CHAIRMAN OF THE JOINT CHIEFS OF STAFF

WASHINGTON, D.C. 20318-9999

CM-510-99
10 March 1999

MEMORANDUM FOR: Distribution List

Subject: Information Operations Condition

1. This memorandum establishes the Information Operations Condition (INFOCON) for the Department of Defense. The system presents a structured, coordinated approach to react to and defend against adversarial attacks on DOD computers and telecommunications. Specific guidance and responsibilities for authorizing and communicating INFOCONs as part of information operations throughout the Department of Defense are provided at the enclosure.

2. INFOCON applies to the Joint Staff, Services, combatant commands, and Defense agencies -- as well as joint, combined, and other DOD activities throughout the entire conflict spectrum -- peacetime through war These procedures are effective immediately and will remain in effect until superseded by DOD instruction. Addressees have 60 days from the date of this memorandum to develop local procedures in compliance with the Enclosure, if required.

(b)(6)
(b)(6)

3. Joint Staff point of contact is Major [redacted] J-3, [redacted] or (b)(6)

JOSEPH W. RALSTON
Acting Chairman
of the Joint Chiefs of Staff

Enclosure

DISTRIBUTION LIST

	Copies
Chief of Staff, US Army	3
Chief of Naval Operations	3
Chief of Staff, US Air Force	3
Commandant of the Marine Corps	3
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)	3
Commander in Chief, North American Aerospace Defense Command	3
Commander in Chief, US Atlantic Command*	3
Commander in Chief, US Central Command	3
US Commander in Chief, Europe	3
Commander in Chief, US Pacific Command	3
Commander in Chief, US Southern Command	3
Commander in Chief, US Space Command	3
Commander in Chief, US Special Operations Command	3
Commander in Chief, US Strategic Command	3
Commander in Chief, US Transportation Command	3
Commander, US Forces Korea	3
Commander, US Element, NORAD	3
Director, Ballistic Missile Defense Organization	3
Director, Defense Advanced Research Projects Agency	3
Director, Defense Commissary Agency	3
Director, Defense Contract Audit Agency	3
Director, Defense Finance & Accounting Service	3
Director, Defense Information Systems Agency	3
Director, Defense Intelligence Agency	3
Director, Defense Security Service	3
Director, Defense Legal Services Agency	3
Director, Defense Logistics Agency	3
Director, Defense Security Cooperation Agency	3
Director, Defense Threat Reduction Agency	3
Director, National Imagery and Mapping Agency	3
Director, National Security Agency/Chief, Central Security Service	3
Commander, Joint Task Force – Computer Network Defense	3
Director, National Reconnaissance Office	3
Director for Manpower, Joint Staff	1
Director for Intelligence, Joint Staff	1
Director for Operations, Joint Staff	1
Director for Logistics, Joint Staff	1
Director for Strategic Plans and Policy	1
Director for Command, Control, Communications, and Computer Sytems, Joint Staff	1
Director for Operational Plans and Interoperability, Joint Staff	1
Director for Force Structure, Resources, and Assessment, Joint Staff	1

ENCLOSURE

INFORMATION OPERATIONS CONDITION (INFOCON)

1. Purpose. The Information Operations Condition (INFOCON) recommends actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks, and to mitigate sustained damage to the **DOD** information infrastructure, including computer and telecommunications networks and systems. The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system impacts all personnel who use DOD information systems, protects systems while supporting mission accomplishment, and coordinates the overall defensive effort through adherence to standards.

2. Description. The INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on DOD computer and telecommunication networks and systems. While all communications systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and standoff capability make computer network attack (CNA) an attractive option to our adversaries at present. The DOD INFOCON criteria and response actions may be expanded at a later date to include all forms of information operations. CNA is defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." INFOCON also outlines countermeasures to scanning, probing, and other suspicious activity; unauthorized access; and data browsing. DOD INFOCON measures focus on computer network-based protective measures, due to the unique nature of CNA (reference paragraph 5). Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are NORMAL (normal activity), ALPHA (increased risk of attack), BRAVO (specific risk of attack), CHARLIE (limited attack), and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions

3. Authority. The INFOCON system is established by the Secretary of Defense, and administered through the Director for Operations, Joint Staff (J-3). The INFOCON system will be administered through the Commander, Joint Task Force for Computer Network Defense (JTF-CND), when the JTF-CND reaches initial operational capability (IOC). All combatant commands, Services, directors of Defense and combat support agencies will develop supplemental INFOCON procedures as required, specific to their command and in consonance with this guidance. Subordinate and operational unit commanders will use the INFOCON procedures developed by their higher

headquarters (e.g., combatant commands or Services). Existing policy and procedures on communications security (COMSEC) may be integrated into local INFOCON procedures at the commander's discretion.

