Federal Maritime Commission

Information Security Incident Response Policy – Breach Notification Plan

Managing Directive 2 **Revised: June 30, 2017**

Supersedes Managing Directive 2011-2 dated September 22, 2016

Table of Contents

Annual Review and Version History

Annual Review Date	Revision Date (if any)	Initiated By	Approved By	Approval Date	Reason
6/30/2017	6/30/2017	A. Haywood, CIO	K. Gregory, MD	6/30/2017	OMB Guidance M-17-12

Section 1. Purpose

The purpose of this directive is to establish security policy and procedures for implementing the Federal Maritime Commission's Information Security Incident Response (ISIR) Policy/Breach Notification Plan for Personally Identifiable Information (PII). This document provides policy on what actions should be taken when it is determined that PII has been compromised and employees and contractors should be notified.

Section 2. Scope

The provisions of this directive apply to all FMC employees, contractors, and others, who process, store, transmit, or have access to any FMC information. This directive shall be applied to all FMC information system resources, at all levels of sensitivity, whether owned and operated by the FMC or operated on behalf of the FMC.

Section 3. Authority

This policy is issued pursuant to Office of Management and Budget (OMB) Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*; United States Computer Emergency Readiness Team (US-CERT) *Federal Incident Reporting Guidelines*; National Institute of Standards and Technology (NIST) Special Publication 800-61, *Computer Security Incident Handling Guide.*

Section 4. Definitions

Breach Response Team (BRT). The Breach Response Team is responsible for advising the FMC Chairman on effectively and efficiently responding to a data breach. As a breach warrants, the BRT shall be comprised of the Senior Agency Official for Privacy (SAOP), the Managing Director, the Deputy Managing Director, the Chief Information Officer (CIO), the Chief Information Security Officers/Senior Information Security Officer (SISO), the Director of Information Technology (OIT), the Secretary or Assistant Secretary acting as the Privacy Act Officer, the General Counsel, the FMC's Senior Advisor – Legislative/Public Affairs, and the Program Manager that is experiencing the breach.

Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for other than an authorized purpose, have access or potential access to personally identifiable information, whether physical or electronic.

Computer Information Security Incident. An act or circumstance in which there is a deviation from the requirements of the governing security regulations. Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of security incidents, including any unauthorized activity that threatens the confidentiality, integrity or availability of FMC information system resources.

Information Systems. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog); includes software, firmware, and hardware.

Personally Identifiable Information (PII). Any piece of information which potentially can be used to uniquely identify, contact, or locate a single person. For example, PII could be an individual's Social Security Number; name or address in conjunction with one or more of the following: date of birth; Social Security Number; driver's license number or state identification; foreign country equivalent to Social Security Number; tax identification number or equivalent; financial account number; and credit or debit card number.

Physical Security Incident. Any breach of the agency's physical records or files involving PII (e.g., theft of a timekeeper's paper records, OTI file folders, etc.) that creates a threat of unauthorized disclosure, unauthorized access, or use of PII by other than an authorized FMC employee or contractor.

Security Officer (for Information Systems Security, Personnel Security, or Physical Security). The appropriate Security Officer, as further defined in Commission Order 80.

Section 5. Responsibilities

a. **FMC Employees and Contractors shall:**

1) As agency information technology users, be familiar with and apply the FMC's Managing Directive 3, *Rules of Behavior for Information Technology,* and this Managing Directive.

2) With respect to all incidents involving a potential breach of PII, an employee who observes suspicious activity with respect to files or data believed to contain PII should take steps to immediately notify the Assistant Managing Director and/or Chief Information Officer.

3) Report immediately upon discovery all potential and actual privacy breaches to the OIT Help Desk at (202) 523-0854 or OIT-HELPDESK@FMC.gov, the Office of the Managing Director at (202) 523-5800 or OMDMaritime@FMC.gov, and the appropriate Security Officer as defined in Commission Order 80.

4) After submitting the initial report, staff must report the incident to their Program Manager, followed by submission of Form FMC-93, *Initial Security Incident Report*.

b. **FMC Information Technology Support Team, and FMC Supervisors shall:**

1) Be responsible for ensuring compliance with security regulations, policies and procedures within their respective organizational components.

