 2003; however, this plan only minimally addresses incident response procedures. MBDA's IT security officer stated that with the departure of its CIO in March 2004, many approved IT documents cannot be located.

The procedures we reviewed for the other operating units varied in detail and completeness. Some were highly formalized with flowcharts and checklists that team members are to use to handle an incident, while others had less formal procedures consisting of generic actions to perform during an incident.

Although Department policy requires review and approval of incident response procedures by each unit's CIO, only EDA, NIST, and NTIS's procedures have received such approval. Two

---

[7] Carnegie Mellon University, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*, CMU/SEI-2003-TR-001, October 2003.

operating units, BIS and NOAA, indicated that their incident procedures were approved.
However, BIS could not locate the approval memorandum signed by the BIS CIO or provide any
other evidence of CIO approval. NOAA's procedures were approved by its director of IT
security after NOAA's CIO delegated approval authority. However, the Department's security
policy does not provide for delegating this authority.

**Table 3. Incident Response Procedures and Approvals of Operating
Units Reviewed in this Evaluation**

Operating Unit	Procedures Documented	Procedures Approved by Operating Unit CIO	Procedures Sufficiently Detailed and Complete	Procedures Approved by Department
BIS	Yes	No[a]	Yes	No
Census	No	No	No	No
EDA	Yes	Yes[b]	No	No
ITA	Yes	No	Yes	No
MBDA	No[c]	No	No	No
NIST	Yes	Yes	Yes	No
NOAA	Yes	No[d]	Yes	No
NTIS	Yes	Yes	Yes	Yes
OS (DOC CIRT)	Yes	No	No	No
USPTO	Yes	No	Yes	No
[a]BIS indicated its procedures had been approved but could not locate the BIS CIO's approval memorandum or provide other evidence of CIO approval. [b]EDA did not have a CIO; however, it's procedures were approved by the deputy CIO and assistant secretary for economic development. [c]MBDA provided draft procedures. [d]NOAA's procedures were approved by NOAA's Director of IT Security.				

There is confusion as to which operating units are required to have their incident response
procedures approved by the Department. The Department CIO's office provided guidance to the
operating units that is not consistent with its information security policy: although the
Department's policy requires submission of *all* operating units' procedures for review and
approval, the guidance states that CIRTs established prior to the issuance of the policy in January
2003 do not have to submit their incident response procedures to the Department for review. If
this guidance were followed, the only CIRTs required to submit procedures would be those
created after the policy was issued—the CIRTs established by BEA, NTIA, and NTIS. Since the
Department's CIO is charged with protecting IT resources throughout the entire Department, we
believe that all operating units should be required to submit their procedures to the Department
CIO's office for review and approval.

The Department's security policy requires that the critical infrastructure program manager
review and approve operating units incident response procedures, but approval of NTIS's
procedures was granted by the IT security program manager. Differences between the security
policy and actual practice need to be reconciled.

In January 2004, NIST published new guidance on incident handling, Special Publication 800-61, *Computer Security Incident Handling Guide,* whose purpose is to assist organizations in establishing incident response capabilities and efficiently and effectively handling incidents. It addresses organizing an incident response capability, establishing incident response policies and procedures, and handling incidents from initial preparation through the post-incident lessons learned phase. To address the problems with current operating unit procedures and promote quality and consistency throughout Commerce, the Department CIO's office should use this guide as a basis for developing a set of procedures applicable to all operating units and DOC CIRT. While operating units should be permitted to tailor those procedures to specific requirements of their organizations, any changes should be reviewed and approved by the CIO of the unit, as well as the Department's IT security manager and critical infrastructure program manager.

Recommendations

The Department CIO should ensure the following:

1. A plan and schedule is prepared for developing incident response procedures in accordance with NIST Special Publication 800-61 for use by all operating units.

2. Any modifications made by an operating unit to the Department's incident response procedures are reviewed and approved by the unit's CIO and the Department's IT security manager and critical infrastructure program manager.