4. Applicability. This document provides guidance for standardized procedures and sets responsibilities for authorizing and communicating INFOCONs as part of information operations (IO) throughout the Department of Defense. The information contained herein applies to the Joint Staff; Services; combatant commands; Defense agencies; and joint, combined, and other DOD activities throughout the entire conflict spectrum -- peacetime through war.

5. Assumptions. Several critical assumptions were made about the nature of computer network attack (CNA) in developing the DOD INFOCON system. Understanding these assumptions is essential to effectively implement this system.

a. Shared Risk. In today's network-centric environment, risk assumed by one is risk shared by all. Unlike most other military operations, a successful network intrusion in one area of responsibility (AOR) may, in many cases, facilitate access into other AORs. This necessitates a common understanding of the situation and responses associated with the declared DOD INFOCON. These actions must be carried out concurrently in all AORs for an effective defense.

b. Advance Preparation. Preparation is key, given the speed and reduced signature of CNA. Protective measures must be planned, prepared, exercised, and often executed well in advance of an attack. Preventive measures are emphasized in INFOCON responses because there may be little time to react effectively during the attack. Prevention of system compromise (see Appendix C for various advisories to consider) is preferable, but may not be achievable.

c. Anonymity of Attacker. Attributing the attack to its ultimate source, if possible, will normally not occur until after the attack has been executed. This limits the range and type of options available to military decision makers. To effectively operate in this environment, knowledge of the adversary's identity cannot be a prerequisite to execution of defensive strategies and tactics

d. Characterization of the Attack. Distinguishing between hacks, attacks, system anomalies, and operator error may be difficult. The most prudent approach is to assume malicious intent until an event is assessed otherwise. (See Appendix C for various assessments to consider.)

6. Structure. This paragraph explains the INFOCON structure, including level, brief description, criteria to declare, and recommended actions. The criteria listed are broad guidance for the commander to consider when declaring an INFOCON, not concrete thresholds. All criteria for a particular INFOCON need

not be met to change to that level. More detailed explanation of routine security measures such as internal security reviews and external vulnerability assessments are located in Appendix A, General Security Practices.

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS

NORMAL
 	
NORMAL ACTIVITY
	No significant activity.	- Ensure all mission critical information and information systems (including applications and databases) and their operational importance are identified.
		- Ensure all points of access and their operational necessity are identified.
		- On a continuing basis, conduct normal security practices. For example:
		  - Conduct education and training for users, administrators, and management.
		  - Ensure an effective password management program is in place.
		  - Conduct periodic internal security reviews and external vulnerability assessments.
		  - Conduct normal auditing, review, and file back-up procedures.
		  - Confirm the existence of newly identified vulnerabilities and install patches.
		- Employ normal reporting procedures IAW para 7d.
		- Periodically review and test higher level INFOCON actions.

ALPHA
 	
INCREASED RISK OF ATTACK
	- Indications and warning (I&W) indicate general threat.
	- Regional events occurring which affect US interests and involve potential adversaries with suspected or known CNA capability.
	- Military operation, contingency or exercise planned or ongoing requiring increased security of information systems.
	- Information system probes, scans or other activities detected indicating a pattern of surveillance.
		- Accomplish all actions required at INFOCON normal.
		- Execute appropriate security practices (see Appendix A). For example:
		  - Increase level of auditing, review, and critical file back-up procedures.
		  - Conduct internal security review on all critical systems.
		  - Heighten awareness of all information system users and administrators.
		  - Execute appropriate defensive tactics (see Appendix B)
		- Employ normal reporting procedures IAW para 7d.
		- Review and test higher level INFOCON actions, and consider proactive execution.

