U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

Office of the Secretary

Commerce Should Take Steps to Strengthen Its IT Security Workforce

Final Audit Report No. CAR-19569-1
September 2009

FOR PUBLIC RELEASE

Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

SEPTEMBER 30, 2009

MEMORANDUM FOR: Dennis F. Hightower
Deputy Secretary of Commerce

FROM: Dr. Brett M. Baker
Assistant Inspector General for Audit

SUBJECT: *Commerce Should Take Steps to Strengthen Its IT Security Workforce*

Final Audit Report No. CAR-19569-1

This memorandum transmits our final report on our audit of IT security workforce at the Department of Commerce. The purpose of the audit was to assess the Department's efforts to develop and maintain an effective IT security workforce to protect its IT systems.

In short, we found that the Department has not devoted sufficient attention to ensuring an adequate IT security workforce; performance management of the IT security workforce needs to be improved; and the IT security workforce lacks appropriate security clearances. We recommended actions the Department should take to address these deficiencies.

Your September 30, 2009, response to our draft report concurs with our audit findings and commits to addressing our recommendations immediately. We summarize the response in our audit report and have included it in its entirety as appendix D. We are pleased to note that the Department has already initiated steps to improve its IT security workforce.

In accordance with Department Administrative Order 213-5, please provide us with an audit action plan within 60 days of the date of this memorandum. Please accept our thanks to the Department and its operating units for the courtesies shown to us during our fieldwork. If you have any questions, please contact me at (202) 482-2600 or Chris Rose at (202) 482-5558.

cc.: John F. Charles, deputy assistant secretary for administration
Suzanne Hilding, chief information officer

Report In Brief

U.S. Department of Commerce Office of Inspector General

September 2009

Why We Did This Review

With the threat of cyber attacks looming over government and private-sector computer networks, the Department of Commerce has become increasingly concerned about the safety of its sensitive information.

The Office of Inspector General (OIG) initiated this audit to address the Department's need for an information technology (IT) security workforce with the skills to protect Commerce's IT systems against cyber attacks.

OIG assessed the Department's efforts to develop and maintain an effective IT security workforce because we have long identified information security as a top challenge for management.

Background

Our audit focused on the IT security personnel at nine Commerce operating units.

We scrutinized the IT security employees' specialized training, certification, security clearances, and professional development efforts.

Our sample consisted of ll information systems at the operating units. We chose systems that we believed the Department and operating units would place particular emphasis on staffing with experienced and trained professionals.

Department of Commerce IT Security Workforce

Commerce Should Take Steps to Strengthen Its Information Technology Security Workforce

What We Found

In our audit, we discovered that the Department needs to devote more attention to the development and guidance of its IT security personnel who protect the Department's sensitive computer systems and information.

- Few of the operating units we reviewed were taking the necessary steps to meet training requirements or keep accurate training records. Moreover, professional development plans were not generally used.
- On the whole, performance management and accountability need to improve. We found several instances in which IT security responsibilities were not included in employees' formal performance plans. Also, personnel with significant security roles were not always formally notified of their duties.
- Finally, we found that some IT security personnel in the operating units we audited did not have the level of security clearance Department policy requires. The IT security workforce on the front line of protecting the Department's assets should have levels of clearance commensurate with their responsibilities.

What We Recommend

To develop and maintain an effective IT security workforce, we recommend Commerce implement a Department-wide plan that will address the deficiencies identified in this audit. We advise Commerce to make necessary revisions to its current IT security policy to support the plan. The plan should include actions to

- enhance the professional development of personnel with significant IT security responsibilities, including developing and implementing a requirement for IT security certifications;
- identify essential training, ensure workforce members receive appropriate role-based and security awareness training, and track the training that has been taken;
- formally document the roles and duties of employees having significant IT security responsibilities and include IT security as a critical element in their performance plans; and
- provide appropriate security clearances for IT security personnel.

Contents

Introduction

When government computer networks come under cyber attack, whether by foreign governments, hackers, identity thieves, or terrorists, the consequences can be catastrophic. In response, the Department of Commerce and our nation as a whole have become increasingly concerned about protecting information technology (IT) systems and data.

