*Pedestrian changes have been made to the directive and appear in blue. – 5/30/2013

FEDERAL DEPOSIT INSURANCE CORPORATION

DIRECTIVE SYSTEM

TYPE AND NUMBER	
Circular 1360.12	
CONTACT	TELEPHONE NUMBER
Roderick Toms	(703) 516-5079
DATE	
June 26, 2003	
DATE OF CANCELLATION *(Bulletins Only)*	

TO: All Divisions and Offices

FROM: Russell G. Pittman
Chief Information Officer and Director
Division of Information Technology

SUBJECT: Reporting Computer Security Incidents

1. Purpose

To issue revised reporting requirements for computer security incidents.

2. Scope

The provisions of this circular apply to all users of Federal Deposit Insurance Corporation (FDIC) Automated Information Systems (AISs) and encompass all FDIC AIS resources, including general support systems and major applications.

3. Revision

This circular revises and supersedes FDIC Circular 1360.12, Reporting Computer Security Incidents, dated July 12, 2001.

4. Policy

All users of FDIC AISs shall report suspected computer security incidents affecting all FDIC AIS resources to the FDIC Computer Security Incident Response Team (CSIRT). FDIC CSIRT shall investigate and track all reported security incidents and report security incidents affecting general support systems and major applications to the Chief Information Officer and FDIC management officials responsible for the security of FDIC AIS resources.

5. Background

To accomplish the FDIC's mission, employees rely on timely access to automated data. Such data typically resides on, and is transmitted across, a number of AISs. These systems must be protected to safeguard the availability, confidentiality, and integrity of data. To protect FDIC AISs while allowing authorized use, Division of Information Technology (DIT), Information Security and Privacy Staff (ISP) establishes policies, procedures, and guidelines for managing access privileges. DIT/ISP recognizes the importance of early detection of computer

Background (cont'd)

security incidents and considers all users as partners in protecting FDIC AISs. The impact of computer security incidents can be minimized when users of FDIC AISs are alert to warning signs of improper activity and act quickly to report suspected violations. Therefore, DIT/ISP is issuing information about warning signs to watch for and whom to notify to enhance protection of FDIC AISs. (See paragraph 7., below, for a list of warning signs.)

---

6. Definitions

The following definitions apply throughout this circular.

a. **Automated Information Systems (AISs)**. An application of information technology that is used to process, store, or transmit information and includes, but is not limited to, mainframe systems, mini/microcomputer systems, personal computers, gateways, private branch exchanges (PBXs), and the networks that connect them and related software. AISs also include commercial and custom developed software, removable media, electronic and paper input documents, and output.

b. **Computer Security Incident**. An event that threatens the security of FDIC AISs, including FDIC's computers, mainframe, networks, software and associated equipment, and information stored or transmitted using that equipment. For examples of computer security incidents, refer to the FDIC CSIRT web site on FDICnet.

c. **FDIC CSIRT**. A team of computer professionals established by FDIC to provide centralized, expeditious technical assistance to effectively investigate, resolve, and close security vulnerabilities and incidents involving FDIC AISs.

d. **General Support System or "system."** An interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

For example, a system can be a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

Definitions (cont'd)

e. **Information Security Manager (ISM)**. An individual assigned to ensure divisional compliance with FDIC Security circulars, implement business specific security practices, and serve as primary liaison between DIT/ISP and the ISM's Division/Office. To identify the ISM for a specific Division/Office, contact DIT/ISP or search "ISM Program" on FDICnet.

f. **Information Security Technician (IST)**. A designated individual authorized to request access on behalf of users.

g. **Major Application**. The use of information resources to satisfy a specific set of user requirements. A major application requires special attention to security due to the combined importance of its confidentiality, integrity, and availability to the FDIC.

Note: All Federal applications require some level of protection. Certain applications require special management oversight because of the information contained within and should be treated as major applications. Adequate protection for other applications should be provided by security of the general support systems in which they operate.

h. **Users.** Employees and contractors who use FDIC AISs, and any other individuals with FDIC AISs related responsibilities (e.g., ISTs, ISMs, developers, operators, AISs owners, and LAN Administrators). This term also includes any other individuals granted access to FDIC AISs (e.g., Government Accountability Office (GAO) auditors, employees of other agencies, or members of the public).

7. Warning Signs

DIT/ISP compiled the following list of warning signs for potential computer security incidents based on recent experiences. A user observing any of the warning signs must promptly report the suspected activity to the FDIC CSIRT and notify the ISM of the affected organization.

a. Strangers in the work area carrying equipment or unauthorized individuals scrutinizing or rifling through someone else's desk or using someone else's personal computer (PC). Observation of these activities should be reported to FDIC security officers first, the FDIC CSIRT, and the ISM.