BRAVO
 	
SPECIFIC RISK OF ATTACK
	- I&W indicate targeting of specific system, location, unit or operation.
	- Major military operation or contingency, planned or ongoing.
	- Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance.
	- Network penetration or denial of service attempted with no impact to DOD operations.
		- Accomplish all actions required at INFOCON ALPHA.
		- Execute appropriate security practices (see Appendix A). For example:
		  - Increase level of auditing, review, and critical file back-up procedures.
		  - Conduct immediate internal security review on all critical systems.
		  - Confirm existence of newly identified vulnerabilities and install patches
		  - Disconnect unclassified dial-up connections not required for current operation.
		  - Execute appropriate defensive tactics (see Appendix B)
		- Ensure increased reporting requirements are met IAW para 7d.
		- Review and test higher level INFOCON actions, and consider proactive execution.

Table 1. INFOCON Structure

LABEL : : (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
CHARLIE **LIMITED ATTACK(S)**	Intelligence attack assessment(s) indicate a limited attack. - Information system attack(s) detected with limited impact to DOD operations: - Minimal success, successfully counteracted. - Little or no data or systems compromised. - Unit able to accomplish mission.	- Accomplish all actions required at INFOCON BRAVO. - Execute appropriate response actions. For example: - Conduct maximum level of auditing, review and critical file back-up procedures. - Consider minimize on appropriate computer networks and telecommunications systems (limit traffic to mission essential communication only). (See Appendix E, ref. e, CJCSI 6900.01A) - Reconfigure information systems to minimize access points and increase security. - Reroute mission-critical communications through unaffected systems. - Disconnect non-mission-critical networks - Employ alternative modes of communication and disseminate new contact information. - Execute appropriate defensive tactics (see Appendix B). - Ensure increased reporting requirements are met IAW para 7d. - Review and test higher level INFOCON actions, and consider proactive execution.
DELTA **GENERAL ATTACK(S)**	- Successful information system attack(s) detected which impact DOD operations. - Widespread incidents that undermine ability to function effectively. - Significant risk of mission failure.	- Accomplish all actions required at INFOCON CHARLIE. - Ensure increased reporting requirements are met IAW para 7d. - Execute applicable portions of continuity of operations plan (See Appendix E, ref. f, DODD 3020.26, Continuity of Operations, Policy and Planning). For example: - Designate alternate information systems and disseminate new communication procedures internally and externally. - Execute procedures for ensuring graceful degradation of information systems. - Implement procedures for conducting operations in "stand-alone" mode or manually. - Isolate compromised systems from rest of network. - Execute appropriate defensive tactics (see Appendix B).

Table 1. INFOCON Structure (continued)

7. Procedures

a. Determining the INFOCON. There are three broad categories of factors that influence the INFOCON: operational, technical, and intelligence, including foreign intelligence and law enforcement intelligence. Some factors may fall into more than one category. The INFOCON level is based on significant changes in one or more of them. Appendix C describes several factors that may be considered when determining the INFOCON. DOD organizations are frequently confronted with unauthorized access to information systems. The decision to change the INFOCON should be tempered by the overall operational and security context at that time. For example, an intruder could gain unauthorized access and not cause damage to systems or data. This may only warrant INFOCON ALPHA or NORMAL during peacetime, but may warrant INFOCON CHARLIE during a crisis; or it may warrant a high INFOCON at the affected unit, but not throughout the command or the Department of Defense as a whole.

b. Declaring INFOCONs. The Joint Staff J3/Commander, JTF-CND (CJTF) will recommend changes in DOD INFOCON through the CJCS to the SecDef IAW paragraph 3. Assimilation and evaluation of information to assess the CND situation DOD-wide will be a collaborative effort focused at the Joint Staff/JTF-CND. The Secretary of Defense may delegate declaration authority to the J-3/CJTF. Commanders are responsible for assessing the situation and establishing the proper INFOCON based on evaluation of all relevant factors. Commanders may change the INFOCON of their organizations; however, they must remain at least as high as the current INFOCON directed by SecDef or the Chairman of the Joint Chiefs of Staff. The commander will report changes in INFOCON IAW subparagraph 7d.