3. The Department's IT security policy reflects the changes to how incident response procedures will be developed and reviewed and any associated guidance is consistent with the policy.

III. Operating Units' Incident Reporting Is Incomplete and Inconsistent

Under FISMA and Department policy, FedCIRC must be notified of computer security incidents, and Department policy also requires DOC CIRT to be notified of incidents. Accurate reporting and analysis of incident data is an important way for the Department to gain a better understanding of its threats and vulnerabilities, as well as to identify actions and resources needed to better protect its sensitive information. In its guidance, NIST points out that a study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be used in the risk assessment process and may lead to the selection and implementation of additional controls.

However, reporting of computer security incidents by the operating units and DOC CIRT is incomplete and inconsistent, as shown in table 2. For operating units that do not have formally established CIRTs, the Department's policy requires DOC CIRT to report incidents to FedCIRC; units with formal CIRTs are to report incidents directly to FedCIRC and send a copy of the information to DOC CIRT. Of the 10 total incidents shown as detected in units without formal CIRTs in FY 2003, 8 were reported to DOC CIRT, but only 2 were reported to FedCIRC. Of the 809 total incidents detected in units with formal CIRTs, only 31 were reported to FedCIRC, with 679 reported to DOC CIRT. Thirty of the 31 incidents reported to FedCIRC were reported by USPTO and 677 of the 679 incidents reported to DOC CIRT were reported by NOAA.

Although NOAA accounts for nearly all of the incidents reported to DOC CIRT, we found the arrangement agreed to by the Department for NOAA's reporting problematic. The Department's policy requires preliminary reporting to DOC CIRT as soon as possible but no later than 24 hours after an incident is discovered; detailed reporting is required within 5 working days of the preliminary report. However, rather than sending specific incident reports, NOAA is permitted to provide DOC CIRT access to its incident database. As a result, DOC CIRT personnel are not explicitly notified of NOAA's incidents. Additionally, our interviews revealed that DOC CIRT personnel are not assessing the information available in NOAA's incident database. NOAA should be required to notify DOC CIRT when an incident occurs, and DOC CIRT should assess the incident information in NOAA's database.

The more than 70,000 incidents shown as detected by NIST and reported to FedCIRC in FY 2003 are actually raw data from NIST's network logs and sensors, which were given to FedCIRC for analysis under a special agreement. While providing this information to FedCIRC, NIST was not reporting specific incidents in accordance with Department policy. Therefore, the information on incidents shown as detected and reported for NIST in the Department's FY 2003 FISMA report is neither meaningful nor correct. NIST officials told us that they no longer send their log and sensor data to FedCIRC and are now providing specific incident reports to both FedCIRC and DOC CIRT. They also told us that in FY 2003, NIST had only one reportable incident, but stated they consider an incident reportable only when a compromise occurs, an interpretation not consistent with the Department's policy, as discussed later in this finding.

Table 2. Incidents Reported by Operating Unit in FY 2003 According to Department FISMA Reporting and DOC CIRT Records

Operating Unit	Number of Incidents Detected, As Reported in Department's 2003 FISMA Report	Number of Incidents Reported to FedCIRC, As Reported in Department's 2003 FISMA Report	Number of Incidents Reported to DOC CIRT, According to DOC CIRT Data
Operating Units Without Formal CIRTs			
BIS	2	2	1
EDA	0	0	1
ESA	1	0	0
ITA	2	0	1
MBDA	0	0	0
OS[a,b]	5	0	5
TA	0	0	0
Total:	10	2	8
Operating Units with Formal CIRTs			
BEA	2	0	0
Census	31	0	0
NIST	72,520[c]	70,952[c]	0
NOAA	677	0	677[d]
NTIA	5	1	2
NTIS	0	0	0
USPTO	94	30	0
Total:	809[e]	31[e]	679

[a]OS reporting includes OIG.
[b]DOC CIRT resides in OS.
[c]NIST used network log and sensor information to determine this number. However, NIST officials later told us that NIST had no reportable incidents according to definition in Department policy.
[d]NOAA provided DOC CIRT access to its incident database to obtain preliminary and detailed information concerning computer incidents.
[e]NIST not included in total. (See note c.)

