



DEPARTMENT OF THE NAVY

NAVAL SEA SYSTEMS COMMAND
2531 JEFFERSON DAVIS HWY
ARLINGTON VA 22242-5160

5230
SER 00I/142

IN REPLY REFER TO

JUL 3 2001

POLICY LETTER 01-09

From: Naval Sea Systems Command, Chief Information Officer (SEA 00I)

Subj: INFORMATION OPERATIONS CONDITION (INFOCON) IMPLEMENTATION

Ref: (a) CNO/N6 Message, 181840Z May 99, Navy Information Operations Condition (INFOCON) Implementation
(b) CJCS Memorandum (with Enclosure), CM-510-99, dated 10 March 1999, Information Operations Condition
(c) ASD(C3I)/USD(P&R) Memorandum (with Attachments), dated 29 June 1998, Information Assurance (IA) Training and Certification
(d) DoN IA Pub-5239-01, dated May 2000, Introduction to Information Assurance (IA)
(e) CNO/N6 Message, 211417Z Oct 98, Information Assurance Vulnerability Alert (IAVA) Process, as amended by CNO/N6 Message, 071310Z Jul 99, Change of IAVA Reporting Agent

Encl: (1) NAVSEA INFOCON action requirements and procedures

1. Purpose. The purpose of this policy is to establish requirements and procedures for NAVSEA elements to set and respond to Information Operations Conditions (INFOCONS) effectively and efficiently, as directed by Reference (a). The NAVSEA INFOCON requirements and actions are provided as Enclosure (1).

2. Application. The provisions of this policy apply to all NAVSEA organizations having information systems under their purview. For the purposes of this policy, the local commander/officer-in-charge will make the initial determination of mission-criticality or mission-essentiality of information systems under his/her purview. The requirement for INFOCON implementation and reporting for the Navy/Marine Corps Intranet (NMCI) will be the responsibility of the Commander, Task Force NMCI. Until NMCI cutover, the local commanding officer/officer-in-charge retains responsibility for the actions required by this policy. The local commander will retain this responsibility for any networks, information systems that do not transition to the NMCI.

3. Scope. This policy consolidates several normal IT security practices into a structured, coordinated approach to defend against computer network attacks and to minimize damage to NAVSEA computer and telecommunications networks and systems. It is consistent with defensive information operations practices across the DoD and the DoN and mandates a level of preparedness for NAVSEA elements to respond successfully to higher-level INFOCONs. It combines routine activities already performed by most organizations and aligns them with the actions recommended for each INFOCON level (NORMAL and ALPHA thru DELTA). Adherence to this policy will enable NAVSEA to comply successfully with DoD and Navy INFOCON policies and operational requirements.

4. Policy. NAVSEA elements will comply fully with INFOCON guidelines set forth in Reference (b), to include achieving a level of preparedness sufficient to respond effectively to any INFOCON level that may be set by operational authority. In the Navy, this operational authority will generally be the Navy Component Task Force for Computer Network Defense (NCTF-CND). Commanders may also declare INFOCON changes for their organizations in response to local conditions in accordance with Paragraph 7b of Reference (b). Minimum mandatory requirements for NAVSEA subordinate commands are included in Enclosure (1).

5. Actions/Responsibilities.

a. The Chief Information Officer (CIO) shall:

- (1) Be responsible for establishing and implementing this INFOCON policy throughout NAVSEA.
- (2) Report NAVSEA compliance with all INFOCON actions as required.

b. The Deputy CIO for Information Assurance (DCIO-IA) shall:

- (1) Provide advice and guidance, as needed, to assist NAVSEA organizations in interpreting the requirements of this policy.
- (2) Support the CIO in implementing the provisions of this policy.
- (3) Maintain the official NAVSEA hierarchical structure within the On-line Compliance Reporting System (OCRS).