c. Response Measures. Response measures associated with INFOCONs are normally recommended actions unless specifically directed by SecDef. Ideally, CND operations will be based on advanced warning of an attack. The intelligence community is developing a capability to provide warning which will become of increasing value as it matures. Measures should be commensurate with the risk, the adversary's assessed capability and intent, and mission requirements. Over-aggressive countermeasures may result in self-inflicted degradation of system performance and communication ability, which may contribute to the adversary's objectives. Commanders must also consider the impact imposing a higher INFOCON for their command will have on connectivity with computer networks and systems of other commands. Combatant commands will notify the Joint Staff if recommended or directed response measures conflict with theater priorities. Additionally, response measures directed by combatant commands will take precedence over response measures directed by Service INFOCONs when applicable. Regardless of the INFOCON level declared at the affected site, it is incumbent upon the affected

site to report all unauthorized accesses in a timely manner IAW subparagraph 7d.

d. Reporting. Technical reporting will be accomplished IAW reference A. Report violations of the law (such as unauthorized access to military computer networks and systems) to servicing military counterintelligence organizations IAW DODI 5240.6, "Counterintelligence Awareness and Briefing Program," and with local and Service/command policy. However, INFOCONs assess potential and/or actual impact to DOD operations and must be reported through operational channels. Additional guidance on INFOCON reporting follows.

(1) Reporting Channels. Combatant commands, Services, and DOD agencies will report INFOCON changes and summary reports to the Joint Staff through the National Military Command Center (NMCC):

CJCS NMCC WASHINGTON DC//J3/J33/J39//

Combatant commands, Services, and DOD agencies will designate a reporting authority and establish reporting procedures for organizational entities under their jurisdictions. Service entities under the operational control of a combatant command will follow the reporting instructions of that combatant command. Individual Service policy may require information copies to higher Service headquarters. Those entities not reporting directly to a CINC will follow Service-reporting procedures (usually to the Service operations center, which would then forward the information to the NMCC).

(2) Reporting Frequency. Services, combatant commands, and Defense agencies will report INFOCON changes to the NMCC NLT 4 hours after the INFOCON has changed. Provide whatever information is available at the time and indicate fields that are unknown or unavailable. Report information missing from the initial report in a follow-up report when it becomes available. Services, combatant commands, and Defense agencies may dictate more frequent internal reporting to subordinate components.

(3) Report Formats. Reports of changes in INFOCON should be accompanied by an operational assessment of the situation when appropriate. Appendix D outlines a process for assessing the operational impact of a computer network attack. Reports will include, as a minimum:

(a) For all INFOCONs: unit/organization and location, date/time of report, current INFOCON, reason for declaration of this INFOCON, response actions taken, POC (name, rank, duty title, contact information).

(b) INFOCON BRAVO and higher. All of the above, plus: unit/organization mission, current operation(s) (name, type, and AOR) unit is supporting, upcoming operation(s) (name, type, AOR, and dates) unit is

projected to support, Service computer emergency/incident response team (CERT/CIRT) or DISA Automated Systems Security Incident Support Team (ASSIST) incident number and law enforcement agency (LEA) case number with POC contact information

(c) INFOCON CHARLIE and higher. All of the above, plus: system(s) affected (network, classification, application, database/data file), degree to which operational functions are affected (command and control; intelligence, surveillance and reconnaissance; movement/maneuver; sustainment; fires; and protection), impact (actual and/or potential) on current/planned missions and/or general capabilities, restoration priorities, workarounds.

(4) Dissemination of DOD INFOCON. The Joint Staff/JTF-CND will send notification to combatant commands, Services, and agencies when the DOD INFOCON is changed. Commands, Services, and agencies are responsible for notifying units assigned to them. Notification will include the following information:

(a) Date/time of report.

(b) Current INFOCON.

(c) Reason for declaration of this INFOCON.

(d) Current/planned operation(s) or capabilities, units/organizations, networks, systems, applications or data assessed to be impacted or at risk.

(e) Recommended or SecDef-directed actions.

(f) References to relevant technical advisories, intelligence assessments, etc.

(g) POC contact information.