Incident reporting is not a problem experienced only by Commerce. In its FY 2003 FISMA report to Congress, OMB noted that the federal government's incident prevention and management capabilities must be improved, including increased information sharing to rapidly identify and respond to cyber threats and critical vulnerabilities. OMB stated that it has a continuing concern regarding the timeliness and accuracy of incident reporting by agencies. OMB pointed out that less than full reporting makes trend analysis difficult and diminishes the ability to correlate ongoing attacks.[8]

Department's Definition of Reportable IT Security Incident

The Department's policy defines a reportable incident as any act that violates an explicit or implied security policy within the Department or its operating units. It further states that an incident is any adverse event that threatens the security of information resources. The policy states that incidents may include but are not limited to the events described below.

Event	Description
Compromise of integrity	A virus infects a system or network.
Denial of service attack	An attacker has disabled a system or a network worm has used all available network bandwidth.
Loss of accountability/ misuse	An intruder or insider uses an account or a system for unauthorized or illegal purposes.
Damage to any part of the system	A virus or disgruntled employee destroys data.
Compromise of confidentiality/intrusion	An unauthorized outsider gains access to your IT resources.

Source: *IT Security Program Policy and Minimum Implementation Standards,* U.S. Department of Commerce, January 24, 2003.

We found that one reason for inadequate reporting is that some operating units are unfamiliar with the Department's reporting requirements, and the Department has not enforced them. As shown in the box, the Department's policy defines reportable incidents, and does not limit them to events involving significant compromise. The Department's definition is the same as that of FedCIRC. Nonetheless, several of the CIRT representatives we interviewed stated they were required to report only incidents resulting in significant compromise. In addition, officials from two CIRTs told us they were not aware of the requirement to provide DOC CIRT with an informational copy of incidents that were reported to FedCIRC. Contributing to the reluctance of operating units to report incidents to DOC CIRT is the lack of a secure means of communications. The Department CIO needs to ensure that all operating units understand the reporting requirements, that a secure means of communications is made available, and a process is put in place for enforcing the requirement for all operating units to identify, track, and report incidents. Table 2 shows that few incidents were detected in most operating units. As discussed in finding V, we believe that weaknesses in unit incident detection approaches is one reason for this.

---

[8] Office of Management and Budget, *FY2003 Report to Congress on Federal Government Information Security Management*, March 1, 2004.

Recommendations

The Department CIO should ensure the following:

1. A formal process is developed to promptly notify DOC CIRT and FedCIRC when an incident occurs, and all operating units and DOC CIRT understand and comply with the Department's policy and process for reporting security incidents.

2. A plan and schedule are developed for implementing an infrastructure for secure communication among the operating units and DOC CIRT.

IV. System Administrators and IT Security Officers Must Improve Their Intrusion Detection Approaches and Obtain Additional Specialized Tools and Training

Although incident detection can help prevent incidents or mitigate their effects, the necessary steps to detect incidents frequently are not taken, including systematically reviewing logging information, preferably using automated tools. In addition, in order for the Department to build and maintain effective incident detection and response capabilities, greater attention must be given to ensuring that staff members responsible for these functions throughout Commerce receive appropriate specialized training.

A. *Intrusion Detection Approach Is Inadequate*

Although an effective incident response capability is essential, preventing incidents or detecting them before significant damage is done is clearly preferable. Prevention and detection can be facilitated by installing intrusion detection systems and reviewing log information on a regular basis. Our review identified weaknesses in the frequency and approach used to review log information from network devices. We found instances where log information was not reviewed, infrequently reviewed, or reviewed only on a monthly basis. We also found instances of log reviews where large quantities of information were examined using visual inspection as opposed to automated log reviews. Because of the large volume of information to be reviewed, this type of inspection approach can be extremely tedious, error prone, and ineffective in detecting malicious activity. We believe that poor incident detection is one reason for few incidents being identified by most operating units, as was shown in table 2.

