MANAGING DIRECTIVE 2011-2

INFORMATION SECURITY INCIDENT RESPONSE POLICY/ BREACH NOTIFICATION PLAN FOR PERSONALLY IDENTIFIABLE INFORMATION

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.

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 FMC or operated on behalf of the FMC. 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.

3. Authority.

This policy is issued pursuant to 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;* and Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*

4. Definitions.

Agency Response Team (ART). At a minimum, an ad hoc ART assembled to address a breach incident consists of the Program Manager of the program experiencing the breach, the Chief Information Officer (CIO), the IT Security Officer, the Managing Director acting as Senior Agency Official for Security and the Senior Agency Official for Privacy, the Secretary acting as the Privacy Act Officer, and the General Counsel.

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 an other than 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 that is 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.

5. Policy for Computer Security Incidents.

a. **Initial Reporting.**

i. **Internal.** All computer security incidents, including suspicious events, shall be reported immediately (orally or via e-mail) to the IT Security Officer and/or CIO, by the employee who has witnessed/identified a breach and/or by the relevant Program Manager, followed by submission of Form FMC-93, *Initial Security Incident Report*.

ii. **External.** All computer security incidents, specifically PII, shall be reported to US-CERT, whether potential or confirmed breach, within one hour of discovery/detection.

b. **Escalation.** The IT Security Officer and/or CIO should be notified immediately when a suspicious event or security incident is reported. The IT Security Officer shall determine if a security incident is indeed underway. If more information is required to determine if the situation represents a security incident, the IT Security Officer may contact the person who supplied the initial report for additional details.

c. **Mitigation and Containment.** Any system, network, or security administrator 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.

d. **Investigation.** 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; storing any potential evidence, such as drives, diskettes, or tapes, in a locked container; and documenting

and controlling the movement and handling of potential evidence in order to maintain a chain of custody. The IT Security Officer or his/her designee shall serve as the focal point for collection of evidence.

e. **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.

f. **Information Dissemination.** Any public release of information concerning a computer security incident shall be coordinated through the ART, and ultimately with the Chairman. Content of notification to affected individuals should follow the guidelines contained in OMB Memorandum M-07-16, to include a brief written description of what happened, a description of the types of PII involved, a statement whether the information was encrypted or otherwise protected, what steps individuals should take to protect themselves from harm, and contact information at the FMC. 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. 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. www.idtheft.gov/reports/StrategicPlan.pdf.

The IT Security Officer and/or the CIO shall manage the dissemination of incident information to external participants, such as law enforcement or other incident response agencies (FedCIRC – US-CERT). After consulting with the ART, 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. The IT 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. The OIG may be required to independently disseminate event information as required under the Inspector General Act of 1978, but care should be taken to reduce exposure of sensitive information concerning security controls or features in place that might provide vulnerability information to the public or could be used to plan future abuses of the FMC network or IT infrastructure. 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 IT Security Officer.

g. **Ongoing Reporting.** After the initial oral or e-mail report is filed, subsequent reports shall be provided directly to the IT Security Officer or his/her designee.

i. The incident reports shall be submitted by those directly involved in addressing the incident.

ii. A written report of the incident shall be filed within 24 hours:

1. Point of contact;

2. Affected systems and locations;

3. System description including hardware, operating system, and application software;

4. Type of information processed, such as Privacy Act, litigation, etc.;

5. Incident description;

6. Incident resolution status;

7. Damage assessment;

8. Organizations contacted (if any); and

9. Corrective actions taken (if any).

iii. A follow-up report shall be submitted upon resolution by those directly involved in addressing the incident.

h. **Review**. After the initial reporting and/or notification, the IT Security Officer 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.

6. Policy for Physical Security Incidents.

a. **Initial Reporting.**

i. **Internal.** Physical security incidents involving PII (e.g., theft of a timekeeper's paper records, OTI file folders, etc.) shall be reported immediately (orally or via e-mail) to the appropriate Security Officer (see Commission Order 80, *Security*), as well as the ART.

ii. **External.** All physical security incidents involving PII shall be reported to US-CERT, if applicable.

b. **Escalation.** The appropriate Security Officer, in consultation with the ART, shall determine if a physical security incident should be reported to outside authorities (e.g., local police).

c. **Mitigation and Containment.** The relevant Program Manager shall take immediate steps to eliminate the method of access utilized during the breach and any related vulnerabilities.