8. Security. Classification guidance and disclosure policy concerning IO is addressed in reference c. Specific guidance related to INFOCON follows.

a. INFOCON labels and descriptions are unclassified.

b. Generic defensive measures, when not tied to a specific INFOCON, are unclassified. Specific measures may be published in a classified appendix, if required.

c. Measures to be taken by all personnel, regardless of INFOCON, are unclassified.

d. General criteria to declare an INFOCON are FOR OFFICIAL USE ONLY (FOUO). Specific criteria may be published in a classified appendix, if required.

e. Classification of the measures associated with a particular INFOCON is the responsibility of the originator and will be classified according to content. However, the measures associated with a particular INFOCON, in aggregate, may require a higher classification than the individual measures. The measures associated with a particular INFOCON, in aggregate, will be FOUO at a minimum.

f. The operational impact of a successful information attack is classified SECRET or higher.

g. CNA intelligence assessments are classified SECRET or higher.

h. Information associated with an ongoing criminal investigation of a CNA may be considered law-enforcement sensitive.

i. A combatant command, Service, or agency may authorize release of its INFOCON system and procedures to allies or coalition partners as necessary to ensure effective protection of its information systems. Locally developed INFOCON procedures should use DODI 3600.2 and the guidance above when considering release to allies or coalition partners.

j. Changes in INFOCON are operational security (OPSEC) indicators and must be protected accordingly. The criteria and response measures are also of value to foreign intelligence Services in assessing the effectiveness of a CNA and in analyzing DOD's response. Do not post INFOCON procedures in publicly accessible locations such as unit web pages on unclassified networks and bulletin boards accessible to outsiders.

9. Relationship of INFOCON to Other Alert Systems. The INFOCON, THREATCON, DEFCON, CNA-WATCHCON, and conventional WATCHCON all interact with each other when the situation warrants it. The INFOCON may be changed based on the world situation (THREATCON, DEFCON), the intelligence community's level of concern (CNA-WATCHCON, conventional WATCHCON), or other factors (reference Appendix C). Likewise, a change in INFOCON may prompt a corresponding change in other alert systems.

a. The defense condition (DEFCON) is a uniform system of progressive conditions describing the types of actions required to bring a command's readiness to the level required by the situation (reference d).

b. The threat condition (THREATCON) is a process that sets the level for a terrorist threat condition at a given location, based on existing intelligence and other information.

c. A watch condition (WATCHCON) is part of the defense warning system indicating the degree of intelligence concern with a particular warning problem.

d. A CNA-WATCHCON is an intelligence assessment that takes into account CNA threat levels, as well as the overall political situation (reference b).

e. The INFOCON addresses risk of attack and protective measures for information and information systems.

10. Assessment

a. Exercises. INFOCON procedures should be practiced in all joint and/or combatant command exercises.

b. Combatant commands, Services, and agencies are requested to submit feedback to the Joint Staff on the effectiveness of the INFOCON system based on real-world and exercise data. The Joint Staff will review the system periodically to ensure it satisfies operational requirements.

11. These procedures are effective immediately and will remain in effect until superseded by DOD instruction.

12. List of Appendixes

a. General Security Practices.

b. Defensive Tactics.

c. Factors Influencing the INFOCON. See Annex A to Appendix C: CNA Intelligence Assessment Sample Format.

d. Operational Impact Assessment.

APPENDIX A

GENERAL SECURITY PRACTICES

Listed below are several measures that can significantly reduce the risk of successful attack against a critical information system. These activities should be the foundation of a sound, prevention-based information assurance/security program.

a. Svstem Securitv Administration. All DOD activities must ensure their systems are administered by technically qualified, experienced personnel who are provided periodic professional training in system administration and security, as well as the necessary tools to assist in effective baseline management, auditing, and network intrusion detection. Configuration management, proper staffing, and strong systems policies are critical to reliable and secure operations.

b. Auditing/Log Review. All DOD activities should regularly review audit logs for suspicious activity, IAW Appendix E, reference a and locally existing guidance. Logging and review requirements may increase with increases in INFOCON, including more frequent reviews, focused string searches, analysis of activity below normal trigger thresholds, and submission of logs to an organization designated to conduct specialized reviews.

c. Critical File Back-up Procedures. All DOD activities should conduct periodic back-ups of files critical to mission accomplishment, IAW Appendix E, reference a and locally existing guidance. Storage of back-up files should be isolated from any network and physically separated from the originating facility. Increases in INFOCON may warrant changes in the frequency of back-ups from quarterly, monthly, or weekly to daily or real-time.

d. Internal Securitv Reviews. All DOD activities should establish procedures for conducting internal security reviews, IAW reference a and locally existing guidance. These reviews should consist of, as a minimum, the following actions:

(1) Check password strengths (searching for default and weak passwords).

