Document Revision History for: ______________________________________

Version	Date	Author	Change Description

SECTION 17 INCIDENT REPORTING

17.1 Purpose

This section addresses some general guidelines and procedures on what to do in the event of a computer security incident. The term incident in this document is defined as any irregular or adverse event that occurs within MARAD. Additional procedures for reporting technical vulnerabilities associated with Maritime Administration are also described in this document. The purpose of this section is as follows:

- Helping personnel quickly and efficiently recover from security incidents
- Minimizing loss or theft of information or Denial of Service (DOS) attacks, which result in disruption of critical computing services
- Supporting the need to respond systematically
- Protecting personnel and systems
- Using resources efficiently
- Incident reporting procedures

17.2 Background

A technical vulnerability is a hardware, firmware, communication, or software weakness, which leaves MARAD open for potential exploitation, either externally or internally, resulting in a security risk to MARAD, its data, and it's users. The following are examples of technical vulnerabilities:

- The use of software commands that unexpectedly disable protection features
- The failure of hardware to separate individual processes or to protect security relevant protective mechanisms from unauthorized access or modification
- A communications channel that allows two cooperating processes to transfer transmission violates the systems overall security policy
- A virus, operating systems exposures, rogue programs, Trojan horses, contamination, and intrusions and/or attempted intrusions.

17.3 Goal

The Goal of incident response planning is to provide reasonable methods for limiting the possibility of an adverse effect on MARAD's Information System due to the occurrence of an information system security incident, and for facilitating the rapid and successful investigation and reporting of an incident, should one occur.

17.4 References

17.4.1 "Escalation Procedures for Security Incidents," Compiled by Michele Crabb-Guel, as part of her classic SANS course on "Building An Effective Security Infrastructure." http://www.sans.org/newlook/resources/policies/policies.htm"

17.4.2 NSA Secure Configuration Guide & CERT CC Checklist

17.4.3 DOT Departmental Information Resources Management Manual (DIRMM) DOT H 1350.255 Departmental Guide to Incident Response Handling

17.4.4 NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems

17.5 Responsibilities

17.5.1 It is the responsibility of MARAD Administrators to ensure that MARAD's IT security program includes provisions for monitoring MARAD's IT systems and networks for IT security incidents and coordinate the notification and distribution of information pertaining to the incident to the appropriate parties (those who need to know) through a predefined escalation path). It is the responsibility of MARAD's Information System Security Officer (ISSO) to oversee MARAD's IT security program. All information concerning the incident is reported directly to the ISSO from network engineering

17.5.2 It is the responsibility of MARAD's system owners to ensure that they are monitoring their systems for evidence of IT security incidents and for reporting any incidents to the Information System Security Officer (ISSO).

17.5.3 It is the responsibility of MARAD's ISSO to manage the Agency's IT security incident monitoring and reporting processes. The ISSO will be the point of contact for the MARAD for all matters related to IT security incidents. The ISSO is responsible for preparing and transmitting all IT security incident reports to OST's Computer Incident Response Center (TCIRC). In the ISSO's absence, an alternate ISSO may assume IT security incident reporting responsibilities.

17.6 Regional Offices Incident Response Reporting

Regional offices review server logs for suspicious activity and submit incident reports of findings to the MARAD HQ network engineering section. These reports are consolidated and submitted to the ISSO for review. The ISSO manages distribution of findings, as appropriate.

17.7 Incident Response

17.7.1 Network engineering has the duties of preventing, detecting and responding to incidents. They manage the network logs, including collection, retention, review and analysis of data. Additionally, they manage the resolution of an incident; manage the remediation of a vulnerability, and provide post-event reporting to the ISSO and TCIRC.

17.7.2 The MARAD LAN Network Engineering section or security officer of the affected major application shall notify the MARAD Information System Security Officer (ISSO) and/or the MARAD CIO of the incident.

17.7.3 The MARAD ISSO shall notify the MARAD security officer and the MARAD CIO of the intrusion. In addition, the ISSO will ensure that an incident report is prepared and submitted, if circumstances warrant, through the DOT automated incident reporting system called Archer. The incident report will be reviewed by the Transportation Cyber Incident Response Center (TCIRC) to determine appropriate action. .

17.7.4 The CIO shall notify the responsible MARAD program officials shall be notified of the incident on an as-needed basis.

17.8 Quarterly Report

On a quarterly basis, MARAD's ISSO will provide the DOT OCIO IT Security Division with a consolidated incident report, in conjunction with the FISMA Quarterly Report that will include the following information:

- Total Number of Incidents, summarized by the following categories:
- Port Probes (attempts to access specific port(s))
- Port Scans (attempts to determine port(s) availability)
- HTTP Attacks (e.g. web defacements)
- Denial of Service (attacks directed to overwhelm network resources)
- Malicious Code (e.g. viruses, worms, Trojan horses)
- Other (e.g. I.P. spoofing, SMTP intrusions, widespread spam, etc.)
- Number of Incidents Reported to DOT OCIO by Category (see above categories)

17.9 Recovery Procedures

Computer security incident handling can be divided into six phases: preparation, identification, containment, eradication, recovery, and follow-up. Understanding these stages, and what can go wrong in each, facilitates responding more methodically and avoids duplication of effort.

17.9.1 Phase 1 Preparation: In the heat of the moment, when an incident has been discovered, decision-making may be haphazard. By establishing policies, procedures, and agreements in advance, you minimize the chance of making catastrophic mistakes. The following steps should be taken in the preparation phase:

17.9.1.1 Establish a security policy, develop management support for an incident handling capability, monitor and analyze the network traffic, assess vulnerabilities, configure your systems wisely, install updates regularly, and establish training programs.

17.9.1.2 Post warning banners.

17.9.1.3 Establish an organizational approach for handling incidents. Select incident handling team members and organize the team. Establish a primary point of contact and an incident command and communications center. Conduct training for team members. Involve system administrators and network managers early.

17.9.1.4 Establish a policy for notifying outside organizations that may be connected to operating unit systems.

17.9.1.5 Update the operating unit's business continuity plan to include computer incident handling.

17.9.1.6 Passwords and encryptions should be up-to-date and accessible.

17.9.1.7 Back up systems on a regular basis.

17.9.1.8 Report all significant incidents to the TCIRC using the template in Appendix 17-1.

17.9.2 Phase 2 Identification: Identification involves determining whether or not an incident has occurred, and if one has occurred, determining the nature of the incident. The following steps should be taken in the identification phase:

17.9.2.1 The ISSO will assign a person to be responsible for handling the incident.

17. 9.2.2 The ISSO will determine whether or not an event is actually an incident, in consultation with the person assigned to handle the incident. Checks for simple mistakes such as errors in system configuration or an application program, hardware failures, and most commonly, user or system administrator errors, should be part of the analysis of the incident.

17.9.2.3 Identify and assess the evidence in detail and maintain a chain of custody. Control access to the evidence.

17.9.2.4 Coordinate with the people who provide operating unit network services.

17. 9.2.5 Notify appropriate officials such as immediate supervisors or managers, MARAD's IT Security Officer, and the CIO. Significant incidents should be reported to TCIRC. TCIRC is responsible for escalating notification of the incident above MARAD level.

17. 9.3 Phase 3 Containment: During this phase the goal is to limit the scope and magnitude of an incident in order to keep the incident from getting worse. The following steps should be taken in the containment phase:

17.9.3.1 Deploy the on-site team to survey the situation.

17.9.3.2 Keep a low profile. Avoid looking for the attacker with obvious methods.

17.9.3.3 Avoid potentially compromised code. Intruders may install trojan horses and similar malicious code in system binaries.

17.9.3.4 Back up the system. It is important to obtain a full back up of the system in order to acquire evidence of illegal activity. Back up to new (unused) media. Store backup tapes in a secure location.

17.9.3.5 Determine the risk of continuing operations.

17.9.3.6 Change passwords on compromised systems and on all systems that regularly interact with the compromised systems.

