



DEPARTMENT OF THE NAVY

OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 5239.19

DON CIO

18 March 2008

SECNAV INSTRUCTION 5239.19

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY COMPUTER NETWORK INCIDENT RESPONSE
AND REPORTING REQUIREMENTS

Ref: (a) SECNAVINST 5239.3A, Department of the Navy
Information Assurance (IA) Policy, of 20 Dec 04
(b) DOD Directive O-8530.1, Computer Network Defense
(CND), of 8 Jan 01
(c) DOD Instruction O-8530.2, Support to CND, of 9 Mar 01
(d) Chairman of the Joint Chief of Staff Manual (CJCSM)
6510.01, Defense-in-Depth: Information Assurance (IA)
and CND, of 8 Mar 06
(e) CNSS Instruction 4009, National Information Assurance
Glossary, of Jun 06
(f) DOD Directive 8500.1, Information Assurance (IA), of
24 Oct 02
(g) DOD Instruction 8500.2, IA Implementation, of 6 Feb
03
(h) National Telecommunications and Information Systems
Security Directive (NTISSD) No. 600, Communications
Security (COMSEC) Monitoring, of 10 Apr 90
(i) Joint DODIIS/Cryptologic Sensitive Compartmented
Information (SCI) Systems Security Standards,
Revision 4, of 1 Jan 06
(j) National Telecommunications and Information Systems
Security Instruction (NSTISSI) No. 4003, Reporting
and Evaluating COMSEC Incidents, of 02 Dec 91
(k) SECNAVINST 5430.107, Mission and Functions of the
Naval Criminal Investigative Service, of 28 Dec 05
(l) SECNAV M-5510.36, DON Information Security Program,
of 30 Jun 06

Encl: (1) List of Acronyms
(2) Glossary
(3) Reference Amplification and Location Table
(4) Incident Categories

1. Purpose. Establish Department of the Navy (DON) incident response policy consistent with reference (a) to align and integrate DON computer incident response and reporting requirements with the Department of Defense (DOD) policy guidance outlined in references (b) through (d).
2. Cancellation. None.
3. Acronyms, Definitions, and References. Acronyms used in this instruction are defined in enclosure (1). Definitions used in this instruction from references (e), (f), and (g) are contained in enclosure (2). Enclosure (3) contains an overview of sources for references and a reference location table.
4. Objectives
 - a. Ensure an integrated and consistent DON approach in Computer Network Defense (CND) incident reporting and timelines per reference (d).
 - b. Define CND incidents as actual or potential adverse operational or technical impact to the DON networks.
 - c. Establish a baseline incident handling methodology to be followed by local network security personnel, the Navy Cyber Defense Operations Command, or the Marine Corps Network Operations and Security Center to detect, contain, assess and report relevant information on CND incidents.
 - d. Provide Commander's Critical Information Requirements for CND incident reporting.
5. Background
 - a. Per reference (a), the DON has implemented a defense-in-depth strategy to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of its information and information systems. This strategy is based on the concept that attacks forced to penetrate multiple protection layers are less likely to succeed. In addition to this layered approach, protection mechanisms are distributed among multiple locations, and each component of defense within the system provides an appropriate level of robustness. The objective under this strategy is risk management.

b. The CND embodies incident detection and response, a critical part of defense-in-depth. The CND synchronizes the technical, operational, and intelligence assessments of a computer attack in order to defend against it. The Joint Task Force for Global Network Operations (JTF-GNO), under U.S. Strategic Command, is the lead organization designated to identify and mitigate threats to DOD information networks and direct the defense of the Global Information Grid (GIG). For the Navy, the Naval Network Warfare Command (NAVNETWARCOM) is the Service component to JTF-GNO while Navy Cyber Defense Operations Command (NCDOC) is the designated Computer Network Defense Service Provider (CNDSP). For the Marine Corps, the Marine Corps Network Operations and Security Center (MCNOSC) is both the Service component to JTF-GNO and the designated CNDSP.

c. Reference (e) defines an incident as an assessed occurrence having actual or potentially adverse effects on an information system. This includes, but is not limited to, attempted entry, unauthorized entry, malicious code execution, and/or an information attack on an information system as indicated by categories in enclosure (4).

6. Scope

a. This instruction applies to:

(1) All Commands, Components, and activities within the Department of the Navy.

(2) All DON owned, DON controlled, and DON-contractor owned information systems that receive, process, store, display, or transmit DOD information, regardless of mission assurance category, classification, or sensitivity.

b. This instruction does not pertain to, alter, or supersede:

(1) Existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence.