This audit was prompted by the Department's need for a more skilled workforce with the experience necessary to protect its IT systems and information and the challenges it faces in achieving this goal. The Department uses more than 300 IT systems to meet its mission of creating economic growth and opportunity by promoting innovation, entrepreneurship, competitiveness, and stewardship.

OMB Circular A-130, *Management of Federal Information Resources,* directs federal agencies to protect government information commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. Consistent with Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems,* 32 of the Department's systems are considered high impact, because a security breach can be expected to have a severe or catastrophic impact on organizational operations, assets, or individuals. The Department's other systems are categorized as moderate impact if the potential adverse impact is serious and low impact if the potential adverse impact is limited.

Our audit focused on the workforce associated with the most sensitive unclassified systems in the Department, because these systems are highly critical to protect and should have the best trained and qualified workforce. We reviewed the IT security workforce responsible for 11 systems at nine Commerce operating units.[1] Not all operating units have high-impact systems, so in those cases we selected moderate-impact systems to get a broader sample of operating units.

We reviewed workforce in the following operating units:

- Bureau of Industry and Security (BIS)
- U.S. Census Bureau
- International Trade Administration (ITA)
- The National Oceanic and Atmospheric Administration's (NOAA) National Environmental Satellite Data and Information Service (NESDIS)
- National Institute of Standards and Technology (NIST)
- National Telecommunications and Information Administration (NTIA)

[1] Eight of the systems we reviewed were high impact; three were moderate impact.

- NOAA's National Weather Service (NWS)
- Office of the Secretary
- U.S. Patent and Trademark Office (USPTO)

As a result of our discussions with senior officials during the course of the audit, the Department has begun to take steps to address many of our findings. We detail the objectives, scope, and methodology of our audit in appendix A.

IT Security Workforce at the Department

The Department defines the roles and responsibilities of IT security positions in the *Department of Commerce 2009 Information Technology Security Program Policy*. IT security is a Department-wide responsibility; it is not solely the duty of the Department and operating unit chief information officers (CIOs) and their staffs. Commerce senior officials are responsible for the day-to-day management and general supervision of the security of information and technology associated with their programs and operating units. System owners are accountable for the security of the systems over which they have day-to-day management and operational control, including selecting appropriate security controls and ensuring that system users and support personnel have the appropriate security training.

Department and operating unit CIOs are charged with ensuring compliance with IT security requirements, developing and maintaining a bureau-wide information security program, ensuring the training of personnel with significant IT security responsibilities, and assisting senior agency program officials in carrying out their IT security responsibilities. To that end, CIOs are tasked with designating a senior information technology security officer (ITSO) to carry out the CIO's IT security instructions. In addition, each system has an information system security officer (ISSO) who works under the supervision of the system owner. The ISSO advises on the security considerations associated with the system and implements appropriate security controls. The Department was unable to provide a complete listing of officials with significant IT security responsibilities, but it was able to identify more than 600 such officials.

The roles defined by Commerce's IT security policy as having significant IT security responsibilities are in appendix B.

Strengthening the IT Security Workforce Is a Government-wide Challenge

OIG has identified information security as a management challenge for the Department since 2000. In our November 2008 top management challenges report,[2] we stated that the Department faces complex problems when putting proper information security controls in place. We noted that despite additional

[2] U.S. Department of Commerce, Office of Inspector General, November 2008. *Top Management Challenges Facing the Department of Commerce,* OIG-19384. Washington, D.C., p. 6.

expenditures to mitigate the problem, the Department has reported information security as a material weakness every year since FY 2001. A material weakness is a control deficiency or combination of deficiencies that in management's judgment should be reported outside the agency. These deficiencies represent significant weaknesses in the design or operation of internal control and could adversely affect the organization's ability to meet its internal control objectives.[3]

Cyber threats are a moving target, increasing in number and sophistication almost daily. This makes system security especially difficult. Our management challenges report observed that in order to be effective in this changing environment, the Department's IT security program must be staffed by professionals who have the appropriate skills and experience to implement required security controls, have the ability to assess the staff's effectiveness, and are able to anticipate and respond to emerging threats.

