SECNAV INSTRUCTION 5239.19A

From: Secretary of the Navy

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

Ref: See enclosure (1)

Encl: (1) References
      (2) Definitions
      (3) Responsibilities
      (4) Incident Categories
      (5) Cybersecurity Service Provider (CSSP) Contact Information

1. Purpose. Establish Department of the Navy (DON) computer incident handling policy consistent with reference (a), and to align and integrate DON computer incident handling and reporting requirements with the Department of Defense (DoD) policy in references (b) and (c).

2. Cancellation. SECNAVINST 5239.19.

3. Definitions. See enclosure (2).

4. Applicability

   a. This instruction applies to:

      (1) The Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all U.S. Navy, U.S. Marine Corps installations, commands, activities, field offices, and all other organizational entities within the DON.

      (2) This instruction applies to all DON owned, controlled, and contractor owned information systems that receive, process, store, display, or transmit DoD information, regardless of mission assurance category, classification, or sensitivity. Actions or missions executed in support of this
instruction are limited to Defensive Cyberspace Operations—Internal Defensive Measures (DCO-IDM).

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

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

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

(3) Signals intelligence, 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.

5. **Policy**

   a. To promote a strategy of risk management DON organizations must maintain Cybersecurity (CS) situational awareness and ensure compliance with CS policy, to include reporting of CS/Cyberspace Defense issues and significant incidents, as required by references (a) through (q).

   b. Defensive Cyberspace Operations (DCO) embodies incident detection and incident response, and synchronizes the technical, operational, and intelligence assessments of a computer attack in order to defend against it.
6. **Responsibilities.** See enclosure (3).

7. **Records Management**

   a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

   b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office.

8. **Reports.** The reporting requirements contained in enclosures (3), (4), and (6) are exempt from information collection control by reference (d), Part IV, paragraph 7c.

   THOMAS B. MODLY
   Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances website https://www.secnav.navy.mil/doni/.
REFERENCES

(a) SECNAVINST 5239.3C
(b) DoD Instruction 8530.01 of 7 March 2016
(c) Chairman of the Joint Chief of Staff Manual 6510.01B, Cyber Incident Handling Program of 10 July 2012
(d) National Telecommunications and Information Systems Security Directive 600, Communications Security Monitoring of 10 April 1990
(e) Deputy Secretary of Defense Memorandum, Defense Industrial Base Cyber Incident Notification Process of 6 May 2019
(f) Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, current edition
(g) Joint Publication 3-12, Cyberspace Operations of 8 June 2018
(i) SECNAVINST 5430.107A
(j) SECNAVINST 5510.36B
(k) DoD Directive 5240.06 of 17 May 2011
(l) DoD Instruction 5240.23 of 16 October 2013
(m) National Institute of Standards and Technology Special Publication 800-61 of August 2012
(n) DoD Directive 5205.16 of 30 September 2014
(o) DoD Instruction 5240.26 of 4 May 2012
(p) Intelligence Community Standard 502-01 of 23 December 2013 (NOTAL)
(q) CNSS Instruction 4003 of June 2016

Enclosure (1)
DEFINITIONS

1. **Cyber Incident.** Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. This includes the exfiltration of information from a network via cyber-enabled means. See reference (e).

2. **CS.** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. See reference (f).

3. **Cyberspace.** A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. See reference (f).

4. **Cyberspace Defense.** Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach CS measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. See reference (g).

5. **Defense Industrial Base.** The DoD, U.S. Government, and private sector industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. See reference (e).

6. **DCO.** Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity. See reference (g).

7. **(DCO-IDM).** Operations in which authorized defense actions occur within the defended portion of cyberspace. Also called DCO-IDM. See reference (g).
8. **Defensive Cyberspace Operations – Response Actions (DCO-RA).** Operations that are part of a DCO mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. Also called DCO-RA. See reference (g).

9. **Denial of Service (DOS) (attack).** The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) See reference (h).

10. **Department of Defense Information Networks (DODIN).** The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called DODIN. See reference (h).

11. **Spillage.** Security incident that results in the transfer of classified information onto an information system not authorized to store or process that information. See reference (h).

12. **Event.** Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. See reference (c).

13. **Global Information Grid (GIG).** The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG Information Technology (IT) includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network. The term “GIG” has been replaced by the term “Department of Defense Information network (DODIN)”. See reference (h).
14. **Incident.** An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. See reference (h).