(2) Communication security monitoring as defined in reference (h).

(3) Signals Intelligence (SIGINT), foreign intelligence, or counter-intelligence collection activities.

(4) Interception of communications for law enforcement purposes.

(5) Authorized vulnerability assessments conducted by systems commands to determine new system technical vulnerabilities or to accomplish integration and installation of systems.

(6) Cooperative Assessments conducted during audits.

(7) Electronic spillage defined as a situation where information of higher classification than a system is authorized to process is introduced into that system, intentionally or otherwise.

7. Action. Commanders/Commanding Officers/Officers-in-Charge/Directors hereafter referred to as Commanders of DON organizations, shall:

a. Report all incidents, as described in enclosure (4) and directed by respective CNDSPs, using the proper classification level (i.e., incidents occurring on unclassified networks such as the Non-Classified Internet Protocol Router Network (NIPRNET) or Defense Research and Engineering Network (DREN) reported via appropriate means, and incidents occurring on classified networks such as the Secret Internet Protocol Router Network (SIPRNET) or Secure Defense Research and Engineering Network (SDREN) reported via classified means). Incidents identified which carry potential grave impact to the operation and sustainment of any DON network or information system should be forwarded immediately to the respective CNDSP through designated channels as indicated by the CNDSP:

(1) Navy reports incidents to Navy CNDSP, which is the Navy Cyber Defense Operations Command (NCDOC):

NIPRNET: <https://www.ncdoc.navy.mil/>
E-mail: ncdoc@ncdoc.navy.mil

SIPRNET: <http://www.ncdoc.navy.smil.mil/forms.php>
E-mail: cndwo@ncdoc.navy.smil.mil

Telephone:
DSN: (312) 537-4024
Commercial: (757) 417-4024 or
Toll Free: 1-888-NAVCDOC (1-888-628-2362)
STU/STE: (312) 537-7952/(757) 417-7952
Plain Language Address: NCDOC NORFOLK VA

(2) Marine Corps reports incidents (including electronic spillages) to Marine Corps CNDSP, which is the Marine Corps Network Operations and Security Center (MCNOSC):

NIPRNET: <https://www.mcnosc.usmc.mil/>
E-mail: commandcenter@mcnosc.usmc.mil

SIPRNET: <http://www.mcnosc.usmc.smil.mil/>
E-mail: commandcenter@mcnosc.usmc.smil.mil

Telephone:
DSN: 278-5300
Commercial: (703) 784-5300

Facsimile:
DSN: 378-1445
Commercial: (703) 432-1445
Plain Language Address: MCNOSC QUANTICO VA

b. Follow all initial reports to the respective CNDSP with interim updates as required and a complete close-out report per reference (d).

c. Contact the network manager immediately to initiate corrective actions for centrally managed networks (i.e., call the help desk).

d. Report and respond to Sensitive Compartmented Information (SCI) network incidents per reference (i).

e. Report losses or compromises of classified information technology (IT) systems, terminals, or equipment to CNO (N09N2) per reference (l).

f. Take the following actions, or ensure the network manager (for centrally managed networks) takes the following actions, at a minimum, in response to confirmed or suspected incidents:

(1) Ensure local or regional information assurance (IA) personnel submit required reports, collect and preserve incident evidence, and act as the primary liaison between the CNDSP and their command.

(2) Consult with respective CNDSP before disconnecting suspect computer(s) from the network upon initial indication or notification of an incident. Do not attempt to troubleshoot or disturb computer(s) in any way. Do not shut down until authorized by the CNDSP.

(3) Have experienced system administrator(s) examine audit and system logs ONLY if directed by the CNDSP. Otherwise, system should remain undisturbed.

(4) If trained personnel are available, capture volatile data, then image and ship computer hard drives to the CNDSP for forensic analysis when requested or required.

(5) Isolate and quarantine backup drives/tapes. Do not attempt to restore any systems using backup drives/tapes unless authorized by the CNDSP.

(6) Continue liaison with the CNDSP from initial incident notification/identification through final incident closure.

g. Protect reports associated with computer network incidents from public disclosure but classify them at the lowest possible level.

h. Report all incidents that have the potential to jeopardize Communications Security (COMSEC) information or material as a Physical COMSEC incident in accordance with reference (j).

8. Responsibilities

a. The Department of the Navy Chief Information Officer (DON CIO) shall:

(1) Develop information security policies sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the DON.

