BY ORDER OF THE COMMANDER

STRATEGIC COMMAND DIRECTIVE (SD) 527-1

27 JAN 2006

Operations, Planning, and Command and Control

DEPARTMENT OF DEFENSE (DOD) INFORMATION OPERATIONS CONDITION (INFOCON) SYSTEM PROCEDURES

NOTICE: COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

This publication is available on the StratWeb Publications page.

OPR: JTF-GNO/J53 (Mr. Luss)
Certified by: J010 (Maj Cort O. Hacker)
Supersedes CM-510-99, 10 March 1999.
Pages: 35
Distribution: F

The purpose of this SD is to establish guidance and procedures for the Department of Defense (DoD) Information Operations Condition (INFOCON) System. This SD applies to the Office of the Secretary of Defense, the Services, the Joint Staff, the Combatant Commands, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereafter referred to collectively as the DoD Components) and any non-DoD Network Operations (NetOps) community of interest (COI) members connected to the DoD-wide Global Information Grid (GIG). This SD implements the policies and responsibilities defined in DoDD O-8530.1, *Computer Network Defense (CND)*, and DoDI O-8530.2, *Support to Computer Network Defense (CND)*, to direct Defense-wide changes in INFOCONs. This SD is effective 90 days after publication. DoD components (to include the combatant commands) and other Federal agencies may obtain copies of this SD from the United States Strategic Command (USSTRATCOM) Publications Page: https://www.stratcom.smil.mil. A glossary of references and supporting information is at **Attachment 1**.

Table of Contents

Chapter 1— INFOCON SYSTEM **4**

1.1. Purpose. 4

1.2. Execution. 4

1.3. Authority. 4

1.4. Background. 4

1.5. Description. 6

1.6. INFOCON Structure. 8

1.7. Tailored Readiness Options (TRO). 9

1.8. (FOUO) Updates. 10

1.9. INFOCON Decision Criteria. 10

Chapter 2— RESPONSIBILITIES **12**

2.1. The Chairman of the Joint Chiefs of Staff. 12

2.2. The Commander, United States Strategic Command. 12

2.3. DoD Components. 12

Chapter 3— INFOCON PROCEDURES **13**

3.1. DoD-Level INFOCON Changes. 13

3.2. Regional and Local (within DoD Component) INFOCON level changes. 13

3.3. Conflict Resolution. 13

3.4. Adding Measures. 14

3.5. Exit Criteria. 14

3.6. Cancellation. 14

3.7. Directive Measures. 14

Chapter 4— GLOBAL INFOCON PROCEDURES **16**

4.1. (FOUO) Overview. 16

4.2. INFOCON 5, Normal Readiness Procedures. 16

Table 4.1. (FOUO) INFOCON 5 Procedures. 16

4.3. INFOCON 4, Increased Military Vigilance Procedures. 18

Table 4.2. (FOUO) INFOCON 4 Procedures. 18

4.4. INFOCON 3, Enhanced Readiness Procedures. 19

Table 4.3. (FOUO) INFOCON 3 Procedures. 19
4.5. INFOCON 2, Greater Readiness Procedures. 19
Table 4.4. (FOUO) INFOCON 2 Procedures. 19
4.6. INFOCON 1, Maximum Readiness Procedures. 20
Table 4.5. (FOUO) INFOCON 1 Procedures. 20

Chapter 5— SAMPLE REPORTING TEMPLATES 21
5.1. DoD INFOCON Change Alert. 21
Figure 5.1. (FOUO) Example CDRUSSTRATCOM DoD INFOCON Alert Message. 22
5.2. DoD INFOCON Change Acknowledgment SITREP. 23
Figure 5.2. (FOUO) Example DoD INFOCON Change Acknowledgement SITREP. 23
5.3. INFOCON Status SITREP. 24
Figure 5.3. (FOUO) Example INFOCON Status SITREP Message. 25
5.4. Local INFOCON Change SITREP. 26
Figure 5.4. (FOUO) Example Local INFOCON Change SITREP. 28

Chapter 6— SAMPLE TAILORED READINESS OPTIONS 29
6.1. General. 29
6.2. TROs. 29
Table 6.1. (FOUO) Elements of TRO ONE. 29
Table 6.2. (FOUO) Elements of TRO TWO. 29
Table 6.3. (FOUO) Elements of TRO THREE. 29
Table 6.4. (FOUO) Elements of TRO FOUR. 29
Table 6.5. (FOUO) Elements of TRO SEVEN. 29
Table 6.6. (FOUO) Elements of TRO EIGHT. 30
Table 6.7. (FOUO) Elements of TRO NINE. 30
Table 6.8. (FOUO) Elements of TRO TEN. 30

Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 31

Chapter 1

INFOCON SYSTEM

1.1. Purpose. The INFOCON system provides a framework within which the Commander USSTRATCOM (CDRUSSTRATCOM), regional commanders, service chiefs, base/post/camp/station/vessel commanders, or agency directors can increase the measurable readiness of their networks to match operational priorities. This SD describes a new INFOCON approach replacing the INFOCON system that has been in place since 1999. Key to this new strategy is a shift from a threat focus to a readiness focus. The readiness strategy provides the ability to continuously maintain and sustain one's own information systems and networks throughout their schedule of deployments, exercises and operational readiness life cycle independent of network attacks or threats. The system provides a framework of prescribed actions and cycles necessary for reestablishing the confidence level and security of information systems for the commander and thereby supporting the entire GIG.

1.2. Execution. The INFOCON system, including responsibilities, processes, and procedures, applies to Non-classified Internet Protocol Routing Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) systems under the purview of the Joint Chiefs of Staff and all DoD activities within the unified commands, military services, and DoD Agencies, as well as the non-DoD NetOps COI (NetOps CONOPS, *Joint Concept of Operations for Global Information Grid NetOps*). It is executed by unified and service commanders, base/post/camp/station/vessel commanders and agency directors with authority over information systems and networks (operational and/or support) (hereafter collectively referred to as "commanders"). The INFOCON system provides commanders the authority, discretion and accountability to prepare their organization's network and information systems at any level they deem appropriate for the current and anticipated environment, as directed in paragraph **3.2.**

1.3. Authority. The Chairman of the Joint Chiefs of Staff established the INFOCON system in CM-510-99. The INFOCON system is executed through the operational authority of CDRUSSTRATCOM as part of his overall responsibility for Global Network Operations (GNO) for the DoD in accordance with (IAW) DoDD O-8530.1.

1.3.1. DoD INFOCON Declaration Authority. The Secretary of Defense delegated the authority to set global INFOCON levels to CDRUSSTRATCOM.

1.3.2. Regional and Local INFOCON Declaration Authority. Commanders **at all levels** of the DoD retain the authority to set INFOCON levels for information systems and networks under their command and control. The INFOCON system reinforces the commander's inherent right to self defense. Commander's have the flexibility to adjust their INFOCON assurance levels as necessary and report when raising regional INFOCON levels above the established global INFOCON. These levels must remain at least as high as the DoD INFOCON level declared by CDRUSSTRATCOM.

1.4. Background.

1.4.1. The INFOCON system was initiated in 1999 and many real world events have highlighted needed changes in system concept, procedures and measures. Foremost among the "must fix" issues was the need to operationalize, standardize, and normalize the INFOCON process across the DoD.

