FDIC DIRECTIVE 1360.12

Reporting Information Security Incidents

Approval Authority: Sylvia Burns, Chief Information Officer and Chief Privacy Officer

Originating Division/Office: Chief Information Officer Organization

Approval Date: 08/29/2023

PURPOSE

This revised Directive provides policy and reporting requirements regarding information security incidents for unclassified information.

SCOPE

This Directive applies to all FDIC Divisions/Offices, including authorized users of FDIC information systems and to all authorized users or possessors of unclassified FDIC information, regardless of form or format.

AUTHORITIES

- Public Law 113-283, Federal Information Security Modernization Act of 2014 (FISMA), as codified in Title 44, United States Code (U.S.C.), Section 3554(b)
- Office of Management and Budget (OMB) Memorandum M-23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements
- FDIC Directive 1360.09, Protecting Information
- FDIC Directive 12000.01, Cooperation with the Office of Inspector General

FORMS

None.

SUMMARY OF CHANGES

This Directive supersedes FDIC Directive 1360.12, Reporting Computer Security Incidents, dated April 17, 2017.

REVISION, dated August 29, 2023

This Directive had been revised to:

- Align with FISMA;
- Change the title from *Reporting Computer Security Incidents* to *Reporting Information Security Incidents*;
- Clarify the Responsibilities for levels ranging from the authorized user to the Chairperson; and
- Add definitions.

TABLE OF CONTENTS

BACKGROUND

Based on federal requirements and mandates, the FDIC is responsible for ensuring Divisions/Offices meet the minimum security requirements for all information resources. To accomplish the mission of FDIC, employees rely on access to information. This information must be protected to safeguard its confidentiality, integrity, and availability. To protect FDIC information, the Office of the Chief Information Security Officer (OCISO) and the Chief Information Officer Organization establish policies, procedures, and guidelines for managing access privileges to FDIC information. It is important that all authorized users actively participate as partners to protect FDIC information and support the timely reporting of information security incidents when they occur.

POLICY

A. Overview

1. The FDIC Information Systems Security Program operates at all levels and capabilities for detecting, reporting, and responding to security incidents where:

   a. Risks are mitigated before substantial damage is done;

   b. The OCISO Security Response Team (SRT) is notified and consulted; and

   c. Congress, federal agencies, law enforcement, the FDIC Office of Inspector General (OIG), and any other organizations are notified and consulted, as appropriate

2. The policy and guidance provided in this Directive supplement existing requirements for reporting fraud, waste, abuse, or any other wrongdoing in accordance with FDIC Directive 12000.01, Cooperation with the Office of Inspector General.

B. Reporting Security Incidents

1. All authorized users of FDIC information systems or possessors of FDIC information, in any form or format (including paper), must immediately report suspected information security incidents affecting FDIC information systems, personally identifiable information (PII), or other sensitive information (in accordance with FDIC Directive 1360.09, Protecting Information), or information to the SRT.

2. SRT investigates, tracks, categorizes, and prioritizes all reported potential information security incidents. Furthermore, SRT reports incidents to the Chief Security Officer and other officials for the security of FDIC resources or information as defined within the Incident Response Plan (IRP).

3. Authorized users must file a report to the SRT immediately after discovery of a theft, misuse of information and information resources, attempt to bypass security controls, or other unauthorized tampering with FDIC information resources.

4. See the Appendix regarding contact information to the SRT.

RESPONSIBILITIES

A. Chairperson:

1. Determines whether an information security incident meets the criteria for a "major" incident as established and defined in OMB Memorandum M-23-03, or most recent update; and

2. Ensures the FDIC notifies Cybersecurity and Infrastructure Security Agency, OMB Office of the Federal Chief Information Officer (CIO), Congress, and the OIG, as required per OMB policy and in accordance with FISMA and other applicable federal laws and regulations.

B. Chief Information Officer:

Advises the Chairperson and other senior officials of the information and possible courses of action relevant to information systems involved in an incident, based on the IRP.

C. Chief Information Security Officer:

Advises the Chairperson and other senior officials of the information and possible courses of action relevant to security concerns involved in an incident, based on the IRP.