- (4) Monitor the OCRS to assess the status of NAVSEA implementation of vulnerability alerts and other Computer Network Defense (CND) task orders.

c. The Commanding Officer/Officer In Charge shall:

- (1) Ensure compliance with all provisions of this policy within his/her command by developing and implementing a site-specific INFOCON process and procedures for executing that process.
- (2) Determine which information systems under his/her purview are mission-critical and/or mission-essential for the purposes of this policy.
- (3) Within 15 days of the date of this policy, designate primary and alternate points of contact (POCs) who will be responsible for coordinating all INFOCON actions required by this policy and by DoN operational authorities. POC information will be reported to the DCIO-IA.
- (4) Add POC information to the Duty/Watch Officer contact list.
- (5) Be ultimately responsible for compliance of his/her organization with all INFOCON requirements and be accountable for any and all non-compliance with this policy. This includes all reporting requirements as described in Section 3 of Enclosure (1).

d. The Designated Points-of-Contact (POCs) shall:

- (1) Obtain copies of References (a) through (e) and become familiar with their contents as they apply to this policy.
- (2) Ensure the availability of the information required by Paragraphs 2.a.1 and 2.a.2 of Enclosure (1).
- (3) Request an account in the OCRS via <https://www.iava.navy.mil/>. The OCRS enables organizations to easily report progress and status of compliance with IAVAs and other CND task orders.
- (4) Coordinate compliance of their organization/command with the requirements of this policy and with any

additional requirements that may be levied by operational authorities during higher-level INFOCONs.

(5) Report INFOCON compliance information via OCRS and provide other required reports and information as described in Section 3 of Enclosure (1).

6. The point of contact for this policy is Mr. Tony Geddie, Deputy CIO for Information Assurance, at (202) 781-3014 or geddieja@navsea.navy.mil.



EDWARD L. SHELTON, III

Subj: INFORMATION OPERATIONS CONDITION (INFOCON) IMPLEMENTATION

1. Definitions.

- a. Information Assurance Vulnerability Alert (IAVA) process - A process established to disseminate information system vulnerabilities and to ensure a means of tracking corrective actions completed by DoD activities.
- b. INFOCON level - A predefined state of vigilance establishing minimum mandatory protections that must be carried out with regard to computer network defense. A total of five INFOCON levels are defined, based upon a number of factors relating to the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. The five levels are:
 - (1) NORMAL (normal activity),
 - (2) ALPHA (increased risk of attack),
 - (3) BRAVO (specific risk of attack),
 - (4) CHARLIE (limited attack), and
 - (5) DELTA (general attack).
- c. Mission-critical Information System - An information system, the loss of which would cause stoppage of warfighter operations or stoppage of direct mission support of warfighter operations.
- d. Mission-essential Information System - An information system that is basic and necessary for accomplishment of the organizational mission.

2. Minimum mandatory requirements for NAVSEA subordinate commands shall include the following:

- a. Establish and maintain INFOCON NORMAL as the routine operational condition for information systems under control of the command. The basic requirements of INFOCON NORMAL include:
 - (1) Identify and document all mission-critical and mission-essential information and information systems under control of the command, and determine their operational importance.

Subj: INFORMATION OPERATIONS CONDITION (INFOCON) IMPLEMENTATION

- (2) Identify and document all points of access to the information systems and determine their operational necessity.
 - (3) Conduct normal security practices on a routine basis throughout the command. Normal security practices shall include, as a minimum:
 - a. education and training for users, administrators and managers
 - b. training and certification of system administrators and maintainers in accordance with Reference (c)
 - c. an effective password management program, as described in Paragraph 4.2.10.4 of Reference (d)
 - d. periodic internal security reviews, auditing and audit log reviews, critical file back-ups
 - e. periodic external vulnerability assessments.
 - (4) Implement all security fixes or patches recommended by the Information Assurance Vulnerability Alert (IAVA) process prescribed by Reference (e) and report compliance within the allotted time.
 - (5) Maintain operational readiness by performing periodic review and test of higher-level INFOCON actions.
- b. For INFOCON ALPHA, perform all foregoing actions plus the following actions that exceed those required for INFOCON NORMAL:
- (1) Double the frequency of audit reviews and critical file backups.
 - (2) Implement all outstanding IAVA vulnerability fixes.
 - (3) Conduct an internal security review of all mission-critical and mission-essential systems upon declaration of INFOCON ALPHA and at least quarterly thereafter.
 - (4) Emphasize to all personnel the need to report all suspicious activity relating to critical information systems.
 - (5) Execute appropriate defensive tactics described in Appendix B of Ref (b).