1.4.2. This SD describes a new INFOCON strategy that shifts from a "threat-based," reactive system to a "readiness-based," proactive approach. This paradigm shift represents a significant change in how commanders at all levels ensure the security and operational readiness of their information networks. While CDRUSSTRATCOM will continue to direct changes in the global INFOCON status, changes in local or regional INFOCON status will now be more actively managed by commanders at all levels (e.g., base, post, camp, station, vessel, major command) using a framework of standardized measures. The INFOCONs mirror Defense Conditions (DEFCON) defined in CJCSM 3402.1B, (S) *Alert System of the Chairman of the Joint Chiefs of Staff* (U), and are a uniform system of five progressive readiness conditions - INFOCON 5, INFOCON 4, INFOCON 3, INFOCON 2, and INFOCON 1. (There is no direct correlation between INFOCON and DEFCON levels, though commanders should consider changes in INFOCON when DEFCON changes.) INFOCON 5 is normal readiness and INFOCON 1 is maximum readiness. Each level represents an increasing level of network readiness based on tradeoffs in resource balancing (e.g., downtime versus level of assured confidence regarding malicious activity) that every commander must make. The INFOCONs are supplemented by Tailored Readiness Options (TRO), which are applied in order to respond to specific intrusion characteristics or activities, directed by CDRUSSTRATCOM or commanders.

1.4.3. The new DoD INFOCON system is predicated on the fact that a determined intruder will **always** compromise a networked system. Returning the system to a pristine, baseline state restores confidence in the system. Any system changes, while not always easily detectable in isolation, are almost always detectable by comparing the current status to a previous known baseline. However, maintaining a baseline snapshot across an enterprise and running the appropriate comparisons are non-trivial tasks for network and system administrators. As such, the readiness posture becomes a resource balance of how often commanders want to ensure their networks (or portions thereof) are free of malicious activity in relation to their own Operational Tempo (OPTEMPO). The readiness postures are designed to provide commanders at all levels the flexibility to set the readiness level they deem most appropriate for their OPTEMPO and available resources.

1.4.4. A commander's decision to raise or lower INFOCON levels or employ certain TROs should be based primarily on the anticipated operational activity of the command and the degree to which those activities are reliant on networked resources. As commanders move their networks up in INFOCON the frequency of assured activities increase and, therefore, the commander's confidence in system availability and performance commensurately will increase. Considerations could include: changes in DEFCON in response to global or regional political situations, increased regional tensions, large scale military maneuvers, exercises, Operations Security (OPSEC), consideration of supported command's INFOCON levels, threat, and recovery from network events.

1.4.5. Procedures for managing the DoD INFOCON level remain essentially the same under the new system. Changes in the DoD INFOCON status will continue to be directed by USSTRATCOM via a Computer Network Event Conference (CNEC) and/or a DoD INFOCON Alert message. The Commander, Joint Task Force for Global Network Operations (CJTF-GNO) will recommend changes only after pre-coordination with the DoD Components (unless the situation is time-critical) to determine the operational impact of changing the DoD INFOCON level.

1.4.6. Authority to change regional and local INFOCON levels is retained by commanders with information systems under their command and control. Commanders will report INFOCON change declarations, status, measures, TROs and compliance through their operational chain of command to JTF-GNO. In those instances where conflicting INFOCON levels prevent full implementation of

INFOCON measures by any party, the respective combatant commander and subordinate or supporting commander must resolve the issue to best meet the intent of the imposed INFOCON level to provide the highest degree of network readiness. CDRUSSTRATCOM will adjudicate situations where INFOCON conflicts between two or more commanders cannot be resolved. On occasion, conflicts may be elevated through the Chairman of the Joint Chiefs of Staff to the Secretary of Defense for resolution.

1.4.7. Measures common to all DoD Components have been identified for each INFOCON and are listed in **Chapter 4**. Commanders will normally accomplish all actions for the INFOCON level declared. However, local operational realities may require that a commander delay, or even omit implementation of specific INFOCON directive measures. In addition to the directive measures prescribed in **Chapter 4**, the declaring commander may direct the implementation of TROs to counter a specific regional or global threat. Decisions to deviate will be immediately communicated up the chain-of-command to JTF-GNO.

1.4.8. This new INFOCON approach will continue to evolve as we gain experience. USSTRATCOM and the JTF-GNO will periodically review and update the INFOCON system procedures as necessary.

1.5. Description.

1.5.1. Network Readiness Posture. The DoD INFOCON system is predicated on the fact that network intruders change a system during the initial exploitation (less skilled) or in follow-on activities (experienced hackers). These changes include creation of "new" users, upgraded permission levels, new executable software (such as Trojans, backdoors, or sniffers), new processes or services, and changes to system configuration (e.g., changes in the registry, changes to key file systems). These changes, while not always easily detectable in isolation, are almost always detectable by comparing the current status to a previous known baseline; this process can be automated with minimal impact to network users.

1.5.2. Scope.

1.5.2.1. Information Systems, Networks, and Interconnections. The INFOCON system pertains to all DoD information systems and networks operating at the Secret level (not to include closed, special enclave, or Intelligence Community (IC) networks) and below. The system also governs any interconnections between Public/DoD Unclassified networks, DoD Unclassified/Classified networks, and Classified/Classified networks.

1.5.2.2. The IC Incident Response Center (IC-IRC) will serve on behalf of the IC Chief Information Officer as the defense IC central reporting and coordination center for Computer Network Defense (CND) activities.

1.5.2.3. Commanders of Secret, closed, special enclave, and/or IC networks may (after coordinating with the IC-IRC) use the INFOCON system as a basis from which to assess and direct similar actions for these networks.

1.5.3. Objectives. Several critical fundamental facts were identified concerning the nature of military operations in a hostile information environment in developing the DoD INFOCON system. Understanding these facts is essential to effectively implement this system.

1.5.4. Self-imposed Denial of Service. INFOCON measures should not result in a self-imposed denial of service, either to specific users or to entire networks. Responses to specific threats that might demand blocking Internet Protocol (IP) addresses, blocking ports/protocols, or eliminating user/maintenance functionality may still be required in response to network activity or threats but will not be implemented as a part of the INFOCON system. Rather, when these measures become necessary they will be carefully and narrowly tailored to focus on the specific situation.

1.5.5. Operational Synchronization. As military operations continue to rely more and more on net-centric operations, INFOCON measures must be tied directly to the operational activities of the corresponding commands.

1.5.6. Implementation Burden. The burden of meeting INFOCON requirements should be placed on network and system administrators rather than on the network's users. This implies INFOCON measures should, to the extent possible, be transparent to the users. It also implies the procedures must be so well rehearsed that the risk of erroneous network-degradation is minimized. It does not however free the end-user from complying with existing regulations (i.e., unauthorized software and peer-to-peer activity.)

1.5.7. Shared Risk. Due to the interconnectivity of all DoD networks, shared risk is a fact of life. The significance of a clear chain of command within the DoD Components allows for evaluation of the risk associated with any given vulnerability or intrusion. Shared risk is mitigated by the thoughtful and synchronized accomplishment of the systematic measures within a directed readiness level.

1.5.8. Insider Threat. Insider threat represents a significant challenge for NetOps and in turn the GIG. The threat is not only from insider personnel but also from outsiders who, because of network trust relationships, are effectively insiders to multiple networks based on compromise of a single network. To the greatest extent possible, INFOCON measures should mitigate insider threats from both authorized and unauthorized users.

1.5.9. Incident Response. In most cases, network intrusions detected by analysis or intrusion detection systems are treated as law enforcement events and handled accordingly with respect to conducting the investigation, preserving evidence, and restoring the network. However, under the INFOCON process where a commander desires an increased level of readiness to support on-going or anticipated operations, commanders may decide to forego a law enforcement response to more quickly return the compromised asset to operational status after coordinating with your servicing Computer Emergency Response Team (CERT)/Computer Incident Response Team (CIRT).

1.5.10. Operational Rhythm. Most information system management activities have a rhythm or cycle of repetition. Increased INFOCON levels may require increased workload and/or decreased cycle time that must be maintained as long as that readiness level is in effect. Administrators/operators must recognize the requirements for sustained increased workload and schedule resources and personnel accordingly. The readiness level is not considered "achieved" until the increased activities are consistently maintained over time and a rhythm is established. Administrators/operators must ensure their commanders understand the potential operational impacts of this increase in activity.

1.5.11. Information Assurance (IA). The INFOCON measures are not a substitute for operating networks using appropriate IA principles and procedures.