The Department's IT security program policy requires that log information from perimeter intrusion detection systems be reviewed on a daily basis, and medium and high criticality servers on internal protected networks be reviewed on a weekly basis. It also requires that host-based intrusion detection systems be reviewed, although it does not specify how often. Frequent review of log information is essential in detecting malicious behavior. NIST guidance notes that organizations may receive thousands or millions of possible signs of incidents each day, recorded mainly by logging and computer security software and that automation is needed to perform an initial analysis of the data and select events of interest for human review. The guidance points out that event correlation software and centralized logging can be of great value in automating the analysis process, but that the effectiveness of the process depends on the quality of the data that goes into it. Thus, every operating unit needs to establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed according to the Department's policy. The Department CIO's office, in cooperation with the operating units, should evaluate the use of automated tools and data reduction techniques to increase log review efficiency and effectiveness in detecting malicious behavior, and consider the purchase of Department-wide licenses for such tools.

B. *Additional Specialized Training Is Needed*

Under the Department's policy, operating units must identify positions that require specialized training, as well as the specific requirements of that training. As we reported in our FY 2003 FISMA independent evaluation, progress in this area has been limited. We noted that training

for personnel with significant information security responsibilities, such as system administrators and IT security officers, appeared to be inconsistent and incomplete at the units we reviewed. In this review of incident response, we found a similar problem of incomplete and inconsistent training at the various operating units. Overall, we found that units had not identified training requirements for system administrators, network administrators, IT security officers, and IT security staff who are responsible for responding to incidents and reviewing audit log information from network devices. Although some specialized security training in these areas is provided, it is not systematic and does not ensure that staff members have the requisite knowledge and skills. Some operating unit officials attributed inadequate training to limited resources. The Department CIO, in conjunction with the operating units, needs to determine the requirements for specialized training in incident prevention, detection, and response and ensure that staff members responsible for these functions receive sufficient training, including periodic refresher training to keep abreast of ongoing changes to threats, vulnerabilities, and security measures.

Recommendations

The Department CIO should ensure the following:

1. Each operating unit follows the Department's policy for reviewing network device log information. This could be done, for example, by developing and requiring the implementation of a formal process for reviewing network device log information that
    a. Identifies the information to be analyzed and review procedures to be performed,
    b. Requires documentation of review findings, and
    c. Ensures that all operating unit IT security officers oversee the log review and evaluate the logs for actions performed by system administrators.

2. Available tools for automating audit log reviews are assessed and operating units implement those that are most appropriate. Consider purchase of a Department-wide license for appropriate tools.

3. Training requirements are defined and appropriate training is implemented for all IT staff with incident prevention, detection, and response duties, including periodic refresher training.

September 17, 2004

MEMORANDUM FOR   Judith J. Gordon
                             Assistant Inspector General for Systems Evaluation

FROM: Thomas N. Pyke, Jr.
                             Chief Information Officer

SUBJECT: Transmittal of Comments on Draft Inspection Report No. OSE-16522, *Management Attention Is Needed to Assure Adequate Computer Incident Response Capability*

Thank you for the opportunity to comment on the draft report evaluating the Department's computer incident response capability. We concur with your findings and recommendations, and the enclosure summarizes our ongoing and planned actions responding to the recommendations.

If you have questions regarding the attachment, please contact Nancy DeFrancesco, the Department's IT Security Program Manager, at (202) 482-3490.

Attachment

Attachment

<p style="text-align:center">Commerce Chief Information Officer Comments on
Draft Inspection Report No. OSE-16522
Management Attention Is Needed to Assure Adequate Computer Incident Response Capability</p>

Finding I.   The Department's Distributed Incident Response Structure Is Appropriate, but the Planned Coordination Mechanism Has Not Been Implemented

Recommendation: The Department CIO should develop a plan and schedule for defining and implementing an approach for achieving the goals presented in the CIRT focus group white paper.