(2) Review pertinent technical advisories; install patches, implement fixes, execute preventive/mitigating actions.

(3) Conduct information system vulnerability scans.

(4) Identify network access points and their operational importance.

(5) Raise awareness level of all users as new vulnerabilities are found.

(6) Examine historically dormant/infrequently used accounts for signs of unusual activity.

e. External Vulnerability Assessments. All DOD activities should establish procedures for coordinating with outside agencies (e.g., Service CERTs/CIRTs, DISA, and NSA) to conduct vulnerability assessments and analyses of their information systems, IAW existing guidance. These assessments may include network scans, OPSEC surveys, COMSEC reviews, and red team operations.

APPENDIX B

DEFENSIVE TACTICS

1. The following list of defensive tactics offers possible responses to several types of suspicious/unauthorized activity. Defensive tactics should not be executed without some knowledge of the degree to which an intruder has penetrated the system and careful consideration of the potential, practical and legal consequences. For instance, changing passwords to lock out unauthorized access to valid accounts may not be prudent if a sniffer has been installed which can capture the new passwords.

2. Types of Activity. Adversary activity may be categorized as reconnaissance/suspicious activity, unauthorized access, denial of service, data browsing, data corruption, and malicious code. Conducting activities such as data browsing and data corruption is dependent upon gaining access to the system. Therefore, actions that prevent or halt unauthorized access might also be used to counteract data browsing and corruption.

3. General Actions. The following actions may or may not be valid responses to several or all types of malicious activity. The decision whether or not to employ them depends on the severity of the attack, and the practical and legal issues relating to such actions.

a. Disseminate reports/alert messages with suspicious Internet Protocol (IP) addresses, attack profiles/signatures.

b. Review thresholds for defensive systems (e.g., firewalls) and update for new/detected threats.

c. Freeze/eliminate compromised or unauthorized accounts.

d. Isolate affected network segment.

e. Re-route intruder to dummy network.

f. Jam communication lines.

g. Review thresholds for defensive systems and update for new/detected threats.

h. Tag critical files.

i. Block offending IP addresses/telephone lines.

j. Isolate compromised portions of affected system and monitor/log all activity.

k. Re-route intruder to a decoy system and continue logging activity.

l. Refer to identified technical advisories/alerts (Service CERTs/CIRTs, DISA ASSIST, NSA IPC, etc.).

m. Recall key information system security personnel.

n. Activate crisis action team to respond to impact of adversary CNA.

4. Reconnaissance/Suspicious Activity

a. Description. Automated scans/manual probes of networks to ascertain if the target system has known vulnerabilities or to get general information about the target system.

b. Possible defensive actions include reconstructing the scan/probing to determine what information was revealed, monitoring all incoming activity from the source IP address, blocking all access from the source IP address.

5. Denial of Service

a. Description: any action that causes all or part of the affected network's service to be stopped entirely, interrupted, or degraded sufficiently to impact network operations. Service may be denied by crashing the system, jamming it with packets, or consuming disk space, processor time or other resources.

b. Possible defensive actions include blocking all incoming activity from the source IP address/phone line.

6. Unauthorized Access

a. Description. Entry into and use of a system by an unauthorized individual.

b. Possible defensive actions include changing passwords; blocking all access from the source IP address; freezing/eliminating compromised, infrequently used, or historically dormant user accounts.

7. Data Browsing

a. Description. Unauthorized reading, capturing and/or downloading of information stored on or transmitted over a network.

b. Possible defensive actions for stored information include: encrypt files/directories; generate dummy files to confuse browsers; hide and/or rename key files or directories; transfer sensitive files from servers to auxiliary storage media; tag potential target files

c. Possible defensive actions for transmitted information include point-to-point encryption, flooding transmission lines with useless information, employing COMSEC procedures (limit traffic, use codes), using cover accounts.