(2) Ensure coordination of IA and CND issues with other military departments, defense agencies, national level organizations, and DOD.

(3) Report periodically, in coordination with other senior officials, to the Secretary of the Navy on the effectiveness of the DON IA and CND program, including progress on remedial actions.

(4) Utilize the reporting incident information to assess the effectiveness of DON IA and CND policy and adjust as required.

(5) Coordinate risk management across the DON by balancing threat against system/data criticality to identify and implement practical solutions.

(6) Ensure incident trends are captured and reflected in DON-wide policy.

b. The Chief of Naval Operations (CNO) and Commandant of the Marine Corps (CMC) shall:

(1) Coordinate overall respective Service computer network defense actions to mitigate security vulnerabilities and to direct incident handling and reporting to Commanders of DON organizations.

(2) Coordinate with the other Services and agencies to share information concerning vulnerabilities, threats, countermeasures, and respective Service cyber defense incidents.

(3) Report all root level intrusions, user level intrusions, denial of service, malicious logic incidents, and any suspect or anomalous incidents (Categories 1, 2, 4, and 7) to the Naval Criminal Investigative Service (NCIS) immediately. Report such incidents to NCIS for investigation and incident response as detailed in references (k) and (l).

Enclosure (4) describes each incident category. Navy and Marine Corps CNDSP personnel, including contractors (or subcontractors at any tier), will cooperate and assist NCIS personnel in the use and performance of any legally authorized investigative technique deemed necessary and permissible by NCIS investigators.

(4) Implement DON incident response methods, countermeasures, and technologies. Operate a 24/7 cyber defense operations watch for rapid response to cyber events. In response to high priority threats, the respective Navy CNDSP Cyber Tactical Team or the MCNOSC Fly-Away Teams will provide global response and mitigation across the respective Service's GIG. Provide trained and equipped personnel to quickly respond to worldwide emerging DON cyber defense incidents.

(5) Monitor all respective Service network protection devices, including routers, firewalls, remote Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), and other network and system protection systems for protecting Service assets worldwide.

(6) Review all reported computer network protection vulnerabilities and incidents, evaluate the requirements for and extent of follow-up actions to ensure accurate situational awareness of threats to the GIG. Coordinate all cyber defense incidents with the NCIS and appropriate law enforcement, DOD, and national agencies.

(7) Root level intrusions, user level intrusions, denial of service, and malicious logic (Categories 1, 2, 4, and 7) are of high interest to the DON. Provide current status of all high interest (Categories 1, 2, 4, and 7) NIPRNET computer network incidents, including any incident that could create media attention or Secretary of the Navy (SECNAV) level attention, to

the DON CIO. Report identified incident trends to the DON CIO to ensure proper DON-wide policy changes and additions.

c. Naval Criminal Investigative Service (NCIS) shall:

(1) Contribute to CND by conducting investigations, operations, proactive programs, and related analyses of cyber incidents and targeting involving DON IT assets.

(2) Collect, track, and report on threats to DON IT assets and disseminate this information to other law enforcement agencies, DOD, DON, and other national agencies as needed.

(3) Conduct cyber-related criminal investigations regarding root level intrusions, user level intrusions, denial of service, malicious logic incidents, and aforementioned suspected incidents (Categories 1, 2, 4, and 7). Enclosure (4) provides explanations of all categories.

(4) Maintain a staff skilled in the investigation of computer crime. The staff should be sufficient in size to handle multiple major incidents and respond to increasing demands of the Department of the Navy.

9. Reports. The reports specified in this instruction are exempt from reports controlled by SECNAVINST 5210.16.

10. Effective Date. This instruction is effective immediately.


Robert J. Carey
Department of Navy
Chief Information Officer

Distribution:

Electronic only, via Department of the Navy Issuances Website
<http://doni.daps.dla.mil>

LIST OF ACRONYMS

C2	Command and Control
CND	Computer Network Defense
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
CNSS	Committee on National Security Systems (formerly the Committee on National Security Telecommunications and Information Systems Security)
COMSEC	Communications Security
DCI	Director of Central Intelligence
DOD	Department of Defense
DODD	DOD Directive
DODI	DOD Instruction
DODIIS	DOD Intelligence Information System
DON	Department of the Navy
GIG	Global Information Grid
IA	Information Assurance
IAVM	Information Assurance Vulnerability Management
IDS	Intrusion Detection System
INFOSEC	Information Security
IPS	Intrusion Prevention System
IT	Information Technology
JTF-GNO	Joint Task Force-Global Network Operations
MCNOSC	Marine Corps Network Operations and Security Center
NCDOC	Navy Cyber Defense Operations Command
NSA	National Security Agency
NSS	National Security Systems
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
SCI	Sensitive Compartmented Information
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SISS	Subcommittee for Information Systems Security
STS	Subcommittee for Telecommunications Security
VA	Vulnerability Assessment

GLOSSARY

Computer Incident Response: Actions conducted to resolve information systems security incidents, restore systems to operational status, and provide technical and administrative corrections to protect systems from further attacks.