1.6. INFOCON Structure.

1.6.1. General. The INFOCON system relies heavily on the capabilities of administrators to manage their networks and data systems ensuring a heightened level of readiness for day-to-day and crisis operations. This is accomplished by implementing the measures in a timely and efficient manner, which can be improved by exercising the INFOCON system regularly. Additionally, the INFOCON system measures rely on establishing an operational rhythm to allow network/system administrators the ability to plan and prioritize their efforts. This means an INFOCON level is not so much achieved as it is activated. The measures are repeated periodically in response to the selected period of the operational rhythm and with the understanding that resources and operational activities will dictate when within the period each measure might be accomplished. INFOCON measures are at **Chapter 4**.

1.6.2. INFOCON 5. INFOCON 5 is characterized by routine NetOps, normal readiness of information systems and networks that can be sustained indefinitely. Information networks are fully operational in a known baseline condition with standard information assurance policies in place and enforced. During INFOCON 5, system and network administrators will create and maintain a snapshot baseline of each server and workstation in a known good configuration and develop processes to update that baseline for authorized changes.

1.6.2.1. OPTEMPO, Training, Preparation for Change in INFOCON. The basic OPTEMPO of a DoD Component varies both internal to, and external from the organization. Factors such as combat operations, deployment, scheduled organizational training, and fiscal responsibilities impact the overall capability of any given organization. Individual organizations, as service providers, are responsible for their own training and preparation program with respect to INFOCON preparation. Occasional global exercises will help to further mature INFOCON, but the majority of OPTEMPO balancing will happen within the DoD Component resources. To this end, each DoD Component should have a robust training and certification program to gain and maintain technical expertise with respect to INFOCON impact and operation on their very network and information systems. This program should be adequate in substance and flexibility to handle internal (to the organization and perceived commitments) and external (global training and certification) requirements.

1.6.2.2. Baselining. As any information network asset is brought on line, it is exposed to ever increasing numbers of threats such as malicious code (worms, virus, Trojans) along with intrusions, and simple human error. In the face of these threats, a commander's confidence in his network defenses and information assurance procedures diminishes over time. The critical process of baselining, however, allows the system and network administrator, either by software or manually, a means to measurably restore that confidence. By comparing a known good baseline of each network asset to its current state, an administrator can detect the presence, or absence, of intruder activity. A major activity, then, of INFOCON 5 is maintaining accurate baselines of those assets. To be successful, a baseline must include the most up-to-date information (i.e., system patches, configuration updates, etc.). Additionally, it must reflect all legitimate changes added during the system(s) lifecycle. DoD standard automated methods for maintaining such baselines, and restoring to them, are essential to the success of this program. Baselining tools and training information, as they become available, will be located at http://www.jtfgno.smil.mil. The community will be notified as the site is updated.

1.6.3. INFOCON 4. INFOCON 4 increases NetOps readiness, in preparation for operations or exercises, with a limited impact to the end-user. System and network administrators will establish an operational rhythm to validate the known good image of an information network against the current state and identify unauthorized changes. Additionally, user profiles and accounts are reviewed and checks conducted for dormant accounts. By increasing the frequency of this validation process, the state of an information network is confirmed as unaltered (i.e., good) or determined to be compromised. This level of readiness may or may not be characterized by an increased intelligence watch and strengthened security (port blocking, increased scans) measures of information systems and networks. Impact to end-users is negligible.

1.6.4. INFOCON 3. INFOCON 3 further increases NetOps readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to end-users is minor.

1.6.5. INFOCON 2. INFOCON 2 is a readiness condition requiring a further increase in frequency of validation of the information network and its corresponding configuration. The impact on system administrators will increase in comparison to INFOCON 3 and will require an increase in preplanning, personnel training, and the exercising and pre-positioning of system rebuilding utilities. Use of "hot spare" equipment can substantially reduce downtime by allowing rebuilding in parallel. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.

1.6.6. INFOCON 1. INFOCON 1 is the highest readiness condition and addresses intrusion techniques that cannot be identified or defeated at lower readiness levels (e.g., kernel root kit). It should be implemented only in those limited cases where INFOCON 2 measures repeatedly indicate anomalous activities that cannot be explained except by the presence of these intrusion techniques. Until such time as more desirable detection methods are available, the most effective method for ensuring the system has not been compromised in this manner is to reload operating system software on key infrastructure servers (e.g., domain controllers, Exchange servers, etc.) from an accurate baseline. Rebuilding should be expanded to other servers as resources permit and intrusion detection levels indicate. Once baseline comparisons no longer indicate anomalous activities, INFOCON 1 should be terminated. The impact on system administrators will be significant and will require an increase in preplanning, personnel training, and the exercising and pre-positioning of system rebuilding utilities. Use of "hot spare" equipment can substantially reduce downtime by allowing rebuilding in parallel. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.

1.7. Tailored Readiness Options (TRO). TROs are supplemental measures to respond to specific intrusion characteristics directed either by CDRUSSTRATCOM or the responsible regional/local commander. They are narrowly focused and meant to supplement the current INFOCON readiness level either globally, regionally or at bases/camps/posts/stations. TROs will document, in standard language, all supplemental INFOCON measures to ensure a common understanding of the level of readiness and mission impact of each measure. Due to the interconnected nature of the GIG, the directing commander must ensure the proper global and regional coordination is accomplished through the operational chain of command with JTF-GNO and that the operational impact of the TRO is assessed by all affected organizations. Our network environment necessitates this list be dynamic in order to meet readiness objectives. USSTRATCOM will coordinate changes with DoD Components prior to updating the document. A list of TROs is maintained at http://www.jtfgno.smil.mil.

1.8. (FOUO) Updates. Our network environment necessitates that the INFOCON measures and TROs be dynamic in order to meet readiness objectives. Therefore, the following procedures have been established to allow for additions, updates and deletions:

1.8.1. (FOUO) The initial measures contained within this SD will be posted online at http://www.jtfgno.smil.mil. USSTRATCOM has the authority to modify the current measures in coordination with DoD Components.

1.8.2. (FOUO) Recommendations for changing actions (either measures or TROs) will be distributed via e-mail to each DoD Component. The message will contain the suspense date (minimum 60 days) required for feedback.

1.8.3. (FOUO) Comments (concur / non-concur) will be made online at http://www.jtfgno.smil.mil. Commands who fail to reply by the suspense date will be marked as concur.

1.8.4. (FOUO) Actions achieving at least 90 percent concurrence will be incorporated as a measure within a specific INFOCON level.

1.8.5. (FOUO) Proposed actions failing to achieve a 90 percent concur will be incorporated into the list of TROs.

1.9. INFOCON Decision Criteria. The foremost determining criteria for changing a command's INFOCON level is the anticipated operational activity of the command and the degree to which those activities are reliant on networked resources. INFOCON levels should be raised prior to the activity to ensure the network is as ready as possible when the operation or exercise begins. Because system and network administrators implement many of the INFOCON measures over a period of time in a pre-determined operational rhythm, commanders should raise INFOCON levels early enough to ensure completion of at least one cycle before the operational activity begins. Recommendations for possible INFOCON changes should be written into Operation Plans (OPLAN) and Concept Plans (CONPLAN).

1.9.1. Commanders should consider OPSEC when determining INFOCON levels to ensure OPSEC and INFOCON processes are coordinated to protect operations. INFOCON measures may prevent adversaries (or potential adversaries) from gaining valuable intelligence about friendly operations. Regional and local commanders should consider whether INFOCON changes provide an indicator(s) to an adversary and increase INFOCON levels on a random basis to ensure the establishment of INFOCON levels does not become an indicator of planned activity.

1.9.2. Regional or local commanders operating in support of other commands shall consider raising the INFOCON levels of all or key portions of their assets to match the level of the supported commander.