8. Data Corruption

a. Description. Unauthorized modification of the contents of a file, database, or transmission. Ranges from subtle alterations that may not be noticed to complete destruction of the information, rendering the file, database, or transmission unusable.

b. Possible defensive actions include resetting file/directory access controls; backing up key verifiable files onto CD-ROM; using back-up files; storing key files/databases on removable storage media; employing checksums, signature files, and file tagging; developing a counter-deception plan.

9. Malicious Logic

a. Description. Hardware, software, or firmware intentionally inserted into an information system for an unauthorized purpose (e.g., Virus and Trojan horse).

b. Possible defensive actions include updating virus signature files and running appropriate virus detection/eradication software (if virus is known); checking all systems and signature files for unauthorized files or changes to files; removing user-specific, nonstandard applications; removing intranet web pages containing executable code fragments; disabling user-installed documents/templates containing macros.

APPENDIX C

FACTORS INFLUENCING THE INFOCON

When determining the appropriate defensive posture, many factors must be considered. This appendix lists several factors that commanders should consider when determining the INFOCON. (Note: This list is offered as broad guidance; other factors may be considered also.)

a. CNA-WATCHCON and threat warning assessments (reference b). Paragraph 9 and reference b provide more information on CNA-WATCHCONs. Also, other threat-warning assessments may be considered when determining the INFOCON.

b. Other indications & warning (including domestic threats). NSA IPC Alerts; National Infrastructure Protection Center (NIPC) advisories, threats, warnings; Service law enforcement agency intrusion reports, etc.

c. CNA intelligence assessment. (See Annex A for sample format). This report provides a fused intelligence assessment of the attack. US intelligence organizations work within legal restrictions on collecting and retaining information on US persons, IAW Executive Order 12333 and implementing DOD and Service regulations. Intelligence personnel will ensure mission accomplishment and compliance with relevant intelligence law by coordinating closely with law enforcement personnel. In the event that a CNA assessment leads intelligence personnel to US person information which they are legally prevented from pursuing further, they will transfer the matter to appropriate law enforcement organization, who will then produce a similar CNA assessment report, sanitized to protect law enforcement-sensitive information.

d. Conventional WATCHCON. Conventional warnings on actors with CNA capability may suggest an increased risk of CNA from those actors.

e. Current world situation. Increased tensions with a nation possessing CNA capability may precede CNA operations against us.

f. Other alert systems such as DEFCON, THREATCON, etc. Reference d, paragraph 9, and local security procedures discuss various alert systems. Local commanders must determine if a change in one alert status will cause a corresponding change in another alert status.

g. Current/planned military operations. The operational context within which an event occurs is critical to determining the appropriate level of response. Any contingencies, crisis actions, exercises, or other operations a

unit is supporting or projected to support must be considered when determining the INFOCON.

h. Dependence of military functions upon particular information systems. Applications directly supporting military functions (i.e., command and control; intelligence, surveillance, and reconnaissance; movement and maneuver; fires; and sustainment) may be predominantly resident on a single network or system. For example, the Global Transportation Network (GTN) is an NIPRNET-based application. If NIPRNET is the affected system, GTN and consequently the sustainment function may be adversely impacted. This type of analysis may suggest the degree to which a particular network, system, application or database is mission critical.

i. Commander's assessment of mission-critical information system readiness. Conceptually similar to 'status of resources and training system' (sorts). Commanders may base unit ability to accomplish the mission in part on the readiness of unit computer networks and systems. This readiness may be determined from the networks' security posture, vulnerability, extent of compromise, etc.

j. Information Assurance Vulnerability Alert (IAVA) bulletins. See reference a for format and explanation.

k. Incident reports. These are roughly analogous to tactical warning/attack assessment. See reference a for format and explanation.

l. Trend analyses. Reports showing number, type, and frequency of attacks; systems targeted; hot IP addresses, etc. See reference a for format and explanation.

