U.S. Department of Health and Human Services

MEMORANDUM

TO: All Chief Information Security Officers (CISOs)

FROM: Daniel Galik
Chief Information Security Officer (CISO), Department of Health and Human Services (HHS)

SUBJECT: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities

DATE: May 16, 2011

The purpose of this updated memorandum is to update the Departmental policy reference and website links. All other content remains the same.

Both the Federal Information Security Management Act (FISMA) and the Office of Personnel Management (OPM) Regulation 5 Code of Federal Regulations (CFR) 930.301 require federal agencies to:

- identify personnel with significant security responsibilities; and
- provide security training commensurate with these responsibilities in the form of role-based training.

Additionally, the requirements within this document are issued under the authority of the Office of the Chief Information Officer (OCIO) *Policy for Information Systems Security and Privacy*.

Within the HHS environment, significant security responsibilities are defined as the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the security posture of one or more HHS systems.

As such, the following roles, consistent with OPM Regulation 5 CFR 930.301 represent the *minimum* set of roles at HHS that possess significant security responsibilities. Each role is characterized by its population - both mandatory and optional members - and relevant responsibilities.

- **Executives**
  - Mandatory Population:
    - All members of the Senior Executive Service (SES)
  - Optional Population:
    - None specified
  - Relevant Responsibilities:
    - Formulation of policy and guidance that may impact information system and/or security policy and operations
    - Allocation of resources to manage enterprise risk related to the use of information and information systems

- **Program and Functional Managers/Information Technology (IT) Functional Management and Operations Personnel**

Mandatory Population:

- All personnel identified as a System Owner, Data Steward, Data Owner, Program Manager, or Project Manager

Optional Population:

- Positions within the following series that might fill this role: GS-0332 Computer Operator, GS-0334 Computer Specialist, GS-2210 Information Technology Management, GS-0340 Program Management Series, and GS-0343, Management and Program Analysis

Relevant Responsibilities:

- Stewardship of a system or its information assets during its development and/or operation

- **Chief Information Officers**

  Mandatory Population:

  - HHS CIO, direct managerial reports and component organizations, OPDIV CIOs, direct managerial reports and component organizations, HHS CISO, and OPDIV CISOs

  Optional Population:

  - None specified

  Relevant Responsibilities:

  - Establishment of information security and/or system policy
  - Management of the IT function and related risks

- **IT Security Program Managers**

  Mandatory Population:

  - Individuals with the titles of Information Systems Security Officer (ISSO), Information Security Officer (ISO), or System Security Officer (SSO) and their information security employees or contractors
  - All information security employees or contractors working for or contracted by the HHS CISO or an OPDIV CISO

  Optional Population:

  - Positions within the GS-2210 Information Technology Management job series might fill this role

  Relevant Responsibilities:

  - Implementation of information security policies

- **IT Auditors**

  Mandatory Population:

  - All personnel engaged in the auditing of HHS or OPDIV systems or networks

  Optional Population:

  - Positions within the GS-0511 Auditing job series might fill this role

  Relevant Responsibilities:

  - Evaluation of systems for appropriate and effective implementation of controls to address security risks

- **Other Security-Oriented Personnel**

  Mandatory Population:

  - Information Technology (IT) administrators (e.g., network, system, and database)

  Optional Population:

- Positions within the GS-1550 Computer Science or the GS-0391 Telecommunications job series might fill this role

Relevant Responsibilities:

- Enable the implementation and operation of one or more system security controls, as outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems* (as amended)

HHS OPDIVs must identify employees and contractors who hold the aforementioned roles or responsibilities. The performance of this identification process is considered the completion of an OPDIV personnel needs assessment. Personnel whose responsibilities are not captured within this memorandum but meet the intent of the significant security responsibilities definition must also be designated. Personnel whose job duties meet these criteria must complete the Department's RBT course(s) associated with their role. Personnel that assume multiple roles must complete training that addresses the unique risks associated with each role. However, this training may be combined at the OPDIV's discretion. HHS RBT courses can be located at http://intranet.hhs.gov/it/cybersecurity/training/role_based/index.html.

Alternatively, an OPDIV may provide equivalent RBT to address the aforementioned roles, or combination of roles, with significant security responsibilities. Individuals beginning work with HHS shall be required to complete the appropriate RBT within three months of their initial start date. .

APPROVED BY:

__________________________________ 5/16/2011

Daniel Galik Date
HHS Chief Information Security Officer

Distribution – All HHS Operating Division Chief Information Officers