1.9.3. The INFOCON system focuses on readiness but threats to the network should still be a consideration for changing INFOCON levels. Indications and warnings or the detection of new network activity from open sources or network sensors represent threats to network readiness. Commanders may choose to increase INFOCON levels as a general response to assure readiness in the face of those threats. However, commanders may forego an INFOCON level increase by implementing TROs to defend against specific threats. Because many of these defensive actions, such as blocking IP addresses or cutting off services until patching is complete, often have unintended consequences in the DoD's highly interconnected network, these measures must be implemented as narrowly as possible and supplement INFOCON directed measures.

1.9.4. Because the INFOCON measures have the effect of eliminating the affects of malicious or unauthorized network activity, commanders may choose to implement INFOCON 4 for one cycle as a recovery mechanism following a worldwide Internet worm or virus attack. Depending on the technical characteristics of the virus the baselining function of INFOCON 4 could be used to ensure all instances of the virus are removed from the network. The baseline must be continuously updated with the proper patches and virus updates to avoid re-infection. Current trust relationships established across the DoD mean the probability of re-infection still exists.

1.9.5. Commanders must ensure system and network managers implement an aggressive training program to maximize the effectiveness of INFOCON measures and minimize network disruption. This is especially true for INFOCON 1 measures. Commanders should therefore periodically raise INFOCON levels for short periods to exercise and test INFOCON procedures for all or part of their networks to ensure a smooth transition between levels.

Chapter 2

RESPONSIBILITIES

2.1. The Chairman of the Joint Chiefs of Staff. The Chairman of the Joint Chiefs of Staff, as the principal military advisor to the President, Secretary of Defense and National Security Council, is responsible for assisting the President and the Secretary of Defense in providing strategic development of United States (U.S.) military policy, positions and concepts supporting CND and IA. To assist the Chairman, the designated Joint Staff directorate head will ensure the following:

2.1.1. The Joint Staff Director for Operations (JS/J-3) will coordinate with CDRUSSTRATCOM to develop joint INFOCON policy and procedures in coordination with Combatant Commanders, Services and Defense Agencies.

2.1.2. The Joint Staff Director for Command, Control, Communications, and Computer Systems (JS/J-6) will provide Director, JS/J-3, network management and IA analysis of proposed INFOCON procedures and measures.

2.2. The Commander, United States Strategic Command. The Commander, United States Strategic Command (CDRUSSTRATCOM) will:

2.2.1. Execute operational authority to direct global changes in DoD-wide INFOCON levels and measures IAW DoDD O-8530.1.

2.2.2. Develop global INFOCON procedures in coordination with Joint Staff, Combatant Commands, Services and Defense Agencies.

2.3. DoD Components. DoD Components will:

2.3.1. Implement the INFOCON system IAW DoDI O-8530.2, this SD, and USSTRATCOM guidance.

2.3.2. Develop supplemental INFOCON procedures, as required, specific to their component and consistent with DoD and Joint guidance.

2.3.3. Ensure subordinate and operational unit commanders use the INFOCON procedures developed by their higher headquarters (e.g., combatant commands or Services) to include supplemental or more restrictive measures as directed. Component commands of a regional combatant command will follow INFOCON guidance from the combatant commander.

Chapter 3

INFOCON PROCEDURES

3.1. DoD-Level INFOCON Changes.

3.1.1. The Commander, Joint Task Force for Global Network Operations (CJTF-GNO) will recommend changes in DoD INFOCON to CDRUSSTRATCOM. Prior to this recommendation, JTF-GNO will coordinate with the DoD Components to determine the operational impact of changing the DoD INFOCON level. This operational assessment will be a critical element in building CJTF-GNO's INFOCON change recommendation to CDRUSSTRATCOM. Upon receiving the recommendation from CJTF-GNO, CDRUSSTRATCOM will assess, and if necessary, direct a DoD-level INFOCON change.

3.1.2. (FOUO) USSTRATCOM will notify DoD Components of a DoD-level INFOCON change via a CNEC and/or a DoD INFOCON Alert message (see paragraph **5.1.**).

3.1.3. (FOUO) DoD Components will acknowledge establishment of the appropriate INFOCON operational rhythm via an acknowledgement message within 24 hours of receipt of the INFOCON Alert Message (see paragraph **5.2.**).

3.2. Regional and Local (within DoD Component) INFOCON level changes.

3.2.1. All DoD commanders retain the authority to declare INFOCON changes for information systems under their command and control.

3.2.2. The INFOCON level declared by a local commander must remain at least as high as the DoD INFOCON level or the level prescribed by a higher authority in their chain of command.

3.2.3. Regional combatant commanders who independently raise INFOCON levels will notify USSTRATCOM (cc: JTF-GNO), other combatant commanders, and the services to provide situational awareness and allow them to consider matching the regional level to better support operations.

3.2.4. Regional commanders and services may establish additional reporting requirements for lower echelon organizations.

3.2.5. (FOUO) Commanders at any level of command whose INFOCON measures or TROs (see **Chapter 6**) have the potential to affect a unified commander's operations will report INFOCON change declarations, status, and compliance through combatant commander channels, in addition to complying with service or agency reporting requirements.

3.3. Conflict Resolution. DoD Component units and elements supporting mission operations of a unified commander may come under conflicting INFOCON levels (e.g., global vs. regional, supported combatant commander vs. supporting combatant commander, combatant commander vs. service, or combatant commander vs. agency). In these cases, the higher INFOCON level takes precedence, unless the combatant commander determines it would interfere with operational actions. In those instances where conflicting INFOCON levels prevent full implementation of INFOCON measures by any party, the respective combatant commander and subordinate or supporting commander must resolve the issue to best meet the intent of the imposed INFOCON level to provide the highest degree of network readiness.

However, the unified commander will retain the final INFOCON declaration authority. CDRUSSTRATCOM will adjudicate situations where INFOCON conflicts between two or more unified commanders cannot be resolved.

3.4. Adding Measures. All commanders and agency directors may publish supplemental detailed INFOCON procedures specific to their missions and operational environment. All such measures will be chosen from published TROs (with local amplifying guidance) or submitted to JTF-GNO Policy and International Affairs Branch (JTF-GNO/J53) for adoption as a new TRO. Any such additional INFOCON guidance will supplement and not supersede the DoD-wide INFOCON system described herein. Subordinate and operational unit commanders will incorporate INFOCON procedures published by their higher headquarters (e.g., combatant commands or Services). In addition, DoD Component supplemental procedures must be provided to respective CND service providers.

3.5. Exit Criteria. Commanders directing INFOCON changes should establish exit criteria for raised INFOCON levels to provide lower echelon commanders the information to balance resources within operational commitments.

3.6. Cancellation. A change from a higher to a lower INFOCON cancels all actions unique to the higher INFOCON level (i.e., actions that are not also conducted at the lower INFOCON level), unless otherwise directed in the message declaring a decrease in INFOCON level.

3.7. Directive Measures.

3.7.1. Common Directive Measures. Actions common to all DoD Components have been identified for each INFOCON and are listed in **Chapter 4**. The directive measures provide a common readiness posture across DoD information systems and networks.

3.7.2. Order of Implementation. When a non-sequential increase in INFOCON occurs (e.g., from 5 to 3), the directive measures from the skipped INFOCON level(s) will be accomplished. Once the higher INFOCON level has been achieved the lower (skipped) INFOCON level will be complete by default.

3.7.3. Directive Measure Exemptions. DoD Components will normally accomplish all actions for the INFOCON level declared. However, local operational realities may require that a commander delay, or even omit implementation of specific INFOCON directive measures. In these situations, local commanders must weigh the risks incurred to DoD information systems and networks from the delay or omission of directive measures against the operational impacts of implementing these measures. The commander declaring the INFOCON will be informed by subordinate commands of any deviations and/or exemptions from directive measures listed in paragraph **4.2.**, or any additional actions directed by CDRUSSTRATCOM in the DoD INFOCON Change Alert Message (see paragraph **5.3.**).