d. **Investigation.** The appropriate Security Officer and Program Manager shall serve as the focal points for collection of evidence, along with any outside authorities who may be involved at this point.

e. **Eradication and Restoration.** The extent of the breach must be determined. The Program Manager shall work with staff to restore the information if possible (through other records, etc.). Security protocols shall be reviewed and amended to ensure the loss of the PII cannot occur again.

f. **Information Dissemination.** Any public release of information concerning a physical security incident involving PII shall be coordinated by the appropriate Security Officer and relevant Program Manager through the ART, and ultimately through the Chairman. Information on incidents that could affect employees, regulated entities or the public should be made available, with care taken to reduce exposure of sensitive information. Other staff should not provide public comment about ongoing activities or disseminate incident information. Notice to those affected by the breach should be provided in a timely manner via e-mail or mailed notice, but without compounding the harm from the initial incident through premature announcement based on incomplete facts. The appropriate Security Officer, in conjunction with the relevant Program Manager, shall provide information to the OIG if a security incident indicates possible misconduct or criminal activities. 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. See also section 5.f above.

g. **Ongoing Reporting.** After the initial report is filed, a subsequent report shall be filed by the appropriate Security Officer and relevant Program Manager to the ART, to include an incident description, reports of those with direct knowledge of the event, incident resolution status, damage assessment, and corrective actions taken or proposed. A follow-up report shall be submitted upon resolution of the incident.

7. Responsibilities for Computer Security Incidents.

a. **Users** are responsible for being familiar with and applying FMC's Managing Directive 2011-3, *Rules of Behavior for Information Technology*. Users shall report all computer security incidents and suspicious events to the IT Security Officer and/or CIO immediately.

b. **System Administrators** shall follow the procedures listed above for users and these additional procedures to ensure that systems under their control adhere to this plan:

i. Encourage users to report computer security incidents to the IT Security Officer and/or CIO to facilitate the development of trend information to recognize system-wide problems.

ii. Participate in the ISIR if a security incident affects their area of responsibility. Duties may include assisting the IT Security Officer by providing detailed reports, monitoring events, isolating affected systems, restoring clean configurations to desktop computers, communicating to management and users, and other similar functions.

c. **The CIO shall:**

i. Determine information technology security incident categories;

ii. Determine appropriate procedures for handling each incident category;

iii. Make reports to the agency regarding incidents;

iv. Determine appropriate procedures for sharing incident information with other Federal organizations;

v. Designate personnel resources from his/her operational staff to ensure participation if the ISIR is activated. This will ensure that security incidents can be quickly isolated by calling the appropriate representative 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. These responsibilities are intended to leverage existing FMC processes and procedures, including Continuity of Operations planning and exercises, and maintenance procedures; and

vi. Provide the IT Security Officer with resources to collect computer security incident information.

d. **The IT Security Officer shall:**

i. Respond to all ISIR activities;

ii. Activate the ISIR process when computer security incidents require action on the part of multiple IT operational staff to contain, analyze, recover from, and prevent a computer security incident;

iii. Report all "computer security incidents" in accordance with the *Computer Security Handling Guide;*

iv. Report all PII incidents to US-CERT within one hour of discovery/detection, following US-CERT's *Federal Incident Reporting Guidelines;*

v. Determine what incident information may be released and to whom, in consultation with the CIO; and

vi. 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.

8. Responsibilities for Physical Security Incidents.

a. **Employees.** Any employee who observes suspicious activity with respect to documents containing PII should take steps to notify appropriate FMC authorities and/or the building guard service immediately to prevent the theft of the information if at all possible.

b. **Supervisors** shall take steps to mitigate breaches, shall authorize employees to have access only to information needed to perform their jobs, shall use means to restrict access to documents containing PII, and shall take immediate steps to eliminate the method of access utilized during a breach and any related vulnerabilities.

c. **Appropriate Security Officer (for Information Security, Personnel Security, or Physical Security).** The appropriate Security Officer, as further defined in Commission Order 80, shall determine the appropriate procedures for handling each incident, in coordination with the appropriate supervisor, and shall make reports to the ART and assist the ART in determining appropriate procedures for sharing incident information outside the agency.

9. References.

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

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

c. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007)

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*

10. Inquiries.

Further information concerning this Managing Directive may be obtained by contacting the Managing Director's Office at (202) 523-5800, the Office of Information Technology at (202) 523-5835, or the Office of Management Services at (202) 523-5900.

Ronald D. Murphy
Managing Director