GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2100.3C
June 23, 2016

GSA ORDER

SUBJECT: Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities

1. Purpose. This Order provides direction and guidance on training requirements for all General Services Administration (GSA) and contractor employees with significant Information Technology (IT) security responsibilities, as set forth in the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Personnel Management (OPM) 5 Code of Federal Regulations (CFR) Part 930.301.

2. Cancellation. This Order cancels, CIO 2100.3B, dated August 13, 2012.

3. Background. Subchapter II of FISMA of 2014, states that the Chief Information Officer is responsible for training and overseeing personnel with significant responsibilities for information security. On June 14, 2004, OPM issued security awareness and training regulations for all Federal agencies in OPM 5 CFR Part 930.301. This Order implements the GSA training requirements for individuals with significant security responsibilities as defined in GSA IT Security Policy, CIO 2100.1J (See Chapter 2, Security Roles and Responsibilities).

4. Applicability. This IT Security Policy applies to all GSA employees and contractors (internal and external), who have significant information security responsibilities as defined by OPM 5 CFR Part 930 and GSA IT security training policy.

5. Policy. Individuals who hold a position defined within any of the OPM roles described below are required to fulfill all the training requirements identified for that role within sixty (60)-days from the time they are given the role and annually thereafter.

a. Executives, who are Authorizing Officials (AOs) as determined by GSA, must receive training in information security basics or policy level training in security planning and management or emerging technologies. AOs are the GSA executives that accept risk for IT systems. Executives may also complete other security training in support of the S/SO functions they support. Completion is defined as at least one (1)-hour of training annually by either completing one course from GSA Online University (OLU) or by completing the training provided by the Chief Information Security Officer (CISO) on emerging threats and/or security best practices as directed in the IT Security Procedural Guide, CIO-IT Security 05-29: IT Security Awareness and Role Based Training Program.

b. IT Security and other security-oriented personnel must receive training in information security basics and broad training in security planning, or system/application security management, or system/application life cycle management, or risk management, and/or contingency planning. GSA has determined these roles to be the Information Systems Security Managers (ISSMs), Information Systems Security Officers (ISSOs), and Regional ISSOs (RISSOs) as defined in the IT Security Point of Contact (POC) list. ISSMs, ISSOs and RISSOs must complete at least three (3)-hours of training annually by either completing CISO approved courses from OLU and/or CISO provided in-person or remote training as documented in the IT Security Procedural Guide, CIO-IT Security 05-29: IT Security Awareness and Role Based Training Program.

c. IT Functional Management and Operations Personnel must receive training in information security basics; management and implementation level training in security planning or system/application security management; or management and implementation level training in system/application life cycle management, or risk management, and/or contingency planning. GSA has determined these roles to be Privileged Users with Short Name Accounts (SNA). A Privileged User is a GSA employee, contractor, and other affiliates with privileged access that are able to modify systems or view highly confidential information. These personnel must satisfy their training requirement by completing the annual OLU Privileged Account Training.

6. References. The following informational material is relevant to this topic and provides additional background and guidance:

- NIST Special Publication 800-16, Information Technology Security Training Requirements, A Role-and Performance-Based Model (http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf).
- Federal Information Security Modernization Act of 2014 (https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf).
- Information Systems Security Awareness Training Program OPM 5 CFR Part 930.301, June 14, 2004 (https://www.gpo.gov/fdsys/granule/CFR-2011-title5-vol2/CFR-2011-title5-vol2-sec930-301).
- GSA IT Security Policy 2100.1J (https://insite.gsa.gov/portal/mediaId/513044/fileName/GSA_Information_Technology_(IT)_Security_Policy_CIO_21001J__12-22-2015.action).
- IT Security Procedural Guide: IT Security Awareness and Role Based Training, CIO-IT Security 05-29R5 (https://insite.gsa.gov/portal/getMediaData?mediaId=704738).

7. Signature.

DAVID SHIVE
Chief Information Officer
Office of GSA IT