Warning Signs (cont'd)

b. Suspension of a password without prior warning or notification from an IST or other responsible official. (In this case, the user should notify the IST; the IST shall notify FDIC CSIRT if the suspension appears suspicious.)

c. Attempts by any individual to use trickery or deception to gain information that could be used to compromise or attack FDIC AISs. Such strategies, called social engineering, exploit normal human motivations and weaknesses, including the desire to be helpful. Examples include:

(1) Anyone inquiring about users' passwords;

(2) Questioning from unknown individuals posing as system administrators, security, or help desk personnel;

(3) Individuals who have no authority or need to know inquiring about users' access privileges; and

(4) Use of contrived emergencies, flattery, or persuasion to pressure users for information related to FDIC AISs.

d. Virus scan messages other than "no viruses found."

e. Files in a personal computer directory seem to be out of order.

f. Unusual messages or notifications from the E-mail system.

g. Any unusual activity that raises doubts about the legitimacy of someone's use of FDIC AISs.

h. Any pattern of unauthorized activity causing concern that an individual may intend to compromise FDIC AISs.

8. Responsibilities

a. **Users** of FDIC AISs shall report all computer security incidents to the FDIC CSIRT (see paragraph 10., below, for telephone numbers). A user shall file a report as soon as a theft, misuse of information resources, attempts to bypass security controls, or other unauthorized tampering with AIS resources is suspected. The report should include the date and time of the incident, location, nature of the activity observed, names or descriptions of the individuals involved, and telephone numbers, when available. This responsibility does not remove or replace reporting requirements established in other current FDIC circulars and policy memorandums.

Responsibilities (cont'd)

b. **The FDIC CSIRT** is responsible for taking corrective action, when appropriate, to contain computer security incidents to minimize impact on FDIC's business. The FDIC CSIRT shall:

(1) Investigate and resolve reported security incidents, track and record the results using the CSIRT incident response database;

(2) Evaluate the seriousness of computer security incidents and take appropriate corrective actions including notifying FDIC senior management and the OIG (specifically suspected violations of criminal law) within 24 hours and other outside entities, when appropriate;

(3) Develop specific procedures for reporting the occurrence, status, and resolution of computer security incidents to the Chief Information Officer and other FDIC management officials with responsibility for general support systems and major applications security. (These procedures shall include submission of a semi-annual report summarizing identified security incident trends and periodic (e.g., biweekly) CSIRT database reports generated for the Chief Information Officer and the OIG, Office of Investigations.);

(4) Notify and consult with the United States Computer Emergency Readiness Team (US-CERT) or any other incident center operated by the Office of Management and Budget (OMB) pursuant to 44 U.S.C. 3546) concerning security incidents. (Section 3546 was enacted by the Federal Information Security Management Act (FISMA), which is title III of the E-Government Act, Pub. L. No. 107-347, Dec. 17, 2002);

(5) Notify and consult with the office identified by the President of the United States on any incident involving a national security system, or with any other agency or office, in accordance with law or as directed by the President. (Such consultation should be rare because FDIC does not own or operate national security systems, as defined in Public Law 107-347. Sharing of information with the US-CERT about an incident involving a national security system must be consistent with standards and guidelines issued under 44 U.S.C. 3546(b)); and

(6) Establish links and mutual support arrangements with external organizations (e.g., other incident response teams, security organizations and associations) to enhance FDIC's awareness of and ability to respond to threats.

Responsibilities (cont'd)	c. **The Office of Inspector General (OIG)** is responsible for investigating allegations of criminal law violations, fraud, waste and abuse, and will evaluate and take action, as appropriate, regarding referrals made by CSIRT. The OIG shall also initiate contacts with the Federal Bureau of Investigation, the Department of Justice, other law enforcement agencies, and relevant OIG offices when circumstances require interaction. d. **Information Security Managers (ISMs) and Information Security Technicians (ISTs)** shall report to FDIC CSIRT computer security incidents that come to their attention and cooperate with FDIC CSIRT, as needed, in the investigation and resolution of such incidents.
9. Other Reporting Requirements	The guidance provided in this circular supplements existing requirements for reporting fraud, waste, abuse, or any other wrongdoing as stated in FDIC Circular 1150.2, Cooperation with Office of Inspector General Activities.
10. Contacting FDIC CSIRT	The FDIC CSIRT team can be reached at the following numbers: Telephone: (703) 516-5760 Toll Free: (877) 791-3377 Mobile: (571) 431-8757 Via E-Mail: fdic-csirt@fdic.gov
11. Additional Information	Refer to FDICnet for further information on services provided by the FDIC CSIRT.
12. Effective Date	The provisions of this circular are effective immediately.