The need to strengthen the IT security workforce is a challenge for the entire federal government, not just the Department. Although the Department can take significant steps to improve its IT security workforce on its own, it is, like all federal agencies, hampered by an antiquated personnel system that impedes the hiring of the best qualified workforce. The Partnership for Public Service and Booz Allen Hamilton reinforce this point in their report on the federal cybersecurity workforce, stating, "[O]ne of the biggest problems with the process for hiring cybersecurity talent is the government's job classification system."[4]

At the same time, the *2008 (ISC)² Global Information Security Workforce Study,* a survey of the public- and private-sector workforce worldwide, states that current threats necessitate that "information security professionals must have the knowledge, skills and ability to properly address these challenges."[5] The study shows the levels of education for the cybersecurity workforce increasing—with over 90 percent in the Americas holding a bachelor's degree or higher.[6] Yet the only federal job classification specifically targeted toward IT security does not require a college degree.

During the past several years, several federal programs have been implemented to attract and retain highly-skilled, cyber-savvy individuals by sponsoring scholarships for students to pursue graduate or undergraduate degrees in the cybersecurity field. In return, scholarship recipients serve in the federal IT security workforce for a period of time. These programs include the Federal Cyber Service: Scholarship for Service, administered by the National Science Foundation in

[3] Revisions to OMB Circular A-123, *Management's Responsibility for Internal Control,* pp. 18-19.
[4] Partnership for Public Service and Booz Allen Hamilton, July 2009. *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce,* p. 9.
[5] A Frost & Sullivan White Paper Sponsored by the International Information Systems Security Certification Consortium, Inc. (ISC)², *The 2008 (ISC)² Global Information Security Workforce Study,* p. 5.
[6] *(ISC)² Global Information Security Workforce Study*, pp. 11-12.

partnership with the Department of Homeland Security and the Information Assurance Scholarship Program at Department of Defense (DoD).

In April 2009, Senators John D. Rockefeller (D-W.Va.), Olympia J. Snowe (R-Maine), Evan Bayh (D-Ind.), and Bill Nelson (D-Fla.) introduced draft legislation (Cybersecurity Act of 2009) requiring, among other things, all providers of cybersecurity services to federal agencies to be certified.[7] Although this legislation is still in committee, Congress's interest reflects a push to further professionalize the IT security workforce. Similar to the programs mentioned, the bill provides for scholarships for students to pursue graduate or undergraduate degrees in the cybersecurity field in return for federal IT security service.

[7] S.773, Senate Cybersecurity Act of 2009, April 2009. Sections 7 and 10.

Findings and Recommendations

I. The Department Has Not Devoted Sufficient Attention to Ensuring An Adequate IT Security Workforce

The Department has not devoted sufficient management attention and resources to ensuring it has an adequately skilled IT security workforce. We found deficiencies in

- the identification of training requirements,
- adequacy and timeliness of training received,
- evaluation of training effectiveness, and
- structured professional development of individual workforce members.

In many cases, the Department and its operating units have not complied with the Department's own IT security policies and procedures. Also, we found that IT security certifications are not required and are not consistently held by staff members. As a result of these factors, Commerce is at risk of not being satisfactorily prepared to protect its IT assets and information.

A. Professional IT Security Certifications Are Not Required and Are Not Consistently Held

Of the Department's IT security personnel, ITSOs and ISSOs have the most technically challenging responsibilities. However, about half of the ITSOs and ISSOs we covered in our review do not possess professional certifications. For the nine operating units we reviewed, only four ITSOs possessed relevant IT security certifications; for the 11 systems we reviewed, six ISSOs held relevant certifications. Section 4.2.2 of the Department's *Information Technology Security Program Policy* states that the "use of professional certification is at the discretion of each operating unit." Therefore, IT security certifications are not required by the Department.

Certifications demonstrate that an individual has "sought out the knowledge, skills, and abilities to defend an organization against possible breaches and build up defenses."[8] Moreover, certification requirements encourage personnel to strive to develop beyond their present levels of experience and maintain currency in their fields. Certifications thereby promote professional development and enhance employees' effectiveness in performing their roles within the organization.

[8] *(ISC)² Global Information Security Workforce,* p. 14.

In 2004, DoD issued a directive establishing a requirement for the credentialing and continuing education of personnel. DoD requires IT security professionals, regardless of occupational series, to obtain a commercial information security credential from a list of approved certifications. They must also maintain their professional certification through annual continuing professional education. This requirement applies to all applicable civilian, military, and contract employees. DoD established an aggressive timetable for full compliance by 2011. The DoD CIO office informed us that while Defense is making progress, it may not meet its target of 70 percent of its IT security work force—approximately 68,000 professionals—certified by the end of 2009.