3.7.4. TROs. In addition to the directive measures prescribed in paragraph **4.2.**, the declaring commander may direct the implementation of TROs to counter a specific threat, by region or globally. Normally, TROs supplement a lower INFOCON level.

3.7.4.1. The additional measures required for a DoD-level INFOCON change will be included in the DoD INFOCON Readiness Message.

3.7.4.2. Additional measures required for a “local” (lower than DoD) INFOCON declaration will be reported to USSTRATCOM and JTF-GNO via the DoD Component INFOCON Readiness Message (Local INFOCON change situation report (SITREP) see paragraph **5.4.**).

3.7.4.3. Additional measures directed by lower echelon commanders may not conflict with DoD measures. In order to limit the risk of network interoperability problems resulting from an INFOCON change, commanders directing the implementation of additional measures will first attempt to coordinate these actions with supporting technical centers, including appropriate service and agency elements.

3.7.5. Pre-coordination of Directive Measures. To expedite INFOCON change actions, all supporting combatant commanders, service and/or agency units will establish a Memorandum of Agreement or directive to pre-coordinate INFOCON procedures and directive measures with the unified commander(s) they support. The coordination should include a determination of which actions may be implemented immediately, and which actions require combatant commander notification prior to implementation. This same process applies to all activities under Host/Tenant agreements, as well as organizations employing cross-domain solutions to connect between different security domains or other trust relationships.

Chapter 4

GLOBAL INFOCON PROCEDURES

4.1. (FOUO) Overview. INFOCON procedures focus on proactively establishing and re-establishing a secure baseline based on a periodic, operational rhythm. This cycle varies, based on perceived operational needs, from bringing systems back to a secure baseline every 180 days at INFOCON 5, to restoring that secure baseline every 15 days at INFOCON 1. As we move from a lower to a higher level, immediately complete the cycle and then use the timeline established for that level for successive cycles. Each level of INFOCON uses the lower level(s) as the basis from which to start all activities. Report all activities to the command setting the INFOCON level (declaring command).

4.2. INFOCON 5, Normal Readiness Procedures.

Table 4.1. (FOUO) INFOCON 5 Procedures.

5-1. (FOUO) Re-establish 'secure baseline' in conjunction with a check for unauthorized changes on a semi-annual (180-day) cycle. This should involve mirroring the drives for subsequent examination, prior to re-loading the secure configuration. If examination of the drives indicates unauthorized changes, first determine if the changes were actually authorized, yet improperly recorded. This may reveal the need for a review of the procedures for updating the database of authorized changes. Unauthorized changes may indicate the need to temporarily increase to a higher INFOCON level, depending on what unauthorized changes are discovered. Without a provision such as this, you may be unaware the network has been compromised.
5-2. (FOUO) Ensure all DoD Information Systems are compliant with guidance and responsibilities outlined within IAW DoDI O-8530.2 and CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*. **5-2.1.** (FOUO) Update and maintain anti-virus, firewall, Information Assurance Vulnerability Alerts (IAVA), and Access Control Lists (ACL) configurations. **5-2.2.** (FOUO) Ensure complexity and periodicity of passwords.
5-3. (FOUO) When moving into/from a higher INFOCON level, acknowledge receipt and report entry into INFOCON Level activities via operational channels to the declaring command. **Chapter 5** provides sample reporting formats.

5-4. (FOUO) Through automated and procedural means, update and maintain a current database of the following characteristics of all critical network infrastructure equipment used to maintain the network (i.e., routers, firewalls, servers, etc.) and a representative sampling of workstations (hereafter called "critical equipment"). Institute appropriate procedures to ensure the baseline is continuously updated to reflect authorized modifications.

5-4.1. (FOUO) User Accounts
5-4.2. (FOUO) Groups
5-4.3. (FOUO) Users in Groups
5-4.4. (FOUO) User/Admin/Group Permissions
5-4.5. (FOUO) Executable files (.exe .com .cmd .vbs .vbe .js .jse .wsf .wsh .dll)
5-4.6. (FOUO) Running Services/Open Ports
5-4.7. (FOUO) Registry keys

- "LMachine!Software/Microsoft/Windows/CurrentVersion/Run"
- "LMachine!Software/Microsoft/Windows/CurrentVersion/RunOnce"
- "LMachine!Software/Microsoft/Windows/CurrentVersion/RunServices"
- "LMachine!Software/Microsoft/Windows/CurrentVersion/RunServiceOnce"
- "CUser!Software/Microsoft/Windows/CurrentVersion/RunOnce"
- "CUser!Software/Microsoft/Windows/CurrentVersion/Run"
- "Lmachine!System/CurrentControlSet/Services"

5-5. (FOUO) Ensure auditing/logging to record, at a minimum: successful and unsuccessful login attempts; file system modifications; and privilege changes. Ensure weekly log review for evidence of abnormal or malicious activity.

5-6. (FOUO) Establish procedures, training, equipment, and administrator certification for the rapid and consistent reestablishment of software baselines for critical equipment.

5-7. (FOUO) Perform operational impact assessment on all mission critical, mission support, and administrative information systems and networks. (Assessing the impact of Computer Network Attack (CNA) on our ability to conduct military operations is key to conducting damage assessment, prioritizing response actions, and assisting in identifying possible adversaries. Identify all critical information systems.)

5-8. (FOUO) Conduct routine vulnerability assessments.

4.3. INFOCON 4, Increased Military Vigilance Procedures.

Table 4.2. (FOUO) INFOCON 4 Procedures.

4-1. (FOUO) Acknowledge receipt/entry into INFOCON 4 and report again upon completion of the first INFOCON 4 cycle.
4-2. (FOUO) Confirm completion of directive measures at previous INFOCON levels.
4-3. (FOUO) Establish exit criteria. (Declaring Command)
4-4. (FOUO) Implement TROs as specified in the implementing message or by regional/local commanders.
4-5. (FOUO) On a 90 day cycle: Upon notification immediately complete the following activities and then every 90 days thereafter. Using manual methods or available automated tools, identify and verify all changes to the system parameters tracked using the database created at INFOCON 5 (step 5-4.). Investigate all unauthorized changes and remove or terminate as appropriate. If this is being conducted automatically, apply the comparison to all servers and workstations. If manual, apply the comparison to critical equipment and a representative sample of workstations.
4-6. (FOUO) If explicit permissions are used on folders or files also check to ensure permissions have not been modified.
4-7. (FOUO) Verify service accounts having administrative privileges on critical equipment and ensure they cannot log on remotely.
4-8. (FOUO) Disable LanMan Hash from all critical equipment if technically feasible.
4-9. (FOUO) Conduct offline rehearsals for the rapid and consistent reestablishment of baselines for SIPRNET and NIPRNET critical equipment as called for in INFOCON 3 Procedures.

4.4. INFOCON 3, Enhanced Readiness Procedures.

Table 4.3. (FOUO) INFOCON 3 Procedures.

3-1. (FOUO) Acknowledge receipt and entry into INFOCON 3 and report again upon completion of the first INFOCON 3 cycle.
3-2. (FOUO) Confirm completion of directive measures at previous INFOCON levels to the declaring Command.
3-3. (FOUO) Establish exit criteria for current INFOCON level. (Declaring Command)
3-4. (FOUO) Implement TROs as specified by implementing message or regional/local commanders.
3-5. (FOUO) Re-establish a secure baseline on a 60-day cycle.
3-6. (FOUO) Conduct offline rehearsals for the rapid and consistent reestablishment of baselines for SIPRNET and NIPRNET critical equipment as called for in INFOCON 2 Procedures.

4.5. INFOCON 2, Greater Readiness Procedures.

Table 4.4. (FOUO) INFOCON 2 Procedures.