Computer Network Attack (CNA): Operations which disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers/networks themselves. (CJCSM 6510.01 reference (d))

Computer Network Defense (CND): Actions taken to protect, monitor, analyze, detect, and defensively respond to unauthorized activity within DOD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND employs IA protection activity and includes deliberate actions taken to modify assurance configurations or conditions in response to CND alerts or threat information. Monitoring, analysis, and detection activities, including trend and pattern analysis, are performed by multiple disciplines within the DOD (e.g., network operations, CND Services, intelligence, counterintelligence, and law enforcement). CND response can include recommendations or actions by network operations (including information assurance), restoration priorities, law enforcement, military forces, and other U.S. Government agencies. (Reference (b))

Denial of Service (DOS) (attack): Result of any action or series of actions that prevents any part of an information system from functioning. (Reference (e))

Electronic Spillage: Information of higher classification or restrictive nature intentionally or inadvertently placed on machines/networks of lower classification/less restrictive policy.

Event: Any observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash, and packet flooding within a network. Events sometimes provide indication that an incident is occurring. (Reference (d))

Global Information Grid (GIG): Globally interconnected, end-to-end information capabilities, associated processes and personnel for collecting, processing, storing, managing, and disseminating information on demand to war fighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalitions, allied and non-DOD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data/information for use by other equipment, software, and services. (Reference (c))

Incident: An assessed occurrence having actual or potentially adverse effects on an information system. (Reference (d))

Intrusion: Unauthorized access to an information system. (Reference (d))

Information Assurance (IA): Information Operations 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. (Reference (g))

Malicious Logic: Hardware, software, or firmware capable of performing an unauthorized function on an information system. (Reference (e))

Virus: A program that embeds itself into other programs. When those other programs are executed, the virus is also executed, and attempts to copy itself into more programs. Viruses, by definition, can "infect" any executable code. Accordingly, they are found on floppy and hard disk boot sectors, executable programs, in macro languages, and executable electronic mail attachments.

Vulnerability: A weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system.

REFERENCES

1. Reference (a) establishes IA policy for the DON and requires commands to report computer incidents.
2. Reference (b) establishes DOD CND policy, definitions, and responsibilities and specifically requires CND-related activity reporting. Part 5.12 sets forth DOD Component requirements for establishment of a certified CNDSP and assignment of all Component information systems and computer networks to that certified CNDSP.
3. Reference (c) implements reference (b) policy. Part 5.5 directs Component Heads to ensure compliance with reporting requirements set forth in reference (d) and to set forth requirements to contribute to network situational awareness, plan/provide for a Common Operational Picture (COP), and establish a CNDSP.
4. Reference (d) provides guidance and procedures for implementing the IA defense-in-depth strategy and standards. Appendix B to Enclosure B contains incident and vulnerability reporting guidelines, including incident categories and timelines.
5. Reference (e) defines terms used in DOD IA.
6. Reference (f) establishes policy and assigns responsibilities to achieve DOD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
7. Reference (g) implements reference (f) requirements. Part 5.7.9 requires vulnerability mitigation and incident response/reporting capability to limit damage and restore service following an incident. It also requires collection/retention of audit data to support technical analysis relating to misuse, penetration reconstruction, or other investigations and to provide this data to appropriate law enforcement or other investigating agencies. Part E3.4.1.3 defines outsourced IT-based services and sets reporting requirements.

8. Reference (h) establishes policy and basic procedures and assigns responsibilities for conducting Communications Security (COMSEC) monitoring activities.
9. Reference (i) Chapter 8 provides SCI incident reporting guidelines.
10. Reference (j) provides guidance on reporting and evaluating COMSEC Incidents, and requires that all incidents involving COMSEC material are reported and evaluated promptly so action can be taken to minimize adverse impacts on security, take recovery measures, and prevent similar incidents from occurring.
11. Reference (k) provides mission and guidance of NCIS.
12. Reference (l) provides guidance for the loss or compromise of classified information.