In March 2009, the Government Accountability Office (GAO) testified that cybersecurity should be made a profession through testing and licensing. [9] The draft Cybersecurity Act of 2009 proposes to assign the development of a certification program to the Department of Commerce.

The *Cyber In-Security* report recommends that for cybersecurity professionals agencies "include a career path with opportunities to earn appropriate certifications."[10] We encourage the Department to take a leadership role in the federal CIO community to work with the Office of Personnel Management to establish more rigorous requirements for IT security professionals, including relevant educational requirements for entry-level positions and professional certification for advancement.

The Department does not have to wait for legislation to implement its own certification requirements. The Department's CIO, in consultation with the CIO Council, should develop certification requirements for Commerce's IT security professionals using DoD's program as a springboard. It should revise its IT security policy to, at a minimum, require certification for ITSOs, who have lead security responsibilities within the operating units, and ISSOs, who are on the front line protecting the Department's IT assets and information.

B. Few Operating Units Have Identified Role-Based Training Requirements

The Department's *Information Technology Security Program Policy* (Section 4.2.2) specifies that operating units must ensure significant information security roles (e.g., ITSOs, ISSOs, CIOs, authorizing officials) receive specialized training within the first 60 days from role appointment notification, and that refresher training must take place annually.

[9] GAO, March 2009. *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture,* GAO-09-432T.
[10] *Cyber In-Security*, p. 18.

We found that, of the nine operating units we reviewed, only the Census Bureau has specific requirements for the number of training hours and types of training needed, and NIST is working on requirements. Most operating units provided no information on the necessary initial training courses or annual refresher training. Without specified training requirements, operating units cannot assure appropriate, sufficient, or timely training. The Department should define a minimum set of training requirements, to be supplemented by the operating units to address their particular security concerns.

C. Many in the IT Security Workforce Do Not Regularly Receive Role-based Training

In our audit, we found that IT security professionals at four operating units had not received training for at least one year. Also, of the personnel we interviewed in the nine operating units covered in our audit, 35 percent (19 of 55) did not receive role-based training in FY 2007 or FY 2008.

The results of our FY 2007 and FY 2008 Federal Information Security Management Act (FISMA) review of role-based training further demonstrate the need for improvement (see appendix C). Lack of role-based training for IT security professionals goes beyond the operating units and systems included in our audit sample. Since training and education are the key factors in the competencies of IT security employees, it is a serious concern that so many do not receive regular role-based training.

D. IT Training Is Not Tracked Consistently

Human Resource Bulletin #076 on training policy requires each bureau to maintain and report accurate training data. In addition, it requires that as of December 10, 2007, Department of Commerce employees must use the Commerce Learning Center (CLC), a Web-based training resource, to initiate, approve, and record completed training. The CLC can identify classes that personnel are enrolled in, track assignments that have been submitted for instructor approval, and record courses and assignments staff members have completed.

Section 4.2.3 of the Department's *Information Technology Security Program Policy* "requires operating units to document and monitor individual information system security training activities including basic security awareness training and specific information system security training." The policy further states that "the [CLC] records documentation shall include the incumbent's name, role, type of training received, and the date when training was accomplished or date professional certification was verified." However, our audit found that CLC was not being used to track role-based training. Specifically, we found that:

1) six operating units use a database or Excel spreadsheet to track role-based training, and

2) three operating units have their employees track role-based training themselves.

We also identified concerns with the tracking of annual IT security awareness training for some Department employees. The CLC database did not have records showing completion of IT security awareness training for FY 2008 for almost 18 percent of our sample (out of 26 employees and 2 contractors, 5 did not have records in the CLC).

Operating units that leave the responsibility of tracking role-based training to their employees cannot ensure that the training records are accurate, timely, and consistent with the employee and organizational needs. A centralized system that identifies expected training, records completed training, and enables periodic review by management should be used to ensure the appropriate and timely training of IT security professionals.

