* Pedestrian changes have been made to the directive and appear in blue. – 3/7/2012

FEDERAL DEPOSIT INSURANCE CORPORATION

DIRECTIVE SYSTEM

TYPE AND NUMBER	
Circular 1360.16	
CONTACT	TELEPHONE NUMBER
Brian H. Seborg	(703) 516-1168
DATE	
July 23, 2002	
DATE OF CANCELLATION *(Bulletins Only)*	

TO: All FDIC Employees and Contractors

FROM: Russell G. Pittman
Chief Information Officer

SUBJECT: Mandatory Information Security Awareness Training

1. Purpose

To mandate annual information security awareness training for all employees and contractors who are involved with the management, use, or operation of a Federal computer system within or under the supervision of FDIC.

2. Scope

This circular applies to all employees and contractors or non-FDIC contractor personnel.

3. Background

Periodic security awareness training is specifically mandated by three Federal issuances.

On October 30, 2000, the Government Information Security Reform Act (GISRA) was signed into law. One of the requirements of GISRA is that each Federal agency shall develop and implement an agency-wide information security program to provide information security for the operations and assets of the agency. This program shall include security awareness training to inform personnel of information security risks associated with the activities of personnel, and responsibilities of personnel in complying with agency policies and procedures designed to reduce such risk.

OMB Circular A-130, Management of Federal Information Resources, establishes policy for the management of Federal information resources.

Appendix III of OMB Circular A-130 requires that prior to being granted access to information technology (IT) applications and systems, all individuals must receive specialized training on their IT security responsibilities and established system rules.

4. Policy

It is FDIC's policy that:

a. Annually, all employees and contractors shall access the FDIC Information Security Awareness web site and review the content of the Security Awareness Orientation. After completing the web-based security awareness orientation, employees and contractors shall acknowledge that they have reviewed the materials relating to information security and agree to abide by the information security requirements as outlined in the referenced directives, under FDIC Directives on the FDIC Information Security Awareness web site. After employees and contractors have reviewed the Security Awareness Orientation, they must click on the Continue to Agreement Page hyperlink and click on the "I Agree" button. This action will record all employees' and contractors' names, network identification (ID), and agreement date in an awareness training database.

b. New employees shall log on and review the FDIC Information Security Awareness web site and orientation as soon as their network access is granted. After completing the orientation, employees will be asked to electronically acknowledge their review. Failure to do so within five working days of receiving a network ID may result in employees' and contractors' access to FDIC systems and applications being revoked. Existing employees and contractors access may also face revocation.

c. Failure of employees or contractors to comply with this policy once within a twelve-month period will result in revocation of access to FDIC applications and systems.

5. Definitions

Terms specific to this circular are defined below:

a. **General Support Systems (GSSs)**. As defined in Appendix III of OMB Circular No. A-130, GSSs are an interconnected set of information resources under the same direct management control, which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. The Director, Division of Information Technology (DIT), will determine GSSs within FDIC. GSSs must have a security plan and undergo an Independent Security Review (ISR) at least every three years, or when significant modifications are made.

b. **Major Applications (MAs)**. Information technology applications that require special security attention due to the combined importance of their confidentiality, integrity, and availability to the FDIC. The preliminary determination of an MA is based on a sensitivity assessment rating of critical. The final

Definitions (cont'd)

determination of whether or not an application is considered to be major is based upon a management decision made by the Director, DIT. MAs must have an application security plan developed that addresses the management, operational, and technical controls necessary to ensure security. MAs must also undergo an ISR upon significant change or at least every three years.

c. **Rules of Behavior**. Guidelines for information security established to hold users accountable for their actions and responsibilities. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program.

d. **Threat**. Any event that can compromise, corrupt, render data unavailable, or undermine the trustworthiness of a document.

e. **Vulnerabilities**. Ways in which an application or system may fail or be disrupted. They include susceptibility to physical dangers such as fire or water, unauthorized access to sensitive data or information, entry of erroneous data, denial of timely service, fraud, etc.

6. Responsibilities

a. **The Division of Information Technology, Information Security and Privacy Staff (DIT ISPS)** shall:

(1) Establish and maintain a security awareness training program. This training will communicate employee and contractor responsibilities, sources of assistance, available security tools, and Rules of Behavior for GSSs and MAs;

(2) Review and update the FDIC Information Security Awareness web site on a quarterly basis to ensure that information is current and effective;

(3) Coordinate the monitoring of user completion of this orientation; and

(4) Provide specialized training for employees with significant responsibilities for information security.

b. **Division and Office Directors** shall:

(1) Ensure that their staff annually review the web-based Security Awareness Orientation; and

(2) Ensure that complete participation in DIT-sponsored security training is achieved within their organizations.

c. **Information Security Managers for Divisions and Offices** shall:

Responsibilities (cont'd)	(1) Ensure divisional compliance with application-specific Rules of Behavior for corporate computer-based applications; and (2) Participate in DIT-sponsored security training including conferences and periodic meetings. d. **Employees and contractors** shall: (1) Remain sensitive to the threats and vulnerabilities concerning computer systems and recognize the need to protect data, information, and systems; and (2) Annually review the web-based Security Awareness Orientation and electronically acknowledge their completion.
7. Disciplinary Action	Users who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to disciplinary action. Any disciplinary action shall be administered in accordance with applicable laws and regulations, including FDIC Circulars 2410.6, Standards of Conduct for Employees of the Federal Deposit Insurance Corporation (FDIC), dated August 22, 2000, and 2750.1, Disciplinary and Adverse Actions, dated January 22, 1999, and applicable collective bargaining agreements.
8. Questions	Questions regarding this circular should be referred to the Associate Director, Information Security and Privacy Staff.
9. Effective Date	The provisions of this circular are effective immediately.