FISSEA
23rd Annual Conference
Identifying Personnel With Significant Responsibilities For Information Security

John B. Ippolito, CISSP, PMP
Director
Allied Technology Group, Inc.
John.Ippolito@Alliedtech.com

Training Objective:
Maintain workforce expertise

- Everyone gets awareness
- Everyone gets basics and literacy
- Selective role-based training
  - Baseline of training to position responsibilities
  - Train relative to responsibilities
  - Certifications and training completion as metrics
  - Contractors fully trained per labor category

FISMA Requirements

CIO Responsibilities

‘‘(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;

Agency Program Components

‘‘(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, …

Performance Plan

‘‘(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

OMB A-130 Appendix III

GSS Control Requirement

b) Training. Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. … periodic refresher training shall be required for continued access to the system.

MA Control Requirement

b) Specialized Training. Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).

OMB A-130 Appendix III Discussion of Major Provisions

b) Training. The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency. Access provided to members of the public should be constrained by controls in the applications through which access is allowed, and training should be within the context of those controls. The Appendix enforces such mandatory training by requiring its completion prior to granting access to the system. Each new user of a general support system in some sense introduces a risk to all other users. Therefore, each user should be versed in acceptable behavior -- the rules of the system -- before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using or security of the system.

Training should be tailored to what a user needs to know to use the system securely, given the nature of that use. Training may be presented in stages, for example as more access is granted. In some cases, the training should be in the form of classroom instruction. In other cases, interactive computer sessions or well-written and understandable brochures may be sufficient, depending on the risk and magnitude of harm.

Over time, attention to security tends to dissipate. In addition, changes to a system may necessitate a change in the rules or user procedures. Therefore, individuals should periodically have refresher training to assure that they continue to understand and abide by the applicable rules. …

OMB A-130 Appendix III Discussion of Major Provisions

b) Training. The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency. Access provided to members of the public should be constrained by controls in the applications through which access is allowed, and training should be within the context of those controls. The Appendix enforces such mandatory training by requiring its completion prior to granting access to the system. Each new user of a general support system in some sense introduces a risk to all other users. Therefore, each user should be versed in acceptable behavior -- the rules of the system -- before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using or security of the system.

Training should be tailored to what a user needs to know to use the system securely, given the nature of that use. Training may be presented in stages, for example as more access is granted. In some cases, the training should be in the form of classroom instruction. In other cases, interactive computer sessions or well-written and understandable brochures may be sufficient, depending on the risk and magnitude of harm.

Over time, attention to security tends to dissipate. In addition, changes to a system may necessitate a change in the rules or user procedures. Therefore, individuals should periodically have refresher training to assure …

Computer Security Act

--Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. …

OMB A-130 Appendix III Discussion of Major Provisions

SSP Requirement
a) Rules. An important new requirement for security plans is the establishment of a set of rules of behavior … The rules should be in writing and will form the basis for security awareness and training.

OMB A-130 Appendix III

Department of Commerce (NIST)
2) Review and update guidelines for training in computer security awareness and accepted computer security practice, with assistance from OPM.

OPM
1)Assure that its regulations concerning computer security training for Federal civilian employees are effective.
2)Assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.

Example Agency Training Assessment

… conducted information technology security awareness training for all users and users with significant information technology security responsibilities, including contractors. Security awareness training was last conducted in ...

If the requirement is to train everyone, shouldn’t our response to “significant responsibilities” be focused on prioritizing training needs and not who does/does not get training?