E. The Effectiveness of IT Security Training Is Not Evaluated

Our audit found that training evaluation was not performed at the nine operating units we reviewed. Consequently, not only are IT security professionals not receiving training regularly, but Commerce management cannot determine how effective any training has been. Several operating units told us that obtaining training resources was difficult and that the quality of courses available from the CLC was inadequate, which raises the concern that IT security staff members are not receiving the most helpful training and the Department is not making the best use of its limited training budget.

NIST Special Publication (SP) 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* which provides guidelines for IT security training, states that course evaluation should be a component of an organization's IT security program. Evaluating courses measures the quality of the training programs being offered and ensures limited budget funds are not put toward ineffective training. If training content is incorrect, outdated, or inappropriate, the training will not meet the needs of the employees or the Department.

F. Professional Development Plans Are Not Generally Used

A development plan is a personal action plan that has been agreed to by the employee and supervisor. It identifies short- and long-term career goals, the training and other development experiences (such as completing relevant assignments or studying materials) needed to achieve those goals, and the time frame in which the plan is to be accomplished. Specifically, development plans

- identify and assess future developmental needs or competency areas,
- identify structured learning experiences linked to an organization's goals and objectives,
- establish agreed-upon developmental activities for the employee's career development,
- promote formal career development, and
- provide a means to fill employee and organizational competency gaps.

In addition, development plans can serve as a tool for collecting the cost information needed to establish a strategy for developing and enhancing the skills and experience of the Department's IT security workforce.

Of the nine Department operating units we reviewed, only the Office of Secretary and the Census Bureau consistently used individual development plans to guide the professional development of their IT security employees and remediate competency limitations or gaps. The other seven operating units infrequently used individual development plans. Officials at these seven units told us that plans for the employees' professional development were not documented, but that supervisors and employees discussed training during performance appraisals.

II. Performance Management of the IT Security Workforce Needs to Be Improved

Our audit found that IT security personnel were not always notified of their responsibilities in writing and that not all personnel with significant IT security roles had IT security as a critical element within their performance plans.

A. Employees with Significant IT Security Responsibilities Are Not Formally Notified of their Roles on a Consistent Basis

Section 4.2.2 of the Department's *Information Technology Security Program Policy* states that for personnel with significant information security roles, role notification must be made within the first 10 business days of appointment. Section 3.3.1 of the policy directs operating unit CIOs to appoint in writing an ITSO to implement the bureau's IT security program. However, the Department's policy does not specify how staff holding other IT security positions are to be notified of their roles and responsibilities.

Our audit found that ITSOs did not consistently receive formal written notification of their roles. We found no written notification for ITSOs at the Census Bureau, NESDIS, and NIST. We found a similar lack of written notification for ISSO positions for specific systems at NWS and USPTO**,** and the written notification of

the ISSO position for a NESDIS system was updated during our audit. While the Department's IT security policy only requires written notification for ITSOs, formally communicating duties to all personnel having significant IT security responsibilities would not only be an effective practice for ensuring they are aware of their responsibilities, but would also establish an audit trail of management's delegation of accountability.

B. Performance Plans Do Not Always Contain IT Security Performance Elements

Department Administrative Order 202-430, *Performance Management System*, establishes Commerce's performance management system for general schedule employees. The order states, "[P]erformance plans are the documentation of performance expectations communicated to employees by supervisors. Plans define the critical elements and the performance standards by which an employee's performance will be evaluated."

The GAO states[11] that "performance evaluation and feedback … should be designed to help understand the connection between employee performance and the organization's success."

Although Department employees were provided regular performance appraisals, we found several instances in which IT security responsibilities were not included in their performance plans. With constantly evolving cyber security threats, protecting the Department's IT assets and information is a critical part of all employees having significant IT security responsibilities. Therefore, performance expectations for IT security should be included as a critical element in employees' performance plans and staff should be held accountable for their performance.

III. The IT Security Workforce Lacks Appropriate Security Clearances

Section 4.13.2 of the *Department of Commerce Information Technology Security Program Policy* states that operating unit ITSOs are required to have a top secret/sensitive compartmented information (TS/SCI) clearance, and a sufficient subset of support staff is required to have a secret clearance.

Our audit found that ITSOs did not always have the level of security clearance that the Department's policy requires. Based on information provided by the Office of Security, we found that eight of nine ITSOs did not have TS/SCI clearances, and three of nine ISSOs did not have secret clearances. Lack of appropriate clearances limits the ability of these employees to obtain complete information on current cybersecurity threats and vulnerabilities and can reduce their effectiveness in

[11] GAO, November 1999. *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1.

protecting the Department's IT assets and information. ISSOs, who are on the front line of protecting the Department's information assets, should have at least secret-level clearances.

