

DRAFT

RITSC-PSW
INFORMATION OPERATIONS CONDITION
RESPONSE MEASURES

1. Purpose. The Information Operations Condition (INFOCON) System recommends actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks (CNA), and to mitigate sustained damage to the Regional Information Technology Services Center (RITSC) information infrastructure, including computer and telecommunications networks and systems. A CNA is defined as “an operation to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” 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 RITSC 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 RITSC computer and telecommunication networks and systems. The RITSC INFOCON criteria and response actions may be expanded at a later date to include all forms of information operations. The INFOCON also outlines countermeasures to scanning, probing, and other suspicious activity; unauthorized access; and data browsing. Each INFOCON level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. The five 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. Applicability. This document sets responsibilities for INFOCON response measures as part of information operations (IO) throughout RITSC- Pacific Southwest/CNRSW.
4. Assumptions.
 - a. 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 is preferable, but may not be achievable.
 - b. 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 the RITSC Information Assurance department. To

effectively operate in this environment, knowledge of the adversary's identity cannot be a prerequisite to execution of defensive strategies and tactics.

- c. 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.

- 5. Structure. This paragraph explains the INFOCON structure, including level, brief description, criteria to declare, and recommended actions.

5.1 NORMAL (No significant activity).

- 5.1.1 This day-to-day condition warrants established routine security procedures. Typical threat activity at this level includes random probes on the RITSC information infrastructure as detected by network automated intrusion detection systems (IDS). Vulnerabilities are assumed to be consistent with those documented in the system security documentation for each computer network, or in previous assessments of other communications systems. At this level, daily information system security measures apply.

5.2 ALPHA (Increased Risk of Attack).

- 5.2.1 This condition is declared when an increased risk of attack on RITSC information systems exists. Typical threat activity at this level includes computer network scans, probes, or mapping. INFOCON ALPHA is also established when military operations, contingencies, or exercises require increased security of information systems or indications and warning or intelligence indicators of planned or increased threat activities indicate an increased surveillance or reconnaissance against RITSC's information infrastructure. Special alerts or advisories have been received from DoD Agencies indicating a general threat or new vulnerabilities may be existent. The measures for this INFOCON must be capable of being maintained indefinitely.

5.3 BRAVO (Specific Risk of Attack).

- 5.3.1 This condition is declared when a specific risk of attack against RITSC information systems exists. This condition may be prompted by an information warfare threat warning assessment indicating specific adversary capabilities with evidence of intent. Typical threat activity at this level includes limited computer network attacks with minor operational impact. Other indicators may include a significant increase in detected viruses, or limited

denial of service attacks. At this level, new or existing vulnerabilities must be identified and actions taken to mitigate them. These measures should be able to be maintained for several weeks without undue personnel hardships or degrading RITSC's ability to operate.

5.4 CHARLIE (Limited Attack).

- 5.4.1 This condition applies when an actual information attack occurs or when intelligence indicates the possibility of an imminent information attack that could result in a significant operational impact. Typical threat activity at this level includes actual or threatened attempts to gain access to RITSC computer network systems for the purpose of massive data destruction, false data creation, wide denial of service, or gaining control of critical systems. The injection across several networks of malicious code, viruses, Trojan horses, and e-mail bombs all fall into this INFOCON. Response measures at this INFOCON are focused at protecting critical systems. When implemented for even short periods of time, response measures at this INFOCON could create personal hardship, affect peacetime capabilities, and have the potential for increased operational costs.

5.5 DELTA (General Attack).

- 5.5.1 This condition applies when general attacks against RITSC information systems and networks significantly degrade readiness and operations. Extensive coordinated regional and global information attacks by entities with hostile intent toward/against the U.S. and its allies are expected. Response measures at this INFOCON are focused on maintaining or restoring RITSC's ability to operate its minimum critical systems. As with INFOCON CHARLIE, the response measures will likely result in personal hardships, increased operational costs (both time and dollars), and degradation of peacetime capabilities.

6. INFOCON Response Measures. Establishing an INFOCON does not presuppose all response measures within the declared INFOCON will be activated. Upon declaration of INFOCON ALPHA or higher, RITSC will direct specific defensive measures for implementation. Directed action may include measures from a higher INFOCON. For example, while in INFOCON ALPHA, RITSC may direct measures listed in INFOCON BRAVO. RITSC activities may implement additional actions dependent on local threat assessments.

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. Department of Navy 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 Navy as a whole.
- b. The following INFOCON chart depicts the actions that the RITSC must take at each INFOCON level. Additional measures may be required for each level as the situation warrants.