17.9.4 Phase 4 Eradication: This phase ensures that the problem is eliminated and vulnerabilities that allow re-entry to the system are eliminated. The following steps should be taken in the eradication phase:

17.9.4.1 Isolate the attack and determine how it was executed.

17.9.4.2 Implement appropriate protection techniques such as firewalls and/or router filters, moving the system to a new name/IP address, or in extreme cases, porting the machine's function to a more secure operating system.

17.9.4.3 Perform vulnerability analysis.

17.9.4.4 Remove the cause of the incident.

17.9.4.5 Locate the most recent clean back up (to prepare for system recovery).

17.9.5 Phase 5 Recovery: This phase ensures that the system is returned to a fully operational status. The following steps should be taken in the recovery phase:

17.9.5.1 Restore the system.

17.9.5.2 Validate the system. Once the system has been restored, verify that the operation was successful and the system is back to its normal condition.

17.9.5.3 Decide when to restore operations. Management may decide to leave the system offline while operating system upgrades and patches are installed.

17.9.5.4 Monitor the systems. Once the system is back on line, continue to monitor for back doors that escaped detection.

17.9.6 Phase 6 Follow-up: This phase is important in identifying lessons learned that will prevent future incidents.

17.9.6.1 The person assigned the responsibility of handling the incident shall prepare a detailed incident report and provide copies to management, the operating unit's ISSO, and the TCIRC.

17.9.6.2 Send recommended changes to management.

17.9.6.3 Implement approved actions.

17.10 Incident Tracking

Incidents are monitored and tracked until resolved by the network engineering section, or by whoever is assigned incident handling responsibility. All relevant information concerning the incident, correcting the root problem leading to the incident, and returning the system to normal operations is documented.

17.11 Training

Annual security awareness training is provided for all MARAD system administrators. Additionally, periodic system specific security training is provided for system administrators.

17.12 Security Alerts and Patch Management

Security alerts are distributed on a daily basis by the ISSO, and may also be distributed by technology vendors. The most critical alert/advisory gets immediate attention:

17.12.1 The Security Team gets various alerts from multiple sources.

17.12.1.1 Alerts from the ISSO. The Security Team will receive an email from the ISSO of details of the latest Vulnerabilities, Outbreaks, Warnings, etc. involving any IT related systems, usually from TCIRC. The Security Team will review the findings and report back to the ISSO of any critically needed patches/fixes.

17.12.1.2 Alerts from Vendors. The Security Team receives email alerts from specific Vendors according to devices/software managed on MARAD's Network. These vendors include Microsoft, Network Associates, and CERT (Computer Emergency Response Team).

17.12.1.3 Alerts from Security Management Software/Hardware Systems, i.e. Cisco IDS, Mcafee Epolicy, Syslog, Cisco Works: Daily/Weekly Security Procedures are performed using these management software systems. The Security Team also reviews, updates, and applies fixes manually through the Vendor Web Sites, MS Server Update Utility, and Vulnerability Scans, in accordance with MARAD's Security Monthly Maintenance Plan.

17.12.2 Non-critical patches will be applied on a regular basis, but no less than once per month.

17.13 A Post Mortem Analysis is conducted

A post mortem analysis and review meeting is held within three to five days of the completion of the incident investigation. Questions asked include:

17.13.1 Did detection and response procedures work as intended? If not, why not?

17.13.2 Are there any additional procedures that would have improved the ability to detect the incident?

17.13.3 What improvements to existing procedures and/or tools would have aided in the response process?

17.13.4 What improvements would have enhanced the ability to contain the incident?

17.13.5 What correction procedures would have improved the effectiveness of the recovery process?

17.13.6 What updates to policies and procedures would have allowed the response and/or recovery processes to operate more smoothly?

17.13.7 How could user and/or system administrator preparedness be improved?

17.13.8 How could communication throughout the detection and response processes be? improved?

17.13.9 The results of these and similar questions are incorporated into a report for senior management review/comment.

17.14 Reporting

17.14.1 The incident is documented and reported by the person assigned the responsibility for handling the incident by the ISSO. The reporting form "MARAD Computer Incident Response Form" at the end of this Section 17 shall be used to prepare the incident report. The ISSO will be briefed and the report will be distributed according to the instructions of the ISSO.