Conclusion

The Department has not been taking the necessary steps to develop and maintain an effective IT security workforce able to combat the cyber threats that continue to increase in both number and complexity.

Our audit found that Department management has not devoted sufficient attention and resources to identifying training requirements, ensuring adequacy and timeliness of training, evaluating training effectiveness, and structuring professional development. We also found a lack of formal assignment of accountability for IT security and inconsistent efforts toward securing appropriate clearances for IT security personnel. Moreover, the Department and its operating units have not complied with the Department's IT security policies and procedures. As a result, Commerce is at risk of not being satisfactorily prepared to protect its IT assets and information.

We are particularly concerned with the weaknesses found among the IT security workforce responsible for high-impact systems, because a security breach would have a severe impact on these systems. The Department and several operating units cite a lack of resources as a major impediment to providing adequate training for IT security personnel. This makes it particularly important for the Department to establish risk-based training priorities and develop a plan for ensuring adequate IT security workforce training.

Initial focus should be placed on strengthening the segment of the workforce responsible for securing the systems that, if compromised, would pose the greatest threat to the Department's ability to meet its mission, safeguard its assets, and protect its information. This risk-based approach would start with training the workforce responsible for high-impact systems and a prioritized set of moderate-impact systems. However, even the workforce associated with low-impact systems needs to be well qualified and trained because vulnerabilities in these systems can be used to stage attacks on high- and moderate-impact systems on the same network, including systems outside the Department of Commerce.

In its September 30, 2009, response to our draft report, the Department agreed with our audit findings and made a commitment to address our recommendations immediately. The Department's Office of the Chief Information Officer is partnering with the Office of Human Resources Management to develop an IT security workforce improvement program.

Recommendations

To develop and maintain an effective IT security workforce, we recommend Commerce establish and implement a Department-wide plan that addresses the deficiencies identified in this audit. The plan should include actions to:

1. enhance the professional development of personnel with significant IT security responsibilities, including developing and implementing a requirement for IT security certifications for, at a minimum, ITSOs and ISSOs;

2. identify essential role-based training and security awareness training, ensure workforce members receive appropriate training, and track the training that has been taken;

3. ensure the individual professional development of members of the IT security workforce;

4. formally document the roles and duties of employees having significant IT security responsibilities, and include IT security as a critical element in their performance plans;

5. provide security clearances commensurate with IT positions and responsibilities;

6. identify the resources and time frame needed to implement the plan; and

7. make necessary revisions to the Department's IT security policy to support the plan.

Other Matters

Developing and maintaining an effective IT security workforce is a government-wide issue. Therefore, we encourage the Department's CIO to take a leadership role on the Federal CIO Council to work with the Office of Personnel Management to reassess the position requirements for the IT security workforce with the goals of better defining duties and responsibilities, establishing certification requirements, and professionalizing the workforce through appropriate educational requirements.

Summary of Agency Response and OIG Comments

In responding to the draft report, the Deputy Secretary of Commerce agreed with the report findings, particularly those pertaining to professional development, performance management, and security clearances. The Deputy Secretary also expressed the Department's commitment to taking immediate action based on our recommendations. The Department's Office of the Chief Information Officer is partnering with the Office of Human Resources Management to develop an IT security workforce improvement program. We support this partnership.

Where appropriate, we modified this report to incorporate comments from other agencies. Based on NIST's remarks, we clarified our position that management and the CIO share responsibility for ensuring IT security training. NIST also feels that we should remove the recommendation that Commerce take a leadership role in the Federal CIO Council to address workforce issues, as the Department is currently represented at the Federal IT Workforce committee. We should note in response that our suggestion was not a formal recommendation; however, if the Department shares any best practices or lessons learned as it corrects its own workforce issues, other agencies would benefit from our experiences.

BEA cautioned that if a TS/SCI clearance becomes mandatory, the requirement must be properly worded in vacancy announcements. Our report notes that TS/SCI clearance is already a requirement, but it is not being followed. We suggest the Department consider BEA's suggestion in its plans to address the recommendations contained within the report. See appendix D for complete agency comments.