D. Incident Response Coordinator, Office of the Chief Information Security Officer:

1. Has overall responsibility for the incident response workflow, including response, remediation, and escalation; and

2. Interacts with other federal agencies' incident response teams, law enforcement organizations, and public safety agencies in response to appropriate incidents.

E. Security Response Team:

1. Serves as the central point of contact for receiving reports of information security incidents;

2. Investigates and resolves (as necessary) reported information security incidents, and records and tracks the results;

3. Evaluates the severity of FDIC information security incidents and coordinates corrective actions, including referrals of incidents to appropriate senior officials and notifying the OIG, in accordance with FDIC Directive 12000.01, Cooperation with the Office of Inspector General;

4. Initiates contact with the OIG, for incidents where significant criminal behavior is suspected;

5. Develops specific procedures for reporting the occurrence, status, and resolution of FDIC information security incidents to the CIO and other appropriate senior officials with responsibility for the security of FDIC information resources or information;

6. Notifies appropriate Division/Office personnel (e.g., Information Security Manager, Information System Security Manager, and FDIC management);

7. Notifies and consults with the Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency pursuant to FISMA, OMB guidance, and DHS Binding Operational Directives;

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

9. Develops and manages internal procedures that identify incidents for expeditious handling that could potentially be considered major incidents, as defined by OMB, and warrant Congressional notification, as required by FISMA.

F. Inspector General, Office of Inspector General:

1. Is responsible for carrying out a comprehensive nationwide program for the detection and investigation of criminal, civil, and administrative misconduct impacting FDIC programs and operations; and

2. Evaluates and takes necessary action, as appropriate.

G. Privacy Program:

Ensures that known or suspected breaches that involve PII are appropriately managed to closure.

H. Division/Office Information Security Managers and Information System Security Managers:

1. Report all information security incidents to the SRT that come to their attention;

2. Cooperate with the SRT in the investigation and resolution of such incidents; and

3. Prepare additional incident risk analyses and other documentation, as required by their respective Division/Office.

I. Authorized Users:

Report all suspected information security incidents to the SRT immediately in accordance with this Directive and any other applicable FDIC directives, policy memorandums, contracts, and agreements.

APPENDIX – SECURITY RESPONSE TEAM CONTACT INFORMATION

Contact information for the SRT is as follows:

Telephone: (703) 516-5760

Toll Free: (877) 791-3377

DIT Service Desk: 1-877-FDIC-999 (1-877-334-2999)

Email: srt@fdic.gov

GLOSSARY OF TERMS

Authorized Users: Employees, contractors, and other individuals who have been granted access to FDIC information based on FDIC business needs.

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 PII; or
- An authorized user accesses PII for an unauthorized purpose.

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.

Incident Response Coordinator: Individual assigned to lead the overall incident response effort, including interacting with internal and external organizations in the course of conducting incident response activities.

Incident Response Plan: Defines information security incidents and the criteria for information security incident categorization, classification, escalation, and reporting requirements in accordance with FDIC policy and NIST Special Publication 800-61. The IRP establishes roles and responsibilities for reporting and responding to incidents, as well as a summary of the FDIC Incident Response Lifecycle.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.

Information Security Manager: An individual assigned to ensure Division/Office compliance with FDIC security policies, implement business-specific security practices, and serve as primary liaison between OCISO and their Division/Office.

Information System Security Manager: An experienced information security professional with expertise and skills in implementing and managing security for federal information systems. Working within OCISO, this individual provides focused attention and expertise to assigned IT projects.

Personally Identifiable Information: 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.

Security Response Team: A team of FDIC professionals established to provide centralized, expeditious, and technical assistance to effectively investigate and resolve security incidents involving FDIC information.

Sensitive Information: Any information, of which the loss, misuse, or unauthorized access to or modification, could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled.

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.

GLOSSARY OF ACRONYMS

CIO: Chief Information Officer

DHS: Department of Homeland Security

DIT: Division of Information Technology

FISMA: Federal Information Security Modernization Act of 2014

IRP: Incident Response Plan

NIST: National Institute of Standards and Technology

OCISO: Office of the Chief Information Security Officer

OIG: Office of Inspector General

OMB: Office of Management and Budget

PII: Personally Identifiable Information

SRT: Security Response Team