DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

and
Headquarters
United States Marine Corps
Washington, DC 20380-1775

IN REPLY REFER TO

OPNAVINST 2201.2
N6
CMC (C4I)

3 MAR 1998

OPNAV INSTRUCTION 2201.2

From: Chief of Naval Operations
Commandant of the Marine Corps
To: All Ships and Stations

Subj: NAVY AND MARINE CORPS COMPUTER NETWORK INCIDENT RESPONSE

Ref: (a) NSTISSP No.5 of 30 Aug 93, National Policy for Incident Response and Vulnerability Reporting for National Security Systems (NOTAL)
(b) DOD Directive S-3600.1 "Information Operations (U)" of 9 Dec 96 (NOTAL)
(c) NTISSD No. 503 of 30 Aug 93, Incident Response and Vulnerability Reporting for National Security Systems (NOTAL)
(d) NAVSO P-5239-19 of Aug 96, Computer Incident Response Guidebook (NOTAL)
(e) Electronic Communications Privacy Act of 1986 (NOTAL)
(f) SECNAVINST 5239.3 "DON Information Systems Security (INFOSEC) Program" (NOTAL)

1. Purpose. To establish requirements and procedures for Navy and Marine Corps to detect, respond, and report computer network incidents.

2. Application. The provisions of this instruction apply to all commands, components, and activities of the U.S. Navy and Marine Corps.

3. Scope

a. Emerging as an overarching strategy, the discipline of information operations (IO) and its subset of information warfare (IW) encompass not only actions that may be taken to potentially affect an adversary's information or information systems, but also address those defensive aspects necessary to ensure that U.S information and information systems are protected against attack. This defensive aspect of IO/IW falls under the subset called information warfare - defense (IW-D)/information assurance (IA). The Navy and Marine Corps IW-D/IA policy, when properly applied, will provide the tools/procedures to ensure a basic defense of USN/USMC information and automated information systems (References (a) through (f) are germane). The detection, response, and reporting of attempts by unauthorized persons to gain access to Navy and Marine Corps computer networks is critical to the success of this IW-D effort.

b. This instruction does not pertain to:

(1) Communication security monitoring as defined in NTISSD 600.

(2) Signals Intelligence (SIGINT), foreign intelligence and counter-intelligence collection activities.

(3) Interception of communications for law enforcement purposes.

(4) Vulnerability assessments conducted by systems commands to determine new system technical insecurities or to accomplish integration and installation of systems.

(5) On-Line-Surveys and Red Teaming conducted during audits and fleet exercises.

4. Definitions. For the purposes of this document, the following terms are defined:

a. Technical Vulnerability - a hardware, firmware, or software weakness or design deficiency that leaves an information system open to potential active or passive exploitation thereby resulting in risk of compromise of information, alteration of information, or denial of service.

b. Administrative Vulnerability - a security weakness caused by incorrect or inadequate implementation of a system's existing security features by the system administrator, security officer, or users. An administrative vulnerability is not the result of a design deficiency but is characterized by the fact that the full correction of the vulnerability is possible through a change in the system's security feature settings/switches or the establishment of a special administrative or security procedure for the system administrators and users.

c. U.S. Navy/Marine Corps Computer Networks - a system of systems, inter-related or interconnected through U.S. Government, commercial and private networks. Examples are the NIPRNET, SIPRNET, JWICS, as well as weapon systems links. These networks have numerous applications, including command and control, weapon control, air traffic control, law enforcement, medical, electric power, transportation, and physical security.

d. Computer Network Attack - operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

e. Computer Network Security Incident - an attempt to exploit or defeat the security features associated with a Navy or Marine Corps computer system such that the actual or potential adverse effects of the computer network attack may involve the compromise of information, loss or damage of property or information, or denial of service.

f. Computer Incident Response - actions conducted to resolve information systems security incidents, restore system to operational status, and provide technical and administrative correction to protect system from further attacks.

g. Information Assurance - IO that protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

5. Policy

a. Reference (a) establishes the requirement to collaborate and cooperate with other appropriate organizations in the sharing of incident, vulnerability, threat, and countermeasures information concerning those systems. Reference (b) specifies that the Service Departments shall vigorously pursue activities to prevent adversarial effects on their information and information systems, and shall work toward a multi-layered information systems defense that incorporates protection, detection, reaction, and reconstitution using risk-based management principles.