We are encouraged that steps have already been initiated to address our recommendations, and we look forward to the Department's action plan that will provide details on the corrective actions to be taken.

Appendix A: Objectives, Scope, and Methodology

The objective of our audit was to assess the Department's efforts in developing and maintaining an effective IT security workforce to protect its systems and data. We self-initiated this audit in February 2009 because we recognized the continued threats to the Department's computer networks, and we have long identified IT security as a top management challenge.

Our review focused on systems identified as high and moderate impact because security breaches of those systems would have the greatest negative impact on the Department. We expected the Department and its operating units to place particular emphasis on ensuring these systems were staffed with experienced and trained professionals.

Specifically, we reviewed the training and professional development, accountability, and security clearances of IT security personnel responsible for eight high-impact systems at operating units that had high-impact systems, and at three moderate-impact systems for operating units that lacked high-impact systems. We performed a non-statistical random sample of the Department's more than 300 systems, of which 32 are high-impact. We initially selected the operating units with high-impact systems and, in cases in which they had more than one such system, we randomly selected the system(s) to be reviewed. To broaden our coverage, we judgmentally selected three additional operating units. For each of these operating units, we randomly selected a moderate-impact system to include in our review.

We obtained an understanding of internal controls through interviews with 55 employees from the Department's Office of Chief Information Officer and officials at nine operating units (BIS, Census, ITA, NESDIS, NIST, NWS, NTIA, Office of the Secretary, and USPTO). In addition, we collected and reviewed information on IT security personnel, including their job series, annual performance plans, professional development plans, receipt of IT security awareness or role-based training, and level of security clearance.

We held our entrance conference at the Department's CIO Council meeting in February 2009 and briefed the Council again on the status and results of our audit work on June 26, 2009. We also had several meetings with the Office of the Chief Information Officer to keep it informed on the results of our work.

To assess the reliability of the data from the CLC, we selected a sample of employees for 2008 and 2009. We found that the CLC database did not always have accurate information; therefore, we did not rely on the computer-processed data for the purposes of our audit.

We reviewed the Department's compliance with applicable provisions of pertinent laws and regulations, including:

- Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 *et seq*;
- OMB Circular A-130, *Management of Federal Information Resources;*
- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- NIST SP 800-50, *Building An Information Technology Security Awareness and Training Program*
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;
- NIST SP 800-16*, Information Technology Security Training Requirements: A Role- and Performance-Based Model*;
- *Department of Commerce Information Technology Security Program Policy* introduced by the CIO on March 9, 2009;
- *Department of Commerce Information Technology Security Program Policy and Minimum Implementation Standards* issued on June 30, 2005;
- Department of Commerce Department Administrative Order 202-430, *Performance Management System;* and
- GAO's *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1).

Our audit findings report on instances in which policies and procedures were not met. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides 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.

We conducted our review from February 2009 through September 2009 under the authority of the Inspector General Act of 1978 and Department Organization Order 10-13. We performed our work at the Department of Commerce headquarters in Washington D.C.; NIST in Gaithersburg, Maryland; NWS in Silver Spring, Maryland; the Bureau of Census in Suitland, Maryland; and USPTO in Alexandria, Virginia.

Appendix B: Significant Information System Security Roles and Responsibilities

Commerce Position	Role
Chief Information Officer	Designates a senior information security officer; develops and maintains information security policies, procedures, and control techniques; and trains and oversees personnel with significant information security responsibilities.
Chief Information Security Officer	Designates a senior information security officer; develops and maintains information security policies, procedures, and control techniques; and trains and oversees personnel with significant information security responsibilities.
Operating Unit Chief Information Officer	Provides the overall management, leadership, and direction to operating unit security programs, including training and overseeing personnel with significant responsibilities for IT security and appointing an ITSO in writing.
Operating Unit Information Technology Security Officer	Has the lead responsibility for IT security within the organization.
Information System Security Officer	Ensures the appropriate operational security posture is maintained for specific information systems.
Authorizing Official	Assumes responsibility for operating information systems at an acceptable level of risk by granting an authorization to operate. Authorizing officials may be line officials or CIOs.
Information Owner/Information System Owner	A line office official responsible for deciding access to the information system and ensuring that system users and support personnel receive the requisite security training.

