Changes to the Information Technology Security Workforce

Office of the Chief Information Officer
Carolyn Schmidt

Outline

- Why change?
- What changes?
- Impact of changes?
- Helping with change?
- Questions and Answers?

U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

Office of the Secretary

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.

IT Security

Continue Enhancing the Department's Ability to Defend Its Systems and Data Against Increasing Cyber Security Threats

Commerce Should Take Steps to Strengthen Its IT Security Workforce

In a recently completed audit, we found 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. For example, 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. We also found that IT security certifications are not required and are not consistently held by staff members.

On the whole, performance management and accountability need to improve. We found several instances in which IT security responsibilities were not included in the formal performance plans of employees with significant security responsibilities.

We recommended Commerce implement a Department-wide plan to address the deficiencies identified in the audit. The Department concurred with our findings and is taking steps to address our recommendations, including developing an enterprise-wide IT security workforce improvement plan.

Why change?

- OIG reports
  - Commerce Should Take Steps to Strengthen Its IT Security Workforce (Final Audit Report No. CAR-19569-1)
  - Top Management Challenges Facing the Department of Commerce (Final Report OIG-9884)
- OCIO did not dispute

- Threat environment warrants
- Inconsistent levels of expertise
- Enable sharing of expertise when responding to incident(s)

What changes?

- Policy
  - Performance metrics
  - Clearances required for some functions
    - CIO/ITSO
    - Reviewing other functions (Authorizing Official, Information System Owner, Information System Security Officer, Certification Agency, Incident Response Personnel, and key contingency roles)
  - Mandatory annual specialized training
    - supplemental to general training
  - Professional certifications required for ITSO, ISSO, IR roles
  - Inclusion of requirements in new vacancies
  - Position Sensitivity

Professional Certification

- ITSO

Role-related, role-approved Professional Certifications[9]
GIAC Information Security Fundamentals (GISF)
GIAC Security Leadership Certification (GSLC)
CompTIA Security+
(ISC)² Certification and Accreditation Professional (CAP)®
ISACA® Certified Information Security Manager (CISM)®
(ISC)² Certified Information System Security Professional (CISSP)® or Associate

Maps to DoD 8570.01-M, Change 2, XX/XX/2009. IAM Levels I, II, and III

- ISSO

Role-related, role-approved Professional Certifications[13]
CompTIA A+
CompTIA Network+
(ISC)² Systems Security Certified Practitioner (SSCP)®
GIAC Security Essentials Certification (GSEC)
CompTIA Security+
Security Certified Program Security Certified Network Professional (SCNP)
ISACA® Certified Information System Auditor (CISA)®
GIAC Security Expert (GSE)
Security Certified Program Security Certified Network Architect (SCNA)
(ISC)² Certified Information System Security Professional (CISSP)® or Associate
GIAC Certified Incident Handler (GCIH)

Maps to DoD 8570.01-M, Change 2, XX/XX/2009. IAM Levels I, II, and III

- IR

Role-related, role-approved Professional Certifications[13]
GIAC Certified Incident Handler (GCIH)
CERT® Certified Computer Security Incident Handler (CSIH)
Electronic Commerce Council Certified Ethical Hacker (CEH)

Maps to DoD 8570.01-M, Change 2, XX/XX/2009. CND Incident Reporter

Impact of changes?

- To DOC
  - Establishing minimum bar for expertise and increases accountability
  - Normalizing expertise across DOC

- To staff
  - Ensure training need to do job
  - Positions at risk if training not met or other requirements not met (i.e., clearances)
  - Establishes professional development path

- To Federal community
  - Use of professional certifications
  - Establishing capability to share staff during incidents

How are we helping with these changes?

- Careers in Motion
  - Career counseling
- Web-based course availability in CLC

- Development Plan

- Cyber Security Development Program (CSDP)
  - Information System Security Officers

CSDP Cyber Security Development Program

General Information

- Grades GS-7 through GS-15 level (or equivalent)
- 9 Months Duration
- Maximum of 20 participants, per cycle
- Competencies Addressed
  - Leadership
  - Expertise
  - Communication

Activities

- Mentoring program
- Participation in issue specific groups
- Web based training
- Rotational/developmental assignment
- Group project
- Networking activities
- Security-related events
- Readings and Discussions
- Industry professional certification

Questions and Answers?