17.14.2 The ISSO will determine if the report should be forwarded to TCIRC. In the ISSO's absence, the report will be submitted to TCIRC, and the ISSO will be briefed at a later date.

17.15 MARAD Incident and Intrusion Response Tips

17.15.1 DON'T

☒ Finger, attempt to access the source, or contact the source.
☒ Change the system files on the suspected/compromised system.
☒ Connect to the system over the network.

17.15.2 DO

☑ Unplug the machine from the network (if mission will allow).
☑ Log-on as system administrator at the server console and do a complete dump of the system.
☑ Make sure you do not alter any files on the system.
☑ Place the complete dump in a secure location.
☑ Place the suspected/compromised system in a secure place. (Limit access to the system).
☑ Complete the Computer Incident Response Form and give all information to the ISSO, and distribute the report to other parties designated by the ISSO.

Appendix 17-1

MARAD Computer Incident Response Form

If you suspect or know a system is compromised, please follow procedures and complete the form.

(**The information below is provided as a sample**.)

1. Report Originator Information:	
Name:	Enter Name of Report Generator
Address:	MARAD
Phone Number:	202-366-6472
Fax Number:	202-366-0419
Position (administrator, security manager, etc.):	Exchange Administrator
E-mail Address:	reportgeneratorname@dot.gov
Date and time first noticed:	05 / 12 / 03 , 06 : 37 (AM)
2. Target Information (if additional targets use separate sheet):	
Network Domain and Host Name (i.e., marad.dot.gov):	marad.dot.gov
IP Address (i.e., 192.168.1.1):	152.119.120.43
Subnet Mask:	255.255.255.0
Computer Model (i.e., Network Server):	Network server
Operating System/Version (Windows NT or 2000):	____ Unix ____ Linux ____ OS2 __X_ Windows NT ____ Windows 2000 ____ Windows XP _____VAX/VMS ____ Sun OS/Solaris ____ Other: _____ **(Provide operating system, version, release numbers if known)**
Security Classification Level:	
Security Classification (i.e., SBU, Secret, etc.):	
Network/System Mission (i.e., administration, communications):	
Network Structure/Type:	
How Detected:	Virus program ScanMail on server detected and deleted the virus infected attachment.
Impact on Mission (if compromised):	Not compromised

3. Security infrastructure in place	
Auditing	*Yes X*
	No ☐
	Type
Firewall	*Yes* X
	No ☐
	Type
IDS	*Yes* X

	No ☐
	Type
System Status	*On-Line X*
	Off-Line ☐

4. Attack Session Information (correlates with the target information)

(If known, include; if unknown, leave blank; and do not access system files)

Date/dates and time of the Session	*Start: May 11, 2003, 12:00:35*
	Stop: May 11, 2003, 12:00:36
Attack Method	Virus
Source IP	
Source Host and Netblock name (if available):	*Host:*
	Netblock:
Organization:	MARAD
Country:	USA

5. Countermeasure(s) Installed (e.g., patches, TCP wrappers, shadow passwords, etc.)

Name and date installed (If known, include; if unknown, leave blank and don't access system files):	Verified that all Exchange servers had updated virus files.

Reviewed By:

Approved By:

6. Brief Scenario (Description of Incident or Intrusion)

____ Web site defacement	____ Theft	____ Intrusion
____ Unauthorized root access	____ Hoax	__X__ Virus/worm
____ Probe(s)	____ Port scans	____ Malformed packets
____ Denial of service	____ Email scams	____ Sys/network vulnerability exploited

_____
_____
_____

7. Notification Checklist (Indicate full name, date, and time notified):

Information System Security Manager (ISSM):	
Information System Security Officer (ISSO):	
System Owner:	
Designated Approving Authority (DAA):	
Computer Incident Response Team (CIRT):	

Emergency Point of Contact Listing

Title	Name	Work	Cell
Information System Security Officer	Mr. Kenneth R. Moore Kenneth.Moore@ dot.gov	202 366-8805	202 306-7228

System Owner	Ms Donna Seymour Donna.Seymour@marad.dot.gov	202-366-1941	202-253-1805
Manager	.Mr. Louis Effa Louis.Effa@.dot.gov	.202-366-9727	.