



Personnel

**ANCILLARY TRAINING - UNDERSTANDING INFORMATION
OPERATIONS CONDITIONS (INFOCON)**

OPR: 446 MSS/SCBN (SMSgt Jason Stenkyft) Certified by: 446 AW/CC (Col Alan Mitchell)
No. of Printed Pages: 8
Distribution: F

This pamphlet implements Air Force Policy Directive (AFPD) 36-22, *Military Training*. Information Operations Conditions (INFOCON) is the computer-communications equivalent to the Operations people's Threat Condition/Defense Condition (THREATCON/DEFCON) status'. The INFOCON system provides a structured approach to react and defend against adversarial attacks on DoD computers and communications. INFOCON applies to activities throughout the entire conflict spectrum, whether in peacetime or war. Since everyone is impacted by INFOCON, everyone needs to have an understanding of how INFOCON works. This pamphlet fulfills the annual requirement to conduct INFOCON training. It applies to all individuals assigned to the 446th Airlift Wing (446 AW).

1. Prescribing Directive:

- 1.1. Chairman Joint Chief of Staffs Memo CM-510-99, Information Operation Conditions (INFOCON).
- 1.2. HQ USAF/XOIW message, DTG 250923Z Mar99, DoD Information Conditions.
- 1.3. Air Force Manual (AFMAN) 10-206, *Operational Reporting*.
- 1.4. Air Force Operations Center (AFOC) message, DTG 030019Z Apr 99, OPREP reporting for communications and computer events/INFOCON reporting. (The AFOC message is an interim change to AFMAN 10-206.)

2. What is Information Operations Condition (INFOCON)?

- 2.1. The Information Operations Condition (INFOCON) system is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of the capabilities and intent of an adversary.
- 2.2. It is important to understand the INFOCON system because a computer network attack (CNA) is an attractive option for our adversaries.

2.3. Computer network attack is defined as "operations to disrupt, deny, degrade, or destroy information resident in computer networks, or the computers and networks themselves."

2.4. The INFOCON system is part of information operations throughout the Department of the Defense (DOD).

2.5. The INFOCON notification process begins at the DOD level and is administered by the Joint Task Force for Computer Network Defense (JTF-CND).

2.5.1. The Commander, Joint Task Force for Computer Network Defense (JTF-DNC) recommends to the Secretary of Defense to change Information Operations Conditions (INFOCON) levels DOD-wide.

2.5.2. Once the Secretary of Defense approves the INFOCON level change, the Commander JTF-CND, notifies combatant commands, services, and defense agencies via Defense Message System (DMS), Automated Digital Network (AUTODIN) or voice message.

2.5.3. The Air Force notification process begins with the Air Force Operations Center (AFOC).

3. Notification Process:

3.1. Downward notification involves the declaration and dissemination of Information Operations Conditions (INFOCON) changes to major commands and lower echelon units.

3.2. Up-channel Reporting must be approved by the Chief of Staff of the Air Force.

3.2.1. The Commander of Air Force forces reports a change to the Air Force-wide INFOCON, made independently of the DOD-wide INFOCON, to the JTF-CND, directly to the Commander JTF-CND and to the Joint Staff through the Air Force Operations Center (AFOC) to the National Military Command Center.

4. INFOCON Levels:

4.1. The INFOCON system provides five different levels based on the appropriate defense posture. The five levels in ascending order are:

4.1.1. The first INFOCON level is **NORMAL**.

4.1.2. Normal day-to-day actions, with no significant activity or unauthorized access.

4.1.3. Criteria:

4.1.3.1. No significant activity.

4.1.4. Recommended Actions:

4.1.4.1. Ensure all mission criteria information and information systems and their operational importance are identified.