Subj: INFORMATION OPERATIONS CONDITION (INFOCON) IMPLEMENTATION

- (6) Review all required higher-level INFOCON actions and be prepared to implement on short notice.
 - (7) Review Naval Computer Incident Response Team (NAVCIRT) advisories and implement as appropriate.
- c. For INFOCON BRAVO, perform all foregoing actions plus the following actions that exceed those required for INFOCON ALPHA:
- (1) Review audit logs and perform critical file backups daily.
 - (2) Conduct an immediate internal security review of all mission-critical and mission-essential systems upon declaration of INFOCON BRAVO and monthly thereafter.
 - (3) Confirm existence of newly identified vulnerabilities and install patches.
 - (4) Change passwords on all accounts and ensure strong passwords are used.
 - (5) Disconnect unclassified dial-up connections that are not required for current operations.
 - (6) Execute appropriate defensive tactics.
 - (7) Review and test higher level INFOCON actions and consider proactive execution.
- d. For INFOCON CHARLIE, perform all foregoing actions plus the following actions that exceed those required for INFOCON BRAVO:
- (1) Review audit logs and perform critical file backups every 12 hours.
 - (2) Minimize use of, and personnel access to, networks and systems connected to external networks.
 - (3) Reconfigure information systems to minimize the number (and bandwidth) of access points and to increase security.
 - (4) Disconnect non-mission-essential networks and systems.

Subj: INFORMATION OPERATIONS CONDITION (INFOCON) IMPLEMENTATION

- (5) Employ alternative communication modes for communicating critical information.
 - (6) Execute appropriate defensive tactics.
 - (7) Review and test higher level INFOCON actions and consider proactive execution.
- e. For INFOCON DELTA, perform all foregoing actions plus the following actions that exceed those required for INFOCON CHARLIE:
- (1) Execute applicable portions of Continuity of Operations Plan.
 - (2) Activate alternative modes of communication.
 - (3) Implement procedures for operating in manual or stand-alone modes.
 - (4) Restrict SIPRNet/JWICS access to Command & Control functions & personnel only.
 - (5) Isolate compromised systems from rest of network.

3. Reporting Requirements.

- a. INFOCON changes made at the local level, in response to threatened or actual computer network attacks, must be reported through operational channels, including the DCIO-IA and NAVCIRT, within four hours of the INFOCON change. Frequency of subsequent reports, as well as reporting format and contents, are prescribed in Paragraph 7d of Reference (b). In addition, whenever an INFOCON level change is declared Navy-wide or DoD-wide, the NCTF-CND will request specific information to be reported to particular DoD and DoN recipients on an accelerated schedule. NAVSEA commands will comply with all INFOCON-related reporting requirements.
- b. INFOCON reporting includes a requirement to assess potential and/or actual impact to DoD operations. Reports generated by NAVSEA commands as a result of INFOCON change must be accompanied by an operational assessment of the situation, when appropriate. Appendix D of Reference (b) outlines a process for assessing the operational impact of a computer network attack. The ability of an organization

Subj: INFORMATION OPERATIONS CONDITION (INFOCON) IMPLEMENTATION

to conduct this assessment successfully is directly related to the completeness, accuracy, and availability of the information required by Paragraphs 2.a.1 and 2.a.2 of this Enclosure (also listed in Paragraph 2 of the aforementioned Appendix D). Accordingly, commanders are urged to develop this information as soon as possible and to update it whenever pertinent changes occur.

- c. The DCIO-IA will monitor the OCRS to assess the status of IAVA implementation and of other CND task orders. Commands shall therefore keep their OCRS entries current. NAVSEA commands shall also report a summary of the results of internal security reviews and external vulnerability assessments on a semiannual basis to the DCIO-IA.
- d. Section 8 of reference (b) contains specific security classification guidance and disclosure policy for INFOCON information and reports. NAVSEA organizations shall adhere to this guidance.
- e. As appropriate to all threats, commanding officers will take appropriate actions to defend their commands. This applies equally to their computer networks as it does to physical security. No requirement for immediate reporting shall override this basic requirement to defend.