2) Encourage users to report computer security and physical security incidents to the Assistant Managing Director and/or Chief Information Officer to facilitate mitigation of threats and the development of trend information to recognize system-wide problems.

3) Invoke incident response procedures commensurate with the situation, and as appropriate, assemble a BRT to advise and assist in ongoing investigation and decision making. The nature of the incident and the type(s) of information involved will determine the make-up of the BRT. The BRT will typically initially include a representative from the bureau/office experiencing the incident, the SISO, Director of OIT, Assistant Managing Director, and the CIO. Duties may include assisting the SISO by providing detailed reports, monitoring events, isolating affected systems, communicating with management and users, and other similar functions.

c. **The Chief Information Officer (CIO) shall:**

1) Serve initially as the incident manager to coordinate an immediate response to a breach incident.

2) Notify the appropriate Security Officer (for Information Systems Security, Personnel Security or Physical Security), as defined in Commission Order 80.

3) Upon receipt of a report of potential or confirmed data breach, impacted system(s), and evaluation of any privacy threats to PII and/or other sensitive data, the CIO will determine whether the agency's response can be conducted at the staff level or whether the agency must activate the Breach Response Team. The CIO may consult with the SAOP, Director of OIT, and the SISO in making this determination.

4) Determine information technology security incident categories.

5) Determine appropriate procedures for handling each incident category.

6) Make reports to the agency regarding incidents.

7) Determine appropriate procedures for sharing incident information with other Federal organizations.

8) Designate or request that personnel resources from OIT operational staff be allocated to participate if the BRT is activated.

9) Ensure that security incidents can be quickly isolated by calling on the appropriate OIT staff member to perform activities such as restricting network access by removing affected machines from the network; saving and analyzing log files for evidence collection; restoring clean configurations from backups; or performing other activities necessary to identify, contain, analyze, and recover from a computer security incident.

10) Provide notice to the Inspector General of persons suspected of intentionally causing a breach or other violations of law.

d. **The Security Officer shall:**

1) Respond to all IT-related security incident activities.

2) For computer security incidents, initiate appropriate processes when computer security incidents require action on the part of multiple OIT operational staff to contain, analyze, recover from, and prevent a computer security incident.

3) For physical security incidents, determine the appropriate procedures for handling each incident, in coordination with the appropriate supervisor, make reports to the BRT and assist the BRT in determining appropriate procedures for sharing incident information outside the agency.

4) Report all PII incidents to US-CERT within one (1) hour of discovery/detection, following the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) Federal Incident Reporting Guidelines, including as applicable, physical security incidents involving loss of IT hardware containing PII.

5) Determine what incident information may be released and to whom, in consultation with the CIO and/or Managing Director.

6) Maintain a repository of incident information for the purpose of analysis to determine if trends exist that could be mitigated through user awareness, training, or the addition of technical security controls.

e. **Senior Agency Official for Privacy.**

The Senior Agency Official for Privacy (SAOP) shall have the responsibilities designated under Commission Order 89, *Privacy Act Implementation*. Consistent with applicable law, the SAOP may delegate to the SISO or CIO the duty to perform particular privacy functions assigned to the SAOP.

f. **Breach Response Team:**

1) The SAOP will lead the Breach Response Team.

2) Identify and assemble supplementary breach response team agency officials, (i.e., Office of Budget and Finance, Office of Human Resources, Office of Management Services and other agency personnel) as required, to respond to a breach incident.

3) Immediately determine the status of the breach (ongoing, active, or post breach) and decide how to investigate and mitigate the data breach.

4) Begin breach response documentation and reporting process.

5) Determine whether notification of affected individuals is appropriate and, if so, when and how to provide notification.

6) Determine whether to notify DHS/authorities/law enforcement.

g. **FMC Inspector General:**

Upon notice by the CIO, or upon his own initiative, may undertake investigations of persons intentionally causing a breach or suspected violations of law; provided that nothing in this directive shall be construed to restrict the independence of the Office of the Inspector General (OIG) in the performance of its duties as prescribed by the Inspector General Act of 1978, as amended.

Section 6. Immediate Reporting of Information Security Incidents

a. Reporting to **Appropriate Security Officer and CIO.** Upon the discovery or detection of any incident involving a potential or confirmed breach of PII and/or security incident with the FMC, the CIO or Assistant Managing Director will, within one (1) hour, report the incident (orally or via e-mail) to the FMC Security Officer for Information Systems Security, Personnel Security, or Physical Security, as appropriate.