Commerce Position	Role
Certification Agent	Is responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system, to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting system requirements.
IT Security Incident Response Personnel	Are responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, coordinating incident response activities, and interacting with the Federation of Computer Incident Response Teams and others to disseminate reasoned and actionable cyber security information.
Key Contingency Roles	Are officials identified in Continuation of Operations, disaster recovery, and IT contingency plans that are responsible for ensuring respective plans are maintained, tested, integrated with other plans, adequate in scope, and relevant.

Appendix C: IT Security Employees Who Received Role-based Training in FY 2007 and FY 2008

Operating Unit Reviewed for FISMA	Employees Requiring Role-based Training	Employees Who Received Role-based Training [a]	Percentage (%) of Employees Who Received Role-based Training
Operating Units Examined in FY 2007			
USPTO Patents	147	84	57
NIST	131	99	76
NOAA/NOS	31	8	26
NTIS	27	23	85
EDA	4	4	100
Operating Units Examined in FY 2008			
NOAA/NESDIS	62	38	61
BIS	8	4	50
BEA	3	3	100
USPTO Trademarks	3	3	100

Source: 2007 and 2008 OIG FISMA Reports

As reported in OIG's FY 2007 and FY 2008 FISMA evaluations

Appendix D: Full Text of Agency Response

THE DEPUTY SECRETARY OF COMMERCE
Washington, D.C. 20230

SEP 30 2009

MEMORANDUM FOR: Dr. Brett M. Baker
Assistant Inspector General for Audit

FROM: Dennis F. Hightower

SUBJECT: Draft OIG Report: *Commerce Should Take Steps to Strengthen Its IT Security Workforce (#CAR-19569-1)*

Thank you for the opportunity to comment on the IT security workforce audit. The Department of Commerce (Department) takes efforts being made to identify areas for improvement in cybersecurity very seriously, and we are in agreement with the report's findings—particularly in the areas of professional development, performance management, and security clearances.

Recently, the Department made advances in technical security and improvements in our security processes; however, we also recognize that people are the key to long term success and that, consequently, more work needs to be done to improve our IT security workforce. We are committed to take immediate action based on your recommendations.

Attached is a list of comments and suggestions provided by the Department's operating units. I appreciate the effort your staff put into the report, and I hope that the recommendations lead to improvements in the Department's IT security posture.

Enclosure

Cc: John F. Charles, Deputy Assistant Secretary for Administration
Suzanne Hilding, Chief Information Officer

Comments on draft OIG IT Security Workforce Audit

Operating Unit	Comments
The Department of Commerce, Office of the Secretary (DOC/OS)	DOC/OS agrees with the introduction of the audit report that IT security is not just the responsibility of the Chief Information Officer (CIO), but rather a broader shared responsibility. For this reason, we are partnering with the Office of Human Resources Management to develop an IT Security workforce improvement program (Audit Report, page 2).
The National Institute of Standards and Technology (NIST)	NIST suggests that: (1) management is responsible for ensuring that staff receive appropriate training in their programs and operating units; (2) CIOs are responsible for local policies regarding training, and for ensuring that policies are complied with and that training is received; and (3) local management—not the CIO—are responsible for ensuring that staff in programs and operating units are qualified to do their (security) work (Audit report, page 2). NIST reported that a few references in the draft (Cybersecurity Act of 2009) should be removed. NIST has concerns that the bill is not yet out of Congressional committee and that the Senate bill does not have a House companion bill. Dozens of bills on cybersecurity have been introduced in previous Congresses, and few become law (Audit report, page 3). NIST responded that the recommendation that DOC take a leadership role in the Federal CIO Council to address workforce issues should be removed. The Department is currently being represented at the Federal IT Workforce committee (Audit report, page 13).
The Bureau of Economic Analysis (BEA)	In practice, the requirement discussed in Paragraph III appears to be overstated. In BEA, TS/SCI data is not meant to be used at the operational level. A better solution would be to have a Senior Intelligence Officer at DOC with authority to sanitize compartmented information to which the operating units need to respond. If a TS/SCI clearance becomes mandatory, it is imperative that the requirement be worded properly on a job announcement to avoid a "Catch-22" scenario. SCI clearances do not transfer from one organization to another (Audit report – page 10).