2-1. (FOUO) Acknowledge receipt and entry into INFOCON 2 and report again upon completion of the first INFOCON 2 cycle.
2-2. (FOUO) Confirm completion of directive measures at previous INFOCON levels to the declaring Command.
2-3. (FOUO) Establish exit criteria for current INFOCON level. (Declaring Command)
2-4. (FOUO) Implement TROs as specified by implementing message or regional/local commanders.
2-5. (FOUO) Re-establish a secure baseline on a 30-day cycle.
2-6. (FOUO) Reestablish known good software baselines on the following servers, PDC/BDC/ DNS/Web server. As stated above, this step is intended to address the intrusion techniques that cannot be identified or defeated by other means. These modifications to the servers may be accomplished anywhere within the established operational rhythm period, at the local commander's discretion to reduce impact on operations or resources.
2-7. (FOUO) Conduct offline rehearsals for the rapid and consistent reestablishment of baselines for SIPRNET and NIPRNET critical equipment as called for in INFOCON 1 Procedures.

4.6. INFOCON 1, Maximum Readiness Procedures.

Table 4.5. (FOUO) INFOCON 1 Procedures.

1-1. (FOUO) Acknowledge receipt and entry into INFOCON 1 and report again upon completion of the first INFOCON 1 cycle.
1-2. (FOUO) Confirm completion of directive measures at previous INFOCON levels to the declaring Command.
1-3. (FOUO) Establish exit criteria for current INFOCON level. (Declaring Command)
1-4. (FOUO) Implement TROs as specified by implementing message or regional/local commanders.
1-5. (FOUO) Re-establish a secure baseline on a 15-day cycle.

Chapter 5

SAMPLE REPORTING TEMPLATES

5.1. DoD INFOCON Change Alert.

5.1.1. Purpose. The DoD INFOCON Alert Message will be used by CDRUSSTRATCOM to declare a DoD-level INFOCON change.

5.1.2. (FOUO) Content. This message will direct all DoD Components to implement a new DoD INFOCON level. The level of detail may require that this message be classified, and may require sanitization before transmitting to lower command levels. The DoD INFOCON Alert Message may include some or all of the following information:

5.1.2.1. (FOUO) Summary of what events/circumstances drove the INFOCON change.

5.1.2.2. (FOUO) Direction to implement TROs (i.e., actions not prescribed in current INFOCON measure guidance, but tailored to the specific circumstances).

5.1.2.3. (FOUO) Direction to exclude certain actions from the standard set of measures prescribed in this SD.

5.1.2.4. (FOUO) Acknowledgement, exemption and implementation status reporting requirements for DoD Components.

5.1.3. **Figure 5.1.** provides an example of the format and content of the DoD INFOCON Alert Message.

Figure 5.1. (FOUO) Example CDRUSSTRATCOM DoD INFOCON Alert Message.

FM USSTRATCOM OFFUTT AFB NE//CC//

TO (DOD Components)

INFO (IF NECESSARY)

CLASSIFICATION

SUBJ/DOD INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO INFOCON 4 //

RMKS/1. CDRUSSTRATCOM DECLARES DOD GLOBAL INFOCON LEVEL 4, EFFECTIVE IMMEDIATELY. COMBATANT COMMANDERS, SERVICES, AND DOD AGENCIES (DOD COMPONENTS) ARE DIRECTED TO PROCEED TO INFOCON 4.

2. DOD COMMANDERS AT ALL LEVELS STILL RETAIN RESPONSIBILITY AND AUTHORITY TO DIRECT A FURTHER INCREASE IN INFOCON LEVEL WHEN CONDITIONS WARRANT. COMMANDERS WHO ESTABLISH AN INFOCON HIGHER THAN THE DOD LEVEL MUST NOTIFY CDRUSSTRATCOM AND JTF-GNO.

3. BASED ON CJTF-GNO RECOMMENDATION, AS WELL AS COORDINATION WITH DOD COMPONENTS, CDRUSSTRATCOM HAS DETERMINED AN INCREASE TO INFOCON 4 IS WARRANTED IN SUPPORT OF OPERATION XXXXXX.

4. PUBLIC AFFAIRS GUIDANCE. THE FOLLOWING STATEMENT MAY BE USED IN RESPONSE TO QUERY: QUOTE – U.S. STRATEGIC COMMAND, LOCATED IN OMAHA, NE IS RESPONSIBLE FOR COORDINATING AND DIRECTING THE DEFENSE OF DOD COMPUTER SYSTEMS AND COMPUTER NETWORKS. UNDER THE AUTHORITY OF THE SECRETARY OF DEFENSE, COMMANDER, U.S. STRATEGIC COMMAND DIRECTS CHANGES TO DOD INFOCON LEVELS TO ENSURE OPTIMAL READINESS OF DOD COMPUTER SYSTEMS AND COMPUTER NETWORKS. JOINT TASK FORCE – GLOBAL NETWORK OPERATIONS (JTF-GNO), LOCATED IN ARLINGTON, VIRGINIA, IS THE OPERATIONAL COMPONENT OF U.S. STRATEGIC COMMAND THAT EXECUTES THE GLOBAL NETOPS MISSION. THE JTF-GNO MONITORS CYBER INTRUSIONS AND POTENTIAL THREATS, AND DIRECTS/ COORDINATES ACTIONS TO STOP OR CONTAIN DAMAGE AND RESTORE COMPUTER NETWORK OPERATIONS. END QUOTE.

5. USSTRATCOM/JTF-GNO WILL CONTINUE TO EVALUATE THE OPERATIONAL ENVIRONMENT, AND WILL CHANGE (RAISE OR LOWER) THE INFOCON LEVEL WHEN A CHANGE IN OPERATING TEMPO WARRANTS A CHANGE IN INFOCON POSTURES OR WHEN OPERATION XXXXX TERMINATES.

6. POC FOR THIS MESSAGE IS USSTRATCOM GLOBAL OPERATIONS CENTER WATCH OFFICER.//

AKNLDG/YES//

DECL/dd mmm yy//

5.2. DoD INFOCON Change Acknowledgment SITREP.

5.2.1. Purpose. The acknowledgment SITREP will be sent by DoD Components' Operations Centers upon receipt of a DoD INFOCON Alert Message. The message will follow the standard SITREP format.

5.2.2. (FOUO) Content. The DoD INFOCON Change Acknowledgment SITREP will provide a brief acknowledgment of the receipt of a CDRUSSTRATCOM DoD INFOCON Alert Message. It may include some or all of the following information:

5.2.2.1. (FOUO) Confirmation that staffs and subordinate organizations are being notified.

5.2.2.2. (FOUO) Estimated time of completion for notifying appropriate staff members and subordinate organizations.

5.2.2.3. (FOUO) Extenuating circumstances that may prevent prompt dissemination of DoD INFOCON change notification.

5.2.2.4. (FOUO) Any additional TROs the command elects to direct.

5.2.3. Figure 5.2. provides an example of the DoD INFOCON Change Acknowledgement SITREP.

Figure 5.2. (FOUO) Example DoD INFOCON Change Acknowledgement SITREP.

FM (CC/S/A)

TO (DOD Components)

INFO (IF NECESSARY)

CLASSIFICATION

MSGID/SITREP/CDRUSSTRATCOM//

REF/A/MSG/CDRUSSTRATCOM/DOD INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO INFOCON 3/DDHHMMZ MMM YY//

PERID/251500Z/TO:281500Z//

GENTEXT/GENERAL/SITREP REPORTS ACKNOWLEDGEMENT OF CDRUSSTRATCOM INFOCON CHANGE MESSAGE

GENTEXT/SITUATION. ACKNOWLEDGE RECEIPT OF CDRUSSTRATCOM MESSAGE, REF A. OPERATIONS CENTER HAS NOTIFIED ALL SUBORDINATE UNITS WHO HAVE INITIATED INFOCON 3 MEASURES. DIRECTOR, XXX HAS ALSO DIRECTED IMPLEMENTATION OF TAILORED READINESS ACTION T1-01.//

GENTEXT/POC INFORMATION. OPERATIONS CENTER WATCH OFFICER, DSN: XXX-XXX-XXXX, NIPRNET: XXX.XXX.MIL.//

DECL/dd mmm yy//

5.3. INFOCON Status SITREP.

5.3.1. Purpose. Commanders will use the INFOCON Status SITREP whenever their INFOCON status changes. Specific examples include reporting INFOCON implementation status, exceptions/deviations to directed measures, and TROs directed in response to a DoD-level INFOCON change.