15. **Incident Handling.** The detection, analysis, and response to any cyber event or incident for the purpose of mitigating any adverse operational or technical impact. See reference (c).

16. **Intrusion.** A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempt to gain, access to a system or system resource without having authorization to do so. See reference (h).

17. **Malicious Logic.** Hardware, firmware, or software that is intentionally included or inserted in a system for harmful purpose. See reference (h).

18. **Offensive Cyberspace Operations.** Cyberspace operations intended to project power by the application of force in or through cyberspace. See reference (g).

19. **Virus.** A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See reference (h).

20. **Vulnerability.** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. See reference (h).
RESPONSIBILITIES

1. Joint Forces Headquarters-DODIN under U.S. Cyber Command (USCYBERCOM) is the lead organization designated to identify and mitigate threats to DODIN. For the Navy, US Fleet Cyberspace Command (USFLTCYBERCOM)/US Tenth Fleet is the Service component to USCYBERCOM and has designated Navy Cyber Defense Operations Command (NCDOC)/Commander, Task Force 1020 as the sole Navy Cybersecurity Service Provider (CSSP). NCDOC is also the designated CSSP for the secretariat. For the Marine Corps, Marine Corps Cyberspace Command is the Service component to USCYBERCOM and the Marine Corps Cyberspace Operations Group (MCCOG) is the designated CSSP.

2. The Department of the Navy Chief Information Officer shall:
   a. 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.
   b. Utilize the reporting incident information to assess the effectiveness of DON CS program and policy, and adjust as required.
   c. Coordinate risk management across the DON by balancing threat against system/data criticality to identify and implement practical solutions.
   d. Ensure incident trends are captured and reflected in DON-wide policy.

3. Using the Navy and Marine Corps Cyber Components and designated Service CSSPs, the CNO and CMC shall:
   a. Coordinate overall respective Service computer network defense actions to mitigate security vulnerabilities and to direct incident handling and reporting to Commanders of DON organizations.
   b. Shall notify SECNAV of all cyber incidents involving the Defense Industry Base that require Congressional notification. SECNAV notification shall precede Congressional notification.
In accordance with reference (e), Congressional notification requirements include:

1. Any compromise of classified information likely to cause significant harm or damage to the national security interests of the U.S.

2. Determination of a significant loss of Controlled Unclassified Information from a defense contractor.

3. Congressional reporting requirements identified in any other existing or future legislation not identified by the references.

4. An Office of the Secretary of Defense (OSD) or Service Damage Assessment Management Office (DAMO) rating of high, very high, serious, severe or equivalent, as per OSD or Service DAMO criteria.

5. Detection of a new threat or emerging tactic, technique, or procedure; and media interest or the potential to attract media interest.

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

d. Report all root level intrusions, user level intrusions, DOS, malicious logic incidents, and any suspect or anomalous incidents (Categories 1, 2, 4, and 7) to the Naval Criminal Investigative Service (NCIS) immediately as detailed in references (i) and (j). Enclosure (4) describes each incident category. Navy and Marine Corps CSSP 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.

e. Report all incidents that are violations of federal law to NCIS. Incidents involving cleared defense contractors will be reported by NCIS to the Defense Security Service as described in reference (i) and (k).
f. Ensure the acquisition and preservation of copies of digital media, logs, and investigative and technical data associated with cyber intrusion incidents, investigations, and operations required for tactical analysis, strategic analysis, or law enforcement or counterintelligence investigations in accordance with references (b) and (k) through (m).

g. 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 Service Cyber Protection Team will provide global response and mitigation across the respective Service’s DODIN. Provide trained and equipped personnel to quickly respond to worldwide emerging DON cyber defense incidents.

h. Monitor all respective Service network protection devices.

i. 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 DODIN. Coordinate all cyberspace defense incidents with the NCIS and appropriate law enforcement, DoD, and national agencies.

j. Root level intrusions, user level intrusions, DOS, 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) Nonsecure Internet Protocol Router Network computer network incidents, including any incident that could create media attention or SECNAV level attention, to the DON Office of the CIO (OCIO). Report identified incident trends to the DON OCIO to ensure proper DON-wide policy changes and additions.

k. The DON Insider Threat Program’s User Activity Monitoring establishes procedures for responding to anomalous user activity, including procedures to mitigate potential damage to data on DON networks and to contact applicable investigative authority when necessary in accordance with references (c), (n), and (o).
4. The Director, NCIS, as a Staff Assistant and the Senior Official for law enforcement investigations and counterintelligence shall:

   a. Contribute to cyberspace defense by conducting investigations, operations, proactive programs, and related analyses of cyber incidents and targeting involving DON IT assets, compromise of data or the exfiltration of data.

   b. 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.