A written report of the incident shall be filed by the BRT within 24 hours and contain: (1) Point of contact; (2) Affected systems and locations; (3) System description including hardware, operating system, and application software; (4) Type of information accessed, such as Privacy Act, litigation, etc.; (5) Incident description; (6) Incident resolution status; (7) Damage assessment; (8) Organizations to be contacted (if any); and (9) Corrective actions taken (if any).

b. Reporting to **Senior Agency Official for Privacy.** Once a data breach has been validated, the Security Officer, Director of OIT, SISO and/or CIO will immediately report the confirmed breach of PII and/or security incident to the SAOP.

c. **Breach Response Team.** Upon notification of the BRT, the BRT will meet as soon as possible, but not later than one (1) day from the date it receives notification.

d. **Department of Homeland Security.** The OIT is the agency's designated Security Operation Center (SOC), responsible for all information technology related incident reporting activities to the DHS-CERT. Within one (1) hour of discovery or detection of breach of PII and/or security incident, the incident shall be reported to US-CERT. The SISO shall promptly apprise the BRT when the notification has been completed.

e. **Reporting to Congress.** Pursuant to the Federal Information Security Modernization Act (FISMA), 44 U.S.C. §§3553-54, the appropriate Congressional Committees shall be notified no later than seven days after the date on which there is a reasonable basis to conclude that a major incident has occurred. The BRT will supplement the initial seven-day notification with a report no later than 30 days after the breach is discovered. See OMB Memorandum M-17-05 or successor guidance for a definition of a major incident.

Section 7. Procedures for Information Security Incidents

a. **Mitigation and Containment.** Any OIT team member who observes an intruder on an FMC network or system shall take action to terminate the intruder's access immediately. Affected systems, such as those infected with malicious code or systems accessed by an intruder, shall be isolated from the network until the extent of the damage can be assessed. System and/or security administrators shall quickly eliminate the method of access used by the intruder and any related vulnerabilities.

For physical security incidents, the relevant Program Manager shall take immediate steps to eliminate the method of access utilized during the breach and any related vulnerabilities.

b. **Investigation.** The appropriate Security Officer or his/her designee shall serve as the focal point for the collection of evidence, and in consultation with the BRT, shall determine if a physical security incident should be reported to outside authorities (e.g., local police).

Every effort shall be made to save log files and system files that could be used as evidence of a security incident. This includes backing up the affected environment; thoroughly documenting all activities performed on the affected platform or environment to contain, mitigate, and restore the environment; preserving any potential evidence, such as system logs, screen shots, hard drives, and/or all other relevant evidence in a secure location; and documenting and controlling the movement and handling of potential evidence in order to maintain a chain of custody.

c. **Eradication and Restoration.** The extent of damage must be determined. If the damage is serious and the integrity of the data is questionable, a system shutdown and reloading of operating systems and/or data may be required. Management notification is required if mission-critical systems must be taken offline for an extended period of time to perform the restoration.

The Program Manager that experienced the breach shall work with OIT staff to restore the information if possible (through other records, etc.). Security protocols shall be reviewed and amended to ensure that breach of the PII cannot occur again.

d. **Information Dissemination.** Any public release of information concerning a computer security incident shall be coordinated through the BRT, and ultimately with the Chairman. Content of notification to affected individuals should follow guidelines contained in OMB Memorandum M-07-16, or successor guidance.

The appropriate Security Officer, SISO and/or the CIO shall manage the dissemination of incident information to external participants, such as law enforcement or other incident response agencies (US-CERT). After consulting with the BRT, he/she shall provide information to the Chairman for incidents that could affect the public, such as web page defacement or denial of service that disrupts systems or applications. Other incident participants, such as technical staff, shall not provide any public comments about ongoing incidents or disseminate incident information, but shall refer all inquiries to the Security Officer. The Security Officer, in conjunction with the CIO, also shall provide information to the OIG if a security incident indicates possible user misconduct or criminal activities.

e. **Ongoing Reporting.** As appropriate, after the initial report is filled, subsequent reports shall be provided by the SISO to the BRT to ensure that FMC is informed and kept updated throughout the incident. A follow-up report (after action report) shall be submitted upon resolution by those directly involved in addressing the incident.

f. **Subsequent Review.** After the initial reporting and/or notification, the appropriate Security Officer, SISO and/or the CIO shall review and reassess the level of impact that has already been assigned to the information using NIST-defined impact levels.