b. In accordance with references (a) and (b), and in response to the growing and more sophisticated threat to computer systems being encountered as new technologies are introduced, the Navy has incorporated the naval computer incident response team (NAVCIRT) as part of the Fleet Information Warfare Center (FLTINFOWARCEN). The FLTINFOWARCEN has overall responsibility for an analysis and response capability to detect, respond, restore, and report attacks and intrusions of Navy and Marine Corps computer network systems.

c. Attacks against Navy and Marine Corps computer systems could be an indication of, or associated with, an organized attack targeted against the entire Defense information infrastructure (DII). To identify and respond to such attacks, all service and national level agencies must work together to detect, protect, and react to computer network attacks and threats. To support this effort, the FLTINFOWARCEN is the designated unit responsible for such coordination and reporting of all Navy and Marine Corps computer incidents to national level agencies.

d. All commands, units, and activities in the Navy and Marine Corps will report any computer intrusion incident, or suspicion of one, to the FLTINFOWARCEN. This reporting is in addition to the requirements levied upon specific Navy and Marine Corps commands by the Defense Intelligence Agency and National Security Agency/Central Security Service.

6. Action

a. Commanding Officer/Officer in Charge. Report all computer network attacks/intrusion incidents against Navy and Marine Corps systems to the FLTINFOWARCEN by the most expeditious means. Paragraphs 6a(1) and 6a(2) contain specifics concerning means and report format. Reports will be protected from public disclosure but classified at the lowest possible level. Unclassified reports should be marked For Official Use Only (FOUO).

(1) Reporting of computer intrusion incidents: Notification of computer intrusion incidents and requests for assistance should be forwarded to the FLTINFOWARCEN via the following means:

(a) Niprnet/Internet:
navcirt@fiwc.navy.mil

(b) Telephone:
DSN 537-4024
Comm (757) 417-4024 or 1-888-NAV-CIRT
24 hour Pager Service: 1-888-402-4236

(c) Facsimile:
Unclass Fax (Attn: NAVCIRT): Comm (757) 417-4031

(d) Naval Message:
FLTINFOWARCEN NORFOLK VA//NAVCIRT//

(2) Reporting format: Reports by units experiencing computer network incidents can be transmitted via any of the above systems. Reports should include as much of the following information as possible; however, reporting should not be delayed in order to gain additional information. Reports submitted via message means should use the following format:

FM NAVY/MARINE CORPS/ACTIVITY/SHIP/CODE//

TO FLTINFOWARCEN NORFOLK VA//NAVCIRT//

INFO (APPROPRIATE CHAIN OF COMMAND)
CNO//N6/N64//
CMC//C4I//

//(APPROPRIATE CLASSIFICATION)//N02201//

SUBJ: POSSIBLE COMPUTER INTRUSION INCIDENT

MSGID/GENADMIN/ //

REF/A/DOC/OPNAVINST 2201.

RMKS/

1. Incident date
2. Physical location of the system attacked
3. How was the attack identified
4. How access was obtained
5. Vulnerability exploited
6. Actions attempted during session
7. Highest classification of information involved
8. Evaluation of attack success
9. Damage or effects resulting from attack
10. Hardware Configuration
11. Operating System
12. Security Software installed
13. Origination point of incident

14. Indication of additional activity
15. IP address
16. Names used
17. Mission of system attacked (e.g. administration, command and control, message handling, etc.)
18. Point of contact (e.g. name, phone number, e-mail address)
19. Additional information

(3) Viruses: Those known viruses with countermeasures available in the NAVCIRT tool-kit should be logged and reported to FLTINFOWARCEN on a monthly basis. Only those viruses not known or without an available countermeasure will be reported in accordance with paragraph 6a(2).

b. Fleet Information Warfare Center (FLTINFOWARCEN). FLTINFOWARCEN will coordinate overall Navy and Marine Corps computer network security systems vulnerability and incident reporting and responses. Paragraphs 6b(3)(a) and 6b(3)(b)contain specifics concerning means and report format.

(1) The Commanding Officer, FLTINFOWARCEN will be responsible for:

(a) facilitating cooperation among other service and national level organizations and agencies in sharing information concerning Navy and Marine Corps computer network security incidents.

(b) establishing an effective and timely response to computer security incidents, to include computer network attacks against or associated with Navy and Marine Corps computer networks.

(c) obtaining and using network intrusion detection tools, incident response methods, countermeasures, and advance technologies.

(d) providing the Chief of Naval Operations, Commandant of the Marine Corps, and Executive Agent for IW with global intrusion and detection capabilities/incident reporting of information systems under their purview.

(e) timely reporting of violation of law to appropriate law enforcement agencies.