INFOCON NORMAL

Item No.	Responsibilities (Note: See Appendixes A-D for detailed instructions in accomplishing the following checklist tasks)	ISSMs	Information Assurance	Engineers	Operations
1	Identify all access points and their operational necessity.				
2	Conduct normal security practices to include education and training for users, administrators, and management.				
3	Periodically review and test higher-level INFOCON actions.				
Note: No loss of services or communications					

INFOCON ALPHA

Item No.	Responsibilities (Note: See Appendixes A-C for detailed instructions in accomplishing the following checklist tasks)	ISSM's	Information Assurance	Engineers	Operations	
4.	Call a meeting of senior RITSC staff and brief current status and the INFOCON actions being taken.					
5	Acknowledge receipt of INFOCON Change Message. Report when ALPHA status is reached. Use secure modes for conducting official business to maximum extent possible					
⑥	Pre-coordinate INFOCON procedures with appropriate personnel and de-conflict procedures with organizations that may be adversely affected.					
✓	7	Ensure all ISSM's, ISSO's, and SA's are briefed on the threat IO activity and response measures.				
⑧	Update Mission Critical user/position list with phone numbers, e-mail addresses, and official message addresses.					
✓	9	Direct all ISSM's, ISSO's, SA's, and users to increase their security awareness, particularly for critical C4ISR systems. Implement a 24X7 response/recall capability for mission critical personnel.				
⑩	Identify and maintain Mission Critical, Mission Support, and Administrative information systems and networks.					
⑪	Identify and maintain list of mission critical applications, files, and backup procedures. Increase frequency of mission critical file backups (minimum requirement is daily).					
⑫	Identify and maintain a baseline for system and network activity.					
✓	13	Ensure compliance with all existing IAVAs. Review and prioritize outstanding IAVAs.				

For Official Use Only

✓ 14	Increase OPSEC awareness. Remind all users to be particularly suspicious of anyone requesting passwords for direct access to RITSC systems.				
✓ 15	Remind all users that scanning computer disks for viruses is mandatory prior to use in RITSC computers.				
✓ 16	Remind all users to report unusual activity, viruses, and potential denials of service of computer or telephone systems including FAXs.				
✓ 17	Remind users of the need for passwords with a minimum of eight random alphanumeric characters.				
18	Identify requirements for, and conduct a review of server, firewall, and IDS audit logs for evidence of unusual or malicious activity. Increase frequency of audit logs reviews. Minimum requirement is daily with random spot checks during the workday.				

INFOCON ALPHA (Con't)

Item No.	Responsibilities	ISSM's	Information Assurance	Engineers	Operations
✓ 19	Ensure routers and firewalls protecting all segmented critical C4ISR systems have proper configuration settings to guard against known vulnerabilities and methods of recent attacks.				
✗ 20	Ensure routers and/or firewalls block appropriate IP hotlist address listings provided by next higher command.				
✓ 21	Confirm existence of newly identified computer system vulnerabilities and install respective patches and or fixes.				
✓ 22	Update computer virus signatures, then run anti-virus software.				
✗ 23	Perform an operational risk assessment of all interconnections. Report connections that are not SABI/TSABI approved and immediately disconnect all devices that are not fully approved.				
✓ 24	Ensure all telephone instruments are at least 3 feet from computers handling classified material.				
✓ 25	Monitor media for indicators of coordinated campaign to manipulate coverage against the U.S. and its allies.				
✗ 26	Update and distribute list of intruder IP addresses for local IP hotlists.				
? ✓ 27	Increase frequency System Administrators run available password crackers against their own systems to at least once every 30 days.				
✓ 28	Ensure all lower-level INFOCON actions are implemented.				
29	Review next higher INFOCON actions.				

Note: Increased duties for SAs and ISSMs. No significant loss of services or communications.

INFOCON BRAVO

Item No.	Specific risk of attack Responsibilities	ISSM's	Information Assurance	Engineers	Operations
30	Place all ISSMs, ISSOs, AND SAs on alert for possible recall after normal duty hours.				
31	Ensure all INFOCON ALPHA measures are implemented as directed.				
32	Verify real-time audit capabilities, if available, are turned on.				
33	Close all remote maintenance ports on routers, firewalls, servers, and electronic phone switches.				
34	Monitor bandwidth utilization, routing patterns, transit times for data packets, and other indicators of a degradation of service on classified and unclassified computer networks.				
35	Review options, and operational impacts, of disconnecting all bridges between unclassified and classified networks, such as Secure Mail Guard between unclassified and classified LANs.				
36	Use only classified mediums of information exchange where feasible, such as STU-III, secure FAX, and SIPRNet systems such as GCCS for conducting official business.				
✓37	Remove all unclassified dial-out capabilities from LAN workstations.				
38	Isolate compromised systems/local network from rest of WAN.				
39	As appropriate, implement alternate FAX numbers in response to denial of service attacks on FAX machines.				
40	Conduct computer network vulnerability assessments to re-verify levels of information security.				
41	Post guards on secondary power generation equipment for critical command and control centers within RITSC.				
42	Direct all ISSMs, ISSOs, and SAs to zero logins and force all accounts to enter new passwords with a minimum of 8 random alphanumeric characters.				
43	Freeze/eliminate compromised or unauthorized computer system accounts.				
44	Remove dial-in access to classified LANs that are not required for current operations. Only Mission Critical personal will use dial-in.				
45	In the case of an actual CNA, isolate the affected terminal or network, ensure evidence is maintained and passed to law enforcement agencies, then clean and recover the terminal or network				

Note: Some loss of services and communications (e.g., dial-up, non-secure phones, etc.)