m. Technical impact assessment. This information may be included in an incident report, or may result from follow-on analysis. This assessment may include the extent of system compromise and/or disruption and the degree to which system confidentiality, integrity, availability, authentication, and non-repudiation have been affected. See reference a for an explanation of these terms.

n. Operational impact assessment--a key element in determining the INFOCON. (See Appendix D for procedures.) The process for assessing operational impact also lays the groundwork for executing preventive measures, developing workarounds, and establishing restoration priorities.

o. Commander's assessment of the potential for an information attack. Although much objective data is available on which to base the decision, the final judgment for declaring an INFOCON change rests with the commander. Objective assessment of the situation and prudent analysis of all available


information must be integrated with the commander's experience and leadership to determine the organization's appropriate defensive posture.

ANNEX A TO APPENDIX C

CNA INTELLIGENCE ASSESSMENT SAMPLE FORMAT

1. Reference. CNA incident source reports (include originating agency, message DTG).

2. Executive Summary. Between 1 and 4 sentences summarizing significant elements of report.

3. Incident Summary. The following information is available from incident reports (reference a) and is included as background in this section of the intelligence assessment report:

a. Time and duration of incident.

b. CNA technique employed.

c. Path of attack/identification and location of origin of attack.

d. Location of system/network targeted.

e. Unit subordination of system/network targeted.

f. Mission of system/network targeted.

g. Actual impact of attack.

h. Potential impact of attack.

4. Intelligence Assessment. Consistent with intelligence law restrictions on the collection of US person information, the following information will be generated by intelligence analysts and included in this section of the intelligence assessment report:

a. Assessed source of attack. (Who did it? A certain terrorist group, government, or sub-organization defined to the best extent possible.)

b. Assessed type of attack. (What did they do? How? Provide simple explanation of the technical basis of the attack technique or tools from the perspective of insights into adversary capabilities.)

c. Assessed motivation of attack. (Why did they do it? Collect intelligence, implant malicious logic, harass/distract, disrupt operations, etc.)

d. Supporting analysis for both of the above assessments. (In addition to the logical inferences based on the current situation, background data should be provided-known CNA organizations, past practices, doctrine, etc.)

e. Contextual data on the situation. (What else is going on other than CNA that is potentially relevant to the current situation?)

f. Follow-on projection. (What can we expect next from the perpetrator? What about use of the particular CNA technique by others?)

APPENDIX D

OPERATIONAL IMPACT ASSESSMENT

1. Assessing the impact of CNA on our ability to conduct military operations is key to conducting damage assessment, prioritizing response actions, and assisting in identifying possible adversaries. This appendix offers an operational impact assessment process that may be used when reporting changes in INFOCON. Note: assessment results are classified SECRET at a minimum. The assessment process itself is unclassified.

2. Prior to an attack:

a. Identify all critical information systems.

b. For each critical information system, identify all resident critical applications and databases.

c. Determine which military functions are supported by each application/database: command and control; intelligence, surveillance, and reconnaissance; movement and maneuver; fires; sustainment; and protection.

3. After an attack or attempted attack has been detected:

a. Identify all critical information systems targeted.

b. List operations the unit is currently supporting or projected to support in the near future.

c. For each information system targeted, determine the technical impact, i.e., to what degree are confidentiality, integrity, availability, authentication, and non-repudiation affected? What critical applications and databases are impacted?

d. For the technical impacts identified, estimate the time and resources required to restore functionality. Identify any interim workarounds.

e. How does the technical impact of the attack affect the unit's ability to function?

f. How does the impact to the unit's ability to function affect support to current/projected operations? If no specific operations are ongoing or projected, how is general capability/readiness affected?

APPENDIX E

REFERENCES

a. CJCSI 65 10.0 1 b, Defensive Information Operations Implementation

b. DIA message 02 1727z JUN 98, Indications and Warning for Information Warfare/Information Operations {CNA-WATCHCON}

c. DODI 3600.2, Classification Guidance for Information Operations

d. CJCSM 3402.01A, Alert System of the Chairman of the Joint Chiefs of Staff

e. CJCSI 6900.0 1A, Telecommunications Economy and Discipline

f. DODD 3020.26, Continuity of Operations, Policies and Planning

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu