FDIC DIRECTIVE 1360.12

Howard G. Whyte
Chief Information Security Officer
Chief Information Officer Organization /
Information Security and Privacy Staff

See signature(s) on Action Log

Reporting Information Security Incidents

PURPOSE

To issue policy and communicate reporting requirements for information security incidents for unclassified information.

SCOPE

The provisions outlined in this Directive apply to all users of FDIC information systems and to all users or possessors of unclassified FDIC information or data regardless of form or format.

AUTHORITIES

- FDIC 1360.9, Protecting Sensitive Information, October 27, 2015
- FDIC 12000.1, Cooperation with the Office of Inspector General, October 1, 2013
- Federal Information Security Modernization Act of 2014 (FISMA) (Pub. L. No. 113-283, as codified at 44 U.S.C. § 3554(b)
- Office of Management and Budget (OMB) Memorandum 17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, November 4, 2016

FORM(S)

None

REVISION(S)

FDIC 1360.12, Reporting Computer Security Incidents, dated June 26, 2003, is hereby revised and superseded.

Action Log

Submission Type *(New, Pedestrian Change, Revision)*	Date	Approval
New	07/12/2001	
Revision	06/26/2003	
Pedestrian Change	05/30/2013	
Revision	4/17/17	

Summary of Changes

The Directive has been updated to align with FISMA.

The title was changed from *Reporting Computer Security Incidents* to *Reporting Information Security Incidents.*

The Responsibilities have been clarified for levels ranging from the User to the Chairman.

Definitions have been added for Breach, Incident, Incident Response Coordinator, Information Security, Personally Identifiable Information (PII), Sensitive Information (SI), and Unclassified Information.

Table of Contents

Policy

A. Background

To accomplish the FDIC's mission, employees rely on access to information. This information must be protected to safeguard its confidentiality, integrity, and availability. To protect FDIC information, the Chief Information Security Officer (CISO), Information Security and Privacy Staff (ISPS), and the Chief Information Officer Organization (CIOO) established policies, procedures, and guidelines for managing access privileges to FDIC information. It is important that all users actively participate as partners to protect FDIC information, and support reporting information security incidents.

B. Policy

All users of FDIC information systems or possessors of FDIC information, in any form or format (including paper), must report suspected information security incidents affecting FDIC information systems, sensitive information including Personally Identifiable Information (PII) or data to Computer Security Incident Response Team (CSIRT) immediately. CSIRT investigates, tracks all reported information security incidents, and reports those incidents to the CISO and other officials responsible for the security of the FDIC resource or information.

Users must file a report to CSIRT immediately after discovery of a theft, misuse of information resources, attempt to bypass security controls, or other unauthorized tampering with FDIC information resources.

The policy and guidance provided in this Directive supplement existing requirements for reporting fraud, waste, abuse, or any other wrongdoing as stated in FDIC 12000.1, Cooperation with the Office of Inspector General, October 1, 2013.

The FDIC CSIRT team can be reached at the following numbers:

Telephone:	(703) 516-5760
Toll Free:	(877) 791-3377
Email:	fdic-csirt@fdic.gov

C. Responsibilities

1. Users are responsible for reporting all information security incidents to CSIRT immediately (see B. Policy). At a minimum, the report will 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 directives, policy memorandums, contracts, and agreements.

2. The Chairman, or designee, is responsible for determining whether an information security incident meets the major incident criteria as established and defined by the OMB. Once there is reasonable basis for the FDIC to conclude that a major incident has occurred, the seven-day Congressional notification requirement is triggered under the FISMA. The Chairman, or designee, is responsible for ensuring the FDIC notifies Congress as required under OMB guidance and in accordance with FISMA.

3. CSIRT will:

    a. Investigate and resolve, as appropriate, reported information security incidents, and record and track the results using the CSIRT incident response database;

    b. Evaluate the seriousness of FDIC information security incidents and take appropriate corrective actions including referring the incident to the appropriate FDIC officials, notifying FDIC senior management and the Office of Inspector General (OIG), as applicable;

    c. Develop specific procedures for reporting the occurrence, status, and resolution of FDIC information security incidents to the Chief Information Officer and other appropriate FDIC management officials with responsibility for the security of the FDIC information resources or the relevant FDIC information;

    d. Notify the Information Security Manager (ISM) and other responsible persons of the affected Division/Office and ISPS about information security incidents, as appropriate;

    e. Notify and consult with the United States Computer Emergency Readiness Team or any other incident center operated by the Department of Homeland Security pursuant to FISMA concerning security incidents, as required or appropriate;

f. 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; and

g. Develop and manage internal procedures that identify incidents for expeditious handling that could potentially be considered major incidents, as the term is defined by OMB, and warrant Congressional notification as required by FISMA.

4. Within the ISPS of the CIOO, the Incident Response Coordinator has overall responsibility for the incident response workflow to include response, remediation, and escalation. This individual will interact with other federal agencies including security-related relationships with other federal incident response teams, law enforcement organizations, and public safety agencies.

5. ISMs will report all information security incidents to CSIRT that come to their attention, cooperate with CSIRT, as needed, in the investigation and resolution of such incidents, and prepare additional incident risk analyses and other documentation, as needed, in connection with any related such investigations and resolutions.

6. The OIG is responsible for investigating allegations of criminal law violations, fraud, waste, and abuse. The OIG is also responsible for evaluating and taking action, as appropriate, regarding referrals made by the CSIRT. Both the OIG and CSIRT may initiate contacts with the Federal Bureau of Investigation, the Department of Justice, the Department of Homeland Security, other law enforcement agencies, and relevant OIG offices when circumstances warrant such contacts.

7. The Privacy Program Lead is responsible for ensuring that known or suspected breaches that involve PII are appropriately managed to closure.

Appendix

None

Glossary of Terms

Term	Definition
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: ▪ a person other than an authorized user accesses or potentially accesses personally identifiable information (PII); or ▪ an authorized user accesses PII for an other than authorized purpose.
Computer Security Incident Response Team (CSIRT)	A team of FDIC professionals established to provide centralized, expeditious, technical assistance to effectively investigate and resolve security incidents involving FDIC information.
Incident	An occurrence that ▪ actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or ▪ constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. An incident that involves PII – and only an incident that involves PII – constitutes a breach, as defined above.
Incident Response Coordinator	This individual is assigned to lead the overall incident response effort, to include interacting with internal and external organizations in the course of conducting incident response activities.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Term	Definition
Information Security Manager (ISM)	An individual assigned to ensure divisional compliance with FDIC security policies, implement business-specific security practices, and serve as primary liaison between ISPS and the ISM's Division/Office.
Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Refer to FDIC 1360.9 Protecting Sensitive Information for a complete definition of PII.
Sensitive Information (SI)	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled. Refer to FDIC 1360.9 Protecting Sensitive Information for a complete definition of SI.
Unclassified Information	Any information that is not properly classified under Executive Order 13526 – Classified National Security Information, dated December 29, 2009, or any related successive Executive Order.
Users	Employees, contractors, and other authorized individuals who have access to FDIC information.

Glossary of Acronyms

Acronym	Definition
CIOO	Chief Information Officer Organization
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
DIT	Division of Information Technology
FISMA	Federal Information Security Modernization Act of 2014
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SI	Sensitive Information