4.1.4.2. Ensure all points of access and their operational necessity are identified.

4.1.4.3. On a continuing basis, conduct normal security practices. For example:

4.1.4.3.1. Conduct education and training for users, administrators, and management

4.1.4.3.2. Ensure an efficient password management program is in place.

4.1.4.3.3. Conduct normal auditing, review, and file back-up procedures.

4.1.4.3.4. Employ normal reporting procedures.

4.1.4.3.5. Periodically review and test higher level INFOCON actions.

4.2. The second INFOCON level is **ALPHA**.

4.2.1. Increased risk of attack.

4.2.2. Criteria:

4.2.2.1. Indications and warnings indicated general threat.

4.2.2.2. Regional events occurring which affect US interests and involve potential adversaries with suspected or known computer network attack capability.

4.2.2.3. Military operation, contingency or exercise planned or ongoing requiring increased security of information systems.

4.2.2.4. Information system probes, scans, or other activities detected indicating a pattern of surveillance.

4.2.3. Recommended Actions:

4.2.3.1. Accomplish all actions required at INFOCON NORMAL.

4.2.3.2. Execute appropriate security practices. For example:

4.2.3.2.1. Increase level of auditing, review, and critical file back-up procedures.

- 4.2.3.2.2. Conduct internal security review on all critical systems
- 4.2.3.2.3. Heighten awareness of all information system users and administrators.
- 4.2.3.2.4. Execute appropriate defensive tactics.
- 4.2.3.2.5. Employ normal reporting procedures.
- 4.2.3.2.6. Review and test higher level INFOCON actions and consider proactive execution.

4.3. The third INFOCON level is **BRAVO**.

4.3.1. INFOCON BRAVO means specific risk of attack.

4.3.2. Criteria:

4.3.2.1. Indications and warnings indicate targeting of specific system, location, unit or operation.

4.3.2.2. Major military operation or contingency, planned or ongoing.

4.3.2.3. Significant level of network probes, scans, or activities detected indicating a pattern of concentrated reconnaissance.

4.3.2.4. Network penetration or denial service attempted with no impact DOD operations.

4.3.3. Recommended Actions:

4.3.3.1. Accomplished all actions required at INFOCON ALPHA.

4.3.3.2. Execute appropriate security practices. For example:

4.3.3.2.1. Increase level of auditing, review, and critical file back-up procedures.

4.3.3.2.2. Conduct immediate internal security review on all critical systems.

4.3.3.2.3. Confirm existence of newly identified vulnerabilities and install patches.

4.3.3.2.4. Disconnect unclassified dial-up connections not required for current operations.

4.3.3.2.5. Execute appropriate defensive tactics.

4.3.3.2.6. Ensure increased reporting requirements are met.

4.3.3.2.7. Review and test higher level INFOCON actions and consider proactive execution.

4.4. The fourth INFOCON level is **CHARLIE**.

4.4.1. INFOCON CHARLIE means limited attacks are imminent.

4.4.2. Criteria:

4.4.2.1. Intelligence attack assessment(s) indicate a limited attack.

4.4.2.2. Information system attack(s) detected with limited impact to DOD operations

4.4.2.3. Minimal success, successfully counteracted.

4.4.2.4. Little or no data or systems compromised.

4.4.2.5. Unit able to accomplish mission.

4.4.3. Recommended Actions:

4.4.3.1. Accomplish all actions required at INFOCON BRAVO.

4.4.3.2. Execute appropriate response actions. For example:

4.4.3.2.1. Conduct maximum level of auditing, review, and critical file back-up procedures.

4.4.3.2.2. Reconfigure information systems to maximize access points and increase security.

4.4.3.2.3. Reroute mission-critical communications through unaffected systems.

4.4.3.2.4. Disconnect non-mission-critical networks.

4.4.3.2.5. Employ alternative modes of communications and disseminate new contact information.

4.4.3.2.6. Execute appropriate defensive tactics.

4.4.3.2.7. Ensure increased reporting requirements are met.

4.4.3.2.8. Review and test higher level INFOCON actions, and consider proactive execution.

4.5. The fifth INFOCON level is **DELTA**.

4.5.1. INFOCON DELTA means general attacks.

4.5.2. Criteria:

4.5.2.1. Successful information system attack(s) detected which impact DOD operations.

4.5.2.2. Widespread incidents that undermined ability to function effectively.

4.5.2.3. Significant risk of mission failure.

4.5.3. Recommended Actions:

4.5.3.1. Accomplish all actions required at INFOCON CHARLIE.

4.5.3.2. Ensure applicable portions on continuity of operations plan. For example:

4.5.3.2.1. Designate alternate information systems and disseminate new communications procedures internally and externally.