(2) To accomplish these objectives, the CO, FLTINFOWARCEN will:

(a) establish and operate a computer incident response center to centrally coordinate actions involving computer network security incidents and vulnerabilities which threaten Navy and Marine Corps computer networks worldwide.

(b) man the computer incident response center with qualified personnel to provide a 24 hour/7 day a week capability with adequate numbers to monitor remote sensors on all deployed naval units and the world-wide naval shore AIS infrastructure.

(c) develop, review, and revise procedures and guidance for the NAVCIRT Program, leveraging Defense Information Systems Agency (DISA) and other services' efforts to minimize duplication and ensure standardize reporting.

(d) review all reported computer network security systems vulnerabilities and incidents; evaluate the requirements for and extent of follow-up actions.

(e) when required, report Navy and Marine Corps computer network security incidents to Navy and Marine Corps authorities using the format contained in paragraph 6b(3).

(f) as appropriate, coordinate with and report to other services and national agencies concerning Navy and Marine Corps computer network incidents.

(g) report Navy and Marine Corps computer security incidents involving violations of law to the appropriate authority.

(h) man computer incident response teams that are trained and equipped to quickly respond world-wide to emerging naval computer network security incidents.

(i) facilitate the development and use of specialized technical tools.

(j) ensure proper handling of incident data.

(3) FLTINFOWARCEN Computer Network Incident Reporting:

(a) FLTINFOWARCEN will report all computer network incidents evaluated as being of interest to Navy and Marine Corps officials by priority message as outlined in paragraph 6b(3)(b). Initial reporting should not be delayed in order to gain additional information. Updates and additional information should be provided via amplification reports. Events deemed trivial (e.g., ping on a single system, unsuccessful logins) should not be reported.

(b) Reporting format: Until a standardized joint reporting format is adopted, reports will include as much of the following information, in non-technical terms, as possible:

```
FM FLTINFOWARCEN NORFOLK VA//00//

TO CINCLANTFLT NORFOLK VA//N02C//
CINCPACFLT PEARL HARBOR HI//N339/N3DC//
CINCUSNAVEUR LONDON UK//N9//
COMUSNAVCENT//N6//
CNO WASHINGTON DC//N6/N64/N31/N312/N515//
CMC WASHINGTON DC//P/C4I/PLI/CSB/CIS//
(OTHER APPROPRIATE COMMANDS)
INFO COMNAVSECGRU FT GEORGE G. MEADE MD//N6/N6P//
DON CIO WASHINGTON DC
(OTHER APPROPRIATE COMMANDS)
//(APPROPRIATE CLASSIFICATION)//N02201//

SUBJ: POSSIBLE COMPUTER INTRUSION INCIDENT

MSGID/GENADMIN//

REF/A/DOC/OPNAVINST 2201.

RMKS/
1. Summary
2. Incident date
```

3. Physical location of the system attacked
4. How was the attack identified
5. How access was obtained
6. Vulnerability exploited
7. Actions attempted during session
8. Highest classification of information involved
9. Evaluation of attack success
10. Damage or effects resulting from attack
11. Origination point of incident
12. Indication of additional activity

(c) Incidents which could have a major impact on Navy and Marine Corps operations or that are evaluated as requiring immediate notification of the CNO and the CMC (e.g., confirmed penetration, access to classified information, gaining system administrator privileges, denial of service, access to password/privilege files, indication of multiple system attacks (whether successful or not), or attempts confirmed to be originating in a foreign country) should be forwarded via Navy OPREP BLUE message. These OPREP BLUE messages will be addressed to OPNAV Command Center and the USMC Command Center for ACTION, DON CIO, CNO (N64), COMNAVSECGRU (N6), FLTCINCs, and the appropriate operational chain of command for INFORMATION. Information contained in the body of the OPREP BLUE messages should be formatted as outlined in the paragraph 6b(3)(b).

(d) Reporting associated with Navy and Marine Corps computer network incidents will be protected from public disclosure but classified at the lowest possible level. Unclassified reports should be marked For Official Use Only (FOUO).

7. Authority. As appropriate to all threats, commanding officers will take appropriate actions to defend commands. This applies equally to their computer networks as it does to physical security. No requirement for immediate reporting shall override this basic requirement.

8. Reports. The reporting requirements contained in this instruction are exempt from reports control per SECNAVINST 5214.2B.

Joseph T Anderson
Joseph T. Anderson
MAJGEN, USMC
AC/S C4I

AK Cebrowski
A. K. CEBROWSKI
Vice Admiral, U.S. Navy
Director, Space, Information
Warfare, Command and Control (N6)

Distribution:
SNDL Parts 1 and 2
MARCORPS PCN 10203352700