5.3.2. (FOUO) Content. The message will provide a commander's status of DoD INFOCON change implementation activities. The message will follow the standard SITREP format, and will include the following INFOCON-specific information:

5.3.2.1. (FOUO) Situation. Brief statement of Commander's operational situation and status of networks, including (as required):

5.3.2.1.1. (FOUO) INFOCON attainment.

5.3.2.1.2. (FOUO) Any assigned networks' INFOCON level within the reporting activity's command that is other than the DoD level.

5.3.2.1.3. (FOUO) Statement of any supporting forces assisting in Commander's INFOCON implementation.

5.3.2.2. (FOUO) Directive Measure Exemptions. Report level of compliance for any directive measure(s) (**Table 4.2.**, Procedure 4-8.) that has either been omitted or whose implementation is delayed:

5.3.2.2.1. (FOUO) Compliance Status. Report level of compliance for this directive measure.

5.3.2.2.2. (FOUO) Estimated Time To Completion. Estimated date/time of compliance with directive measure.

5.3.2.2.3. (FOUO) Rationale For Delay Or Omission. List brief rationale for delay or omission of directive measure.

5.3.2.2.4. (FOUO) Limiting Factors. List any factors that will delay or prevent full implementation of directive measure. Limiting factors may include personnel or other resource constraints, overriding mission operations requirements, etc.

5.3.2.2.5. (FOUO) Repeat DIRECTIVE MEASURE EXEMPTIONS for each delayed or omitted directive measure within the declared DoD INFOCON level.

5.3.2.3. (FOUO) Additional Measures. List any additional measures that have been locally directed in association with the DoD INFOCON change.

5.3.2.4. (FOUO) Operational Impacts. Include a brief statement of operational impact(s) associated with the implementation of INFOCON directive measures, and describe the risk incurred until INFOCON measures are implemented.

5.3.2.4.1. (FOUO) Intelligence-Reconnaissance. Provide any intelligence information as it relates to INFOCON implementation within the DoD Component.

5.3.2.4.2. (FOUO) Logistics. Provide any additional relevant information regarding logistics as it relates to INFOCON implementation that was not already listed as a limiting factor.

5.3.2.4.3. (FOUO) Communications Connectivity. Provide any additional relevant information regarding communications connectivity as it relates to INFOCON implementation that was not already listed as a limiting factor.

5.3.2.4.4. (FOUO) Personnel. Provide any additional relevant information regarding the status, training, or availability of personnel not listed as a limiting factor.

5.3.2.4.5. (FOUO) Significant Political-Military-Diplomatic Events. Significant political, military, and/or diplomatic events associated with or impacting INFOCON implementation and compliance.

5.3.2.4.6. (FOUO) Commander's Evaluation. Include:

5.3.2.4.6.1. (FOUO) Commander's assessment of operational situation.

5.3.2.4.6.2. (FOUO) Estimated date of full INFOCON implementation.

5.3.2.4.6.3. (FOUO) Any additional information as it relates to operational implementation of the INFOCON.

5.3.2.4.6.4. (FOUO) Request for INFOCON/GNO-related support from USSTRATCOM and/or JTF-GNO.

Figure 5.3. (FOUO) Example INFOCON Status SITREP Message.

FM (DOD COMPONENT)

TO (DOD COMPONENT)

INFO (IF NECESSARY)

CLASSIFICATION

MSGID/SITREP/CDRXXX//

REF/A/MSG/CDRUSSTRATCOM/DOD INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO INFOCON 3/DDHHMMZ MMM YY//
APMN/REF A IS CDRUSSTRATCOM MESSAGE DECLARING DOD INFOCON CHANGE.//

PERID/251500Z/TO:281500Z//

GENTEXT/GENERAL/SITREP REPORTS STATUS OF USXXX INFOCON 3 IMPLEMENTATION//

GENTEXT/SITUATION. USXXX INFORMATION NETWORKS ARE FULLY OPERATIONAL. ALL FORCES IMPLEMENTING CDRUSSTRATCOM-DIRECTED INFOCON 3, EFFECTIVE DDHHMMZ MMM YY//

GENTEXT/OPERATIONS//
1. DIRECTIVE MEASURE EXEMPTIONS. DOD A-XX. COMPLIANCE STATUS: ALL MS9X SYSTEMS NON-COMPLIANT. ESTIMATED TIME TO COMPLETION: UNKNOWN, PENDING XXX DISABLE OF LANMAN HASH. RATIONALE FOR DELAY: LANMAN HASH REQUIRED FOR INTERFACE CAPABILITY BETWEEN KEY SERVERS AND LEGACY SERVERS (MS9X). LIMITING FACTORS: REFERENCE JTF-GNO GUIDANCE ON LANMAN HASH DISABLING.
2. ADDITIONAL MEASURES. PASSWORD CHANGES. CDRUSXXX/J3 HAS DIRECTED PASSWORD CHANGES FOR ALL USXXX PERSONNEL WITHIN 72 HOURS.
3. OPERATIONAL IMPACTS. OPS IMPACT OF DIRECTED MEASURE IMPLEMENTATION IS MINIMAL//

GENTEXT/INTELLIGENCE-RECONNAISSANCE. NSTR//

GENTEXT/LOGISTICS. USXXX WILL INCUR ADDITIONAL COSTS FOR OVERTIME CONTRACT SYSTEM ADMINISTRATOR SUPPORT. CDRUSXXX IS ASSESSING REQUIREMENT FOR CONTINGENCY FUND SITE//

GENTEXT/COMMANDER'S EVALUATION. ESTIMATED DATE FOR FULL COMPLIANCE WITH DOD INFOCON 3 IS UNKNOWN, PENDING COMPLIANCE WITH MEASURE B-7. CDRUSXXX'S ASSESSMENT OF OVERALL THREAT TO XXX NETWORKS IS MEDIUM, GIVEN CURRENT INVOLVEMENT IN PEACE SUPPORT OPERATIONS IN COUNTRY ORANGE. WE CONTINUE TO ASSESS ANY DEVELOPING LOCAL THREATS AGAINST OUR INFORMATION NETWORKS AND ARE REVIEWING LOGISTICS AND PERSONNEL REQUIREMENTS SHOULD A FURTHER INCREASE IN DOD INFOCON LEVELS BE WARRANTED. CDRUSXXX REQUESTS NO ADDITIONAL CND-RELATED ASSISTANCE FROM CDRUSSTRATCOM AT THIS TIME.//

DECL/dd mmm yy//

5.4. Local INFOCON Change SITREP.

5.4.1. Purpose. The Local INFOCON Change SITREP will be used by DoD Components to report "local" (within the DoD Component) changes in INFOCON level, and to report INFOCON changes declared at the DoD Component level, respectively.

5.4.2. (FOUO) Content. The content requirements for the Local INFOCON Change SITREP are listed below. The message will follow the standard SITREP format, and will include the following INFOCON-specific information:

5.4.2.1. (FOUO) Situation. Brief statement of commander's operational situation and status of networks, including (as required):

5.4.2.1.1. (FOUO) Description of event/activities leading up to INFOCON change declaration.

5.4.2.1.2. (FOUO) Old INFOCON level prior to level change, and newly declared INFOCON level.

5.4.2.1.3. (FOUO) Date and time of the INFOCON change declaration and name of the organization declaring the INFOCON change.

5.4.2.1.4. (FOUO) Statement of any supporting forces assisting in the commander's INFOCON implementation.

5.4.2.2. (FOUO) Operations.