REFERENCE LOCATION TABLE

REF	SUBJECT	LOCATION
a	SECNAVINST 5239.3A, DON Information Assurance Policy, 20 Dec 04	http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.3A.pdf
b	DODD O-8530.1, Computer Network Defense (CND), 8 Jan 01	https://powhatan.iiie.disa.mil/policy/DODD_O_8530.1.pdf (A DOD PKI Certificate is required for access) Accessed from the DISA Policy homepage: http://iase.disa.mil/policy.html
c	DODI O-8530.2, Support to Computer Network Defense (CND), 9 Mar 01	https://powhatan.iiie.disa.mil/policy/DODI_O_8530.2.pdf (A DOD PKI Certificate is required for access) Accessed from the DISA Policy homepage: http://iase.disa.mil/policy.html
d	CJCSM 6510.01 Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), verified current, 08 Mar 06	https://ca.dtic.mil/cjcs_directives/cdata/limited/m651001.pdf (Restricted to .gov and .mil access) Accessed from the DISA Policy homepage: http://iase.disa.mil/policy.html
e	CNSS Inst 4009, National Information Assurance Glossary, Jun 06	http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
f	DODD 8500.1, Information Assurance (IA), 24 Oct 02	http://www.dtic.mil/whs/directives/corres/html/85001.htm Accessed from the DISA Policy homepage: http://iase.disa.mil/policy.html
g	DODI 8500.2, Information Assurance (IA) Implementation, 6 Feb 03	http://www.dtic.mil/whs/directives/corres/html/85002.htm Accessed from the DISA Policy homepage: http://iase.disa.mil/policy.html
h	NTISSD No. 600, Communications Security (COMSEC) Monitoring, 10 Apr 90	http://www.iad.nsa.smil.mil/library/cnss_section/pdf/nstissd_600.pdf (SIPRNET access required)
i	Joint DODIIS/ Cryptologic SCI Systems Security Standards Revision 4, 1 Jan 06	http://www.nmic.navy.smil.mil/ssowi/Distro/references/JDCSISSSr3.doc (SIPRNET access required)
j	NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, 02 Dec 91	http://www.iad.nsa.smil.mil/library/cnss_section/pdf/nstissd_4003.pdf (SIPRNET access required)
k	SECNAVINST 5430.107, Mission and Function of The Naval Criminal Investigative Service (NCIS), 28 Dec 05	http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-400%20Organization%20and%20Functional%20Support%20Services/5430.107.pdf
l	SECNAV M-5510.36, DON Information Security Program, 30 Jun 06	https://doni.daps.dla.mil/SECNAV%20Manuals1/5510.36.pdf

Incident Categories

Category 1-9	Description
1	Root Level Intrusion (Incident): Unauthorized privileged access (administrative or root access) to a DOD system.
2	User Level Intrusion (Incident): Unauthorized non-privileged access (user-level permissions) to a DOD system. Automated tools, targeted exploits, or self-propagating malicious logic may also attain these privileges.
3	Unsuccessful Activity Attempted (Event): Attempt to gain unauthorized access to the system, which is defeated by normal defensive mechanisms. Attempt fails to gain access to the system (i.e., attacker attempt valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Can include reporting of quarantined malicious code.
4	Denial of Service (DOS) (Incident): Activity that impairs, impedes, or halts normal functionality of a system or network.
5	Non-Compliance Activity (Event): This category is used for activity that due to DOD actions (either configuration or usage) makes DOD systems potentially vulnerable (e.g., missing security patches, connections across security domains, installation of vulnerable applications, etc.). In all cases, this category is not used if an actual compromise has occurred. Information that fits this category is the result of non-compliant or improper configuration changes or handling by authorized users.
6	Reconnaissance (Event): An activity (scan/probe) that seeks to identify a computer, an open port, an open service, or any combination for later exploit. This activity does not directly result in a compromise.
7	Malicious Logic (Incident): Installation of malicious software (e.g., Trojan, backdoor, virus, or worm).
8	Investigating (Event): Events that are potentially malicious or anomalous activity deemed suspicious and warrants, or is undergoing, further review. No event will be closed out as a Category 8. Category 8 will be re-categorized to appropriate Category 1-7 or 9 prior to closure.
9	Explained Anomaly (Event): Events that are initially suspected as being malicious but after investigation are determined not to fit the criteria for any of the other categories (e.g., system malfunction or false positive).