INFOCON CHARLIE

Item No.	Limited Attack	ISSM's	Information Assurance	Engineers	Operations
	Responsibilities				
46	Ensure all INFOCON ALPHA and BRAVO measures are implemented as directed.				
47	Disconnect Secure Mail Guards between unclassified and classified LANs.				
48	Review current IDS coverage and expand to additional computer networks, if operationally feasible.				
49	Disconnect the Secure Gateway Systems to isolate classified LANs.				
50	Increase monitoring and audit review of Flag officer accounts. Secure the hard drives for flag officer systems not in use.				
51	Conduct maximum level of auditing.				
52	Reroute mission critical communications through unaffected systems.				
53	Disconnect non-mission critical C4ISR systems.				
Note: Increased loss of non-mission critical services and communications.					

INFOCON DELTA

Item No.	General Attack	ISSM's	Information Assurance	Engineers	Operations
	Responsibilities				
54	Ensure all INFOCON ALPHA, BRAVO, and CHARLIE measures are implemented as directed.				
55	Disconnect all critical C4ISR systems capable of operating in a stand-alone mode.				
56	Remove all hard drives from systems not in use.				
57	Execute continuity of operations plans, and disseminate new contact information.				
Note: Significant loss of non-mission critical services and communications.					

8. Security. 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.

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.

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.

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.

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

10. These procedures are effective immediately and will remain in effect until superseded by RITSC instruction.

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 for the CNRSW.

a. System Security Administration. All CNRSW 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 CNRSW activities should regularly review audit logs for suspicious activity. 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 CNRSW activities should conduct periodic back-ups of files critical to mission accomplishment. 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 Security Reviews. All CNRSW activities should establish procedures for conducting internal security reviews. 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.

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. Review thresholds for defensive systems and update for new/detected threats.
 - g. Block offending IP addresses/telephone lines.
 - h. Isolate compromised portions of affected system and monitor/log all activity.
 - i. Re-route intruder to a decoy system and continue logging activity.
 - j. Refer to identified technical advisories/alerts (Service CERTs/CIRTs, DISA ASSIST, NSA IPC, etc.).
 - k. Recall key information system security personnel.

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

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 D

TO DO LIST FOR INFOCON EXERCISE:

1. N1: Acknowledge receipt of INFOCON Change message.
 - a. Acknowledge receipt
 - b. Report Status as directed in the msg
 - c. Report when ALPHA is reached
 - d. Use secure modes for conducting official business to maximum extent possible.
2. N3: Identify and maintain a list of mission critical, mission support, and administrative information systems and networks
3. N5: Identify and maintain a mission critical information systems positions/users list.
Only develop a list of:
 - a. Critical NIPRNet users who need access to perform their duties
 - b. Of that list, those users who must access the Internet to perform duties
 - c. Critical SIPRNet users who need access to perform their duties.
 - d. Validate the mission critical information systems positions/users list.
4. N6: Identify and review remote access requirements
 - a. Validate remote network access requirements
5. N7: Identify and maintain a list of mission critical files and backup procedures.
 - a. Perform and, as required, increase frequency of mission critical file backups.
 - b. Minimum requirement is daily.
6. N8: Identify and maintain a baseline for system and network activity.
7. N9: Identify the requirements for, and conduct a review of server, firewall, and IDS audit logs for evidence of unusual or malicious activity.
 - a. Increase frequency of server, firewall, and IDS audit logs reviews.
 - b. Minimum requirement is daily with random spot checks during the workday.
8. N10: Ensure compliance with existing IAVAs.
 - a. Request assistance if necessary to close vulnerabilities and achieve 100% IAVA compliance.
 - b. Review and prioritize outstanding IAVAs and TAs, and implement if appropriate.
9. N11: Perform an operational risk assessment of all interconnections.
 - a. Report all connections that are not SABIT/TSABI approved.
 - b. Immediately disconnect all devices that are not fully approved and report to CPF N69.
 - c. Risk assessment consists of determining operational need for continued operation.
10. N15: Pre-coordinate INFOCON procedures with appropriate personnel.

For Official Use Only

- a. Pre-coordinate and de-conflict INFOCON procedures with any organizations that may be impacted by certain actions and/or whose actions may conflict.
 - b. As required, document implementation processes in a MOA/MOU.
11. Implement a 24X7 response/recall capability for mission essential network personnel.
 12. Ensure all lower-level INFOCON actions are implemented.
 - a. Ensure INFOCON Normal actions are completed.
 - b. Review and revalidate actions baselined in INFOCON Normal.
 13. Review next higher INFOCON actions.
 - a. Review DOD and local INFOCON actions for the next higher level.
 - b. Anticipate critical measures requiring resources for actions with long implementation times.

APPENDIX E

REFERENCES

- a. CJCSI 6510.01b, Defensive Information Operations Implementation
- b. DIA message 021727z 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 6900.01A, Telecommunications Economy and Discipline
- f. DODD 3020.26, Continuity of Operations, Policies and Planning