4.5.3.2.2. Execute procedures for ensuring graceful degradation of information systems.

4.5.3.2.3. Implement procedures for conducting operations in "stand-alone" mode or manual.

4.5.3.2.4. Isolate compromised systems from rest of network.

4.5.3.2.5. Execute appropriate defensive tactics.

5. INFOCON Categories:

5.1. INFOCON levels may be lowered or heightened by commanders at the major command, numbered air force, wing or base level.

5.2. There are three broad categories of factors.

5.3. However, other factors may also be considered that would influence an INFOCON level.

5.4. The three categories are:

5.4.1. Operational:

5.4.1.1. The first category is **OPERATIONAL**.

5.4.1.2. Operational refers to "a heightened concern due to ongoing or planned contingency operations."

5.4.2. Technical:

5.4.2.1. The second category is **TECHNICAL**.

5.4.2.2. Technical refers to the "assessment of vulnerability or effects of attacks on networks."

5.4.3. Intelligence:

5.4.3.1. The third category is **INTELLIGENCE**.

5.4.3.2. Intelligence refers to the "assessment of adversary attack via foreign information gathering or law enforcement intelligence."

5.5. A commander at any level uses these three categories, Operational, Technical, and Intelligence to determine the appropriate INFOCON.

6. INFOCON Deconflicting:

6.1. Major command, Numbered Air Force, wing, base or unit commanders are responsible for determining and establishing the proper INFOCON level based on evaluation of all relevant factors in the three categories.

6.2. 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 yet not cause damage to systems or data.

6.3. The Commander of the Air Force Information Warfare (AFIWC) Joint Task Computer Network Defense (JTF-CND) will reassess the Air Force-wide INFOCON. Major command, direct reporting unit, and subordinate commanders will reassess locally directed INFOCON as required by ongoing events or whenever a higher headquarters issues an INFOCON change.

6.3.1. INFOCON levels at each echelon are lowered by the same authority and possesses that raised them, based on the three broad categories.

6.3.2. This is applicable to all base units.

6.3.3. Including AF tenant units who will generally use the host-installation INFOCON level.

6.3.4. An exception to this rule would be if the tenant Commander-in-Chief or designated Air Force Component Commander determines it would interfere with Commander-in-Chief directed operational actions.

6.4. Major Command, numbered air force, and units may be subject to conflicting Commander-in-Chief and service INFOCON levels. In such cases, the higher INFOCON takes precedence, unless the Major Commander INFOCON determines it would interfere with the Commander-in-Chief directed operational actions.

6.5. Air Force forces actively participating in on-going operations will follow the INFOCON of their Joint Task Force Commander.

6.6. Air Force entities under the operational control of a combatant command, such as Central Command, must follow the reporting instructions of the combatant command in addition to any Air Force reporting requirements.

7. Module Summary:

7.1. The Information Operations Conditions (INFOCON) system is to provide a structured approach to reach to and defend against adversarial attacks on Department of Defense (DOD) computers and telecommunications.

7.2. The INFOCON notification process begins at the DOD level and is administered by the Joint Task Force for Computer Network Defense (JTF-CND).

7.3. The INFOCON system provides five different levels based on the appropriate defense posture.

INFOCON	DESCRIPTION	RECOMMENDED ACTIONS
NORMAL	Normal Activity	
ALPHA	Increased Risk	Increase auditing/review, heighten awareness
BRAVO	Specific Risk	Increase auditing, internal security review, install patches
CHARLIE	Limited Attack	Maximum auditing, limit traffic, disconnect non-essential networks
DELTA	General Attack(s)	Isolate compromised system, select alternate information system

ALAN M. MITCHELL, Colonel, USAFR
Commander