Section 8. Breach Notification to Affected Parties

The BRT will consider six elements in evaluating the situation and respond in accordance with established agency procedures: (1) whether breach notification is required; (2) timeliness of the notice; (3) responsibility for the notice; (4) contents of the notice; (5) means of providing the notice; (6) and public outreach in response to the notice. In addition to the consideration of breach notification, the BRT will ensure that appropriate steps are initiated to mitigate the breach's impact and recurrence, in accordance with US-CERT and NIST guidance.

a. **Assessing Need for Breach Notification.** To determine whether notification of a breach is required, the BRT will assess the likelihood of harm occurring and then assess the magnitude of potential harm. In assessing the likely risk of harm, the BRT will consider six factors: (1) the nature of the breach; (2) the type of PII data elements breached; (3) the number of individuals affected; (4) the likelihood that the information is accessible and usable; (5) the likelihood that the breach might lead to harm; and (6) the ability of the FMC to mitigate the risk of harm.

Information available from the President's Identity Theft Task Force April 2007 Report, *Combating Identity Theft – A Strategic Plan*, may be of assistance in disseminating information, preparing for follow-on inquiries, and preparing counterpart entities that may receive a surge in inquiries.

b. **Timeliness of Notice.** When notification is appropriate, the BRT will provide notification to the individuals affected without unreasonable delay. The FMC will determine the most appropriate means of providing notification, whether by telephone; first-class mail; email; existing government- wide services; newspapers or other public media outlets. Means of providing the information to affected individuals should follow the guidelines contained in OMB Memorandum M-07-16, and accommodations regarding visually or hearing impaired individuals should be consistent with Section 508 of the Rehabilitation Act of 1973, as amended.

c. **Responsibility for Breach Notification.** In coordination with the BRT, the FMC bureau/office affected by the breach will issue the breach notification to the affected individual(s), unless other instructions are given by the BRT. For breaches arising from FMC area offices, the Director of Field Investigations will issue the breach notification.

d. The breach incident notice should include the following elements: (1) A description of what happened, including the date(s) of the breach and the date of its discovery; (2) A description of the types of PII involved in the breach (e.g., the full name, SSN, date of birth, home address, account numbers); (3) An advisory that the individual should contact their financial institution(s) to determine actions to take to protect the account(s); (4) FMC contacts for more information, including phone number, email address, and postal address; (5) Information on how to request a free annual credit report and recommendation to place an initial fraud alert on credit reports maintained by the three major credit bureaus; (6) The steps the affected individual(s) should take to protect themselves from harm, if any.

Section 9. Staff Training on Breach Policy and Procedures

Yearly, as part of the agency annual information security training, FMC staff will be given training on how to prevent breach incidents, and their roles and responsibilities for responding to security incidents.

The FMC shall perform an annual incident response test/exercise to assess the agency's preparedness and approach to resolve security incidents.

Section 10. References

a. Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*

b. NIST Special Publication 800-61, *Computer Security Incident Handling Guide*

c. US-CERT, *Federal Incident Reporting Guidelines*

d. President's Identity Theft Task Force Report, *Combating Identity Theft: A Strategic Plan* (April 2007)

e. Commission Order 56, *Automated Information Security Program*

f. Commission Order 80, *Security*

g. Commission Order 89, *Privacy Act Implementation*

h. Managing Directive 2011-3, *Rules of Behavior for Information Technology*

i. FMC Continuity of Operations Plan, February 2017

j. FMC Disaster Recovery Plan, December 2015

Section 11. Effect of Issuances

The policies, procedures, and administrative requirements contained in issuances made pursuant to this directive shall remain in full force and effect until superseded, modified, or canceled. In the event of a conflict between a Commission Order and a Managing Directive, the Commission Order receives precedent.

Section 12. Inquiries

Further information concerning this Managing Directive may be obtained by contacting the Managing Director's Office at (202) 523-5800.

Karen V. Gregory
Managing Director