5.4.2.2.1. (FOUO) Directive Measure Exemptions. Report level of compliance for any directive measure(s) **(Table 4.4.**, Procedure 2-1.) that have either been omitted or whose implementation is delayed:

5.4.2.2.1.1. (FOUO) Compliance Status. Level of DoD Component compliance for this directive measure.

5.4.2.2.1.2. (FOUO) Estimated Time To Completion. Estimated date/time of compliance with directive measure.

5.4.2.2.1.3. (FOUO) Rationale For Delay Or Omission. List brief rationale for delay or omission of directive measure.

5.4.2.2.1.4. (FOUO) Limiting Factors. List any factors that will delay or prevent full implementation of directive measure. Limiting factors may include personnel or other resource constraints, overriding mission operations requirements, etc.

5.4.2.2.1.5. (FOUO) Repeat DIRECTIVE MEASURE EXEMPTIONS for each delayed or omitted directive measure within the declared DoD INFOCON level.

5.4.2.2.2. (FOUO) Additional Measures. List all specific operational and/or technical measures directed in addition to the DoD-level directive measures.

5.4.2.2.3. (FOUO) Operational Impacts. Provide a brief summary of impacted systems/missions. Include a:

5.4.2.2.3.1. (FOUO) Damage/operational assessment.

5.4.2.2.3.2. (FOUO) Description of capabilities, units/organizations, networks, systems, applications, and/or data assessed to be impacted or at risk. Include classification of network(s)/system(s) affected.

5.4.2.2.3.3. (FOUO) Technical assessment of network capabilities.

5.4.2.2.4. (FOUO) Intelligence-Reconnaissance. Provide any intelligence information as it relates to INFOCON implementation within the DoD Component.

5.4.2.2.5. (FOUO) Logistics. Provide any additional relevant information regarding logistics as it relates to INFOCON implementation that was not already listed as a limiting factor in paragraph **5.4.2.2.**

5.4.2.2.6. (FOUO) Communications Connectivity. Provide any additional relevant information regarding communications connectivity as it relates to INFOCON implementation that was not already listed as a limiting factor in paragraph **5.4.2.2.**

5.4.2.2.7. (FOUO) Personnel. Provide any additional relevant information regarding the status, training, or availability of personnel that was not listed as a limiting factor in paragraph **5.4.2.2.**

5.4.2.2.8. (FOUO) Significant Political-Military-Diplomatic Events. Significant political, military, and/or diplomatic events associated with or impacting INFOCON implementation and compliance.

5.4.2.2.9. (FOUO) Commander's Evaluation. Include:

5.4.2.2.9.1. (FOUO) Commander's assessment of operational situation.

5.4.2.2.9.2. (FOUO) Estimated date of full INFOCON implementation.

5.4.2.2.9.3. (FOUO) Any additional information as it relates to operational implementation of INFOCON.

5.4.2.2.9.4. (FOUO) Request for INFOCON/CND-related support from USSTRATCOM and/or JTF-GNO.

5.4.2.2.9.5. (FOUO) Exit criteria.

Figure 5.4. (FOUO) Example Local INFOCON Change SITREP.

FM DOD COMPONENT

TO DOD COMPONENT

INFO (IF NECESSARY)

CLASSIFICATION

MSGID/SITREP/CDRXXX//

REF/A/USPACOM INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO INFOCON 3/DDHHMMZ MMM YY//
APMN/REF A IS CDRXXX MESSAGE DECLARING DOD INFOCON CHANGE.//

PERID/1051500Z/TO: 151500Z//

GENTEXT/GENERAL/SITREP REPORTS STATUS OF USXXX INFOCON 3 CHANGE AND IMPLEMENTATION//

GENTEXT/SITUATION. TACTICAL COMM BACKBONE SUPPORTING DEPLOYED FORCES ASSESSED AS COMPROMISED. INITIAL ASSESSMENT INDICATES INTRUDER MAY BE ASSOCIATED WITH HACKER GROUP SUPPORTING COUNTRY ORANGE. CLASSIFICATION OF NETWORK IS SECRET/RELEASABLE TO COALITION FORCES. ALL USXXX FORCES IMPLEMENTING CDRUSXXX-DIRECTED INFOCON LEVEL INCREASE FROM INFOCON 4 TO INFOCON 3, EFFECTIVE DDHHMMZ MMM YY//

GENTEXT/OPERATIONS//
1. DIRECTIVE MEASURE EXEMPTIONS. NONE. COMPLIANCE STATUS: NSTR. ESTIMATED TIME TO COMPLETION: UNKNOWN. LIMITING FACTORS: LIMITED COUNTRY ORANGE CNE/CNA INTELLIGENCE.
2. ADDITIONAL MEASURES. PASSWORD CHANGES. CDRXXXXXX/J3 HAS DIRECTED PASSWORD CHANGES FOR ALL XXXXXXX PERSONNEL WITHIN 72 HOURS.
3. OPERATIONAL IMPACTS. OPERATIONAL IMPACT OF ACTIVITY IS SERIOUS; LOSS ASSESSMENT ONGOING. COUNTRY ORANGE MAY HAVE ACCESSED OPERATIONS AND INTELLIGENCE INFORMATION RELATED TO COALITION FORCES MISSION EXECUTION. //

GENTEXT/INTELLIGENCE-RECONNAISSANCE. NSTR//

GENTEXT/LOGISTICS. USXXX WILL INCUR ADDITIONAL COSTS FOR OVERTIME CONTRACT SYSTEM ADMINISTRATOR SUPPORT. CDRUSXXX IS ASSESSING REQUIREMENT FOR CONTINGENCY FUND SITE//

GENTEXT/COMMUNICATIONS CONNECTIVITY. NSTR//

GENTEXT/PERSONNEL. NSTR//

GENTEXT/SIGNIFICANT POLITICAL-MILITARY-DIPLOMATIC EVENTS. NSTR//

GENTEXT/COMMANDER'S EVALUATION. ESTIMATED DATE FOR FULL COMPLIANCE WITH USXXXXX INFOCON 3 IS UNKNOWN, CDRUSXXX'S ASSESSMENT OF OVERALL THREAT TO XXX NETWORKS IS HIGH, GIVEN CURRENT INVOLVEMENT IN PEACE SUPPORT OPERATIONS IN COUNTRY ORANGE. WE CONTINUE TO ASSESS LOCAL EVENTS AND ACTIVITIES DIRECTED AT OUR INFORMATION NETWORKS. WE ARE REVIEWING LOGISTICS AND PERSONNEL REQUIREMENTS SHOULD A FURTHER INCREASE IN USXXX INFOCON LEVELS BE WARRANTED. CDRUSXXX REQUESTS NO ADDITIONAL CND-RELATED ASSISTANCE FROM CDRUSSTRATCOM AT THIS TIME. EXIT CRITERIA FOR DETERMINING WHETHER TO EXIT INFOCON 3 SHALL INCLUDE A CHANGE OF ADVERSARY ACTIVITIES. //

DECL/dd mmm yy//

Chapter 6

SAMPLE TAILORED READINESS OPTIONS

6.1. General. Any item from the standard INFOCON measures can be implemented as a stand-alone TRO.

6.2. TROs. (Examples for **illustration** only).

6.2.1. (FOUO) TRO ONE - Passwords.

Table 6.1. (FOUO) Elements of TRO ONE.

T1-01	Issue Passwords
T1-02	Include multiple non-printable characters
T1-03	Change passwords only with face to face contact

6.2.2. (FOUO) TRO TWO - Rebuilding of key servers.

Table 6.2. (FOUO) Elements of TRO TWO.

T2-01	Rebuild SIPRNET Domain Controllers
T2-02	Rebuild SIPRNET Web Servers

6.2.3. (FOUO) TRO THREE – Permissions.

Table 6.3. (FOUO) Elements of TRO THREE.

T3-01	Reduce all permissions except trusted super user to minimum levels and reinstitute only with face-to-face contact

6.2.4. (FOUO) TRO FOUR - Anti-virus definitions