Corrective Actions Planned/In Place:

The focus group that created the white paper will be re-convened as an Incident Handling Management Task Force no later than the end of September 2004, and will be charged with advising on revised policy, Department-wide procedures, and overall implementation, with an aggressive schedule, with full implementation scheduled for no later than June 2005.

Finding II.   Some Commerce Operating Units Lack Adequate Incident Response Procedures and Most Lack the Required Reviews and Approvals

Recommendations: The Department CIO should ensure the following:

1. A plan and schedule is prepared for developing incident response procedures in accordance with NIST Special Publication 800-61 for use by all operating units.

2. Any modifications made by an operating unit to the Department's incident response procedures are reviewed and approved by the unit's CIO and the Department's IT security manager and critical infrastructure program manager.

3. The Department's IT security policy reflects the changes to how incident response procedures will be developed and reviewed and any associated guidance is consistent with the policy.

Corrective Actions Planned/In Place:

1. The Department's FY 2004 IT Security Compliance Review Program includes review of operating unit policies and procedures for consistency with NIST SP 800-61. This effort is underway and on track for completion by September 30, 2004. Based in part on the results of this review and with the involvement of the task force, appropriate updates will be made to the Commerce IT Security Program Policy and Minimum Implementation by November 2004, and a Department "model CIRT procedures" document will be issued as guidance for Commerce operating units no later than January 2005.

2. Once the Department "model CIRT procedures" are established, the operating units will have the opportunity to develop or revise their CIRT operating procedures so they are consistent with these model procedures. The revised IT Security policy will require that any operating unit procedures that are not consistent with the model Department procedures be reviewed and approved by the operating unit CIO and the Department's IT security Program manager and, as appropriate, by the Department's Critical Infrastructure Program Manager.

3. The revised policy and model CIRT procedures and any associated guidance will be developed so as to be mutually consistent.

Finding III.   Operating Units' Incident Reporting Is Incomplete and Inconsistent

Recommendations: The Department CIO should ensure the following:

1. A formal process is developed to promptly notify DOC CIRT and FedCIRC when an incident occurs, and all operating units and DOC CIRT understand and comply with the Department's policy and process for reporting security incidents.

2. A plan and schedule are developed for implementing an infrastructure for secure communication among the operating units and DOC CIRT.

Corrective Actions Planned/In Place:

1. The revised policy and procedures will provide for prompt notification of incidents of the Department CIRT oversight staff and of FedCIRC. A training session for all IT security officers and CIRT personnel covering the CIRT-related IT Security policy and the Department model procedures will be held in FY 2005, and implementation will be monitored through the Department's annual Compliance Review Program.

2. The task force will address secure communication requirements, and a secure communications solution will be in place no later than April 2005.

Finding IV.   System Administrators and IT Security Officers Must Improve Their Intrusion Detection Approaches and Obtain Additional Specialized Tools and Training

Recommendations: The Department CIO should ensure the following:

1. Each operating unit follows the Department's policy for reviewing network device log information. This could be done, for example, by developing and requiring the implementation of a formal process for reviewing network device log information that

    a. Identifies the information to be analyzed and review procedures to be performed,

    b. Requires documentation of review findings, and

    c. Ensures that all operating unit IT security officers oversee the log review and evaluate the logs for actions performed by system administrators.

2. Available tools for automating audit log reviews are assessed and operating units implement those that are most appropriate. Consider purchase of a Department-wide license for appropriate tools.

3. Training requirements are defined and appropriate training is implemented for all IT staff with incident prevention, detection, and response duties, including periodic refresher training.

Corrective Actions Planned/In Place:

1. Network device log information handling will be addressed in the revised policy and model procedures, and appropriate tools will be selected and acquired to support this policy and these procedures by March 2005. Compliance monitoring will include this effort.

2. Available tools for automating audit log reviews will be assessed and operating units will implement those that are most appropriate supported by the task force during the

Attachment

development of the model procedures, with implementation no later than June 2005. Department-wide acquisition of these tools will be considered.

3. Requirements for training for CIRT staff will be determined, both for the short term and for periodic refresher training, with a training plan and schedule in place by March 2005.