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

   d. Maintain a staff skilled in the investigation and analysis of cybercrimes. The staff should be sufficient in size to handle multiple major incidents and respond to increasing demands of the DON.

5. For the Navy, USFLTCYBERCOM through NCDOC’s authority as the Navy CSSP, and for the Marines the MCCOG will establish baseline incident handling methodologies to identify, detect, respond and recover from cyber events or incidents. NCDOC and MCCOG will direct the actions to execute Incident Response procedures.

6. All DON components shall:

   a. Report all incidents, as described in enclosure (4) and directed by appropriate CSSP (paragraph 1), using the proper classification level. 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 CSSP through designated channels as indicated by the CSSP.

   b. At a minimum, Category 1, 2, 4, and 7 incidents will be reported to NCIS, per reference (c).
c. Follow all initial reports to the respective CSSP with interim updates as required and a complete close-out report per reference (c).

d. Report and respond to SCI network incidents, per reference (p).

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

f. Respond to confirmed or suspected incidents/events in accordance with reference (c).

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 (q).

i. Integrate and support criminal and counterintelligence investigations and operations to help defend DON computer networks and protect critical DON data, per references (b), (l) and (k).
## INCIDENT CATEGORIES

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><strong>Training and Exercises:</strong> Operations performed for training purposes and support to Combatant Commands, Services, Defense Agencies, DoD Field Activities exercise.</td>
</tr>
<tr>
<td>1</td>
<td><strong>Root Level Intrusion (Incident):</strong> Unauthorized privileged access to an Information System (IS). Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.</td>
</tr>
<tr>
<td>2</td>
<td><strong>User Level Intrusion (Incident):</strong> Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Unsuccessful Activity Attempted (Event):</strong> Deliberate attempts to gain unauthorized access to an IS that are defeated by normal defensive mechanisms. Attacker fails to gain access to the IS (i.e., attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders. Note the above CAT 3 explanation does not cover the “run-of-the mill” virus that is defeated/deleted by AV software. “Run-of-the mill” viruses that are defeated/deleted by AV software are not reportable events or incidents and</td>
</tr>
<tr>
<td>Enclosure (4)</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>should not be annotated in the Joint Incident Management System.</td>
</tr>
<tr>
<td>4</td>
<td><strong>DOS (Incident):</strong> Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Non-Compliance Activity (Event):</strong> Activity that potentially exposes ISs to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of existing DoD policy. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.</td>
</tr>
<tr>
<td>6</td>
<td><strong>Reconnaissance (Event):</strong> Activity that seeks to gather information used to characterize ISs, applications, DoD information networks, and users that may be useful in formulating an attack. This includes activity such as mapping DoD information networks, IS devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.</td>
</tr>
<tr>
<td>7</td>
<td><strong>Malicious Logic (Incident):</strong> Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.</td>
</tr>
<tr>
<td>8</td>
<td><strong>Investigating (Event):</strong> Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are 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.</td>
</tr>
<tr>
<td>9</td>
<td><strong>Explained Anomaly (Event):</strong> Suspicious events that after further investigation are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as IS malfunctions and false alarms. When reporting these events, the reason for which it cannot be otherwise categorized must be clearly specified.</td>
</tr>
</tbody>
</table>
CYBERSECURITY SERVICE PROVIDER (CSSP) CONTACT INFORMATION

1. Secretariat and Navy commands report incidents to the Navy CSSP, which is NCDOC:
   NIPRNET:  https://www.ncdoc.navy.mil/
   E-mail:  ncdoc@ncdoc.navy.mil
   SIPRNET:  https://www.ncdoc.navy.smil.mil
   E-mail:  cndwo@ncdoc.navy.smil.mil
   Telephone:
   DSN:  (312) 668-0911
   Commercial:  (757) 203-0911 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 commands report incidents (including electronic spillages) to Marine Corps CSSP, which is the MCCOG:
   E-mail:  operationscenter@usmc.mil
   E-mail:  operationscenter@usmc.smil.mil
   Telephone:
   DSN:  (312) 278-5300
   Commercial:  (703) 784-5300
   Facsimile:
   DSN:  (312) 378-6654
   Commercial:  (703) 432-6654
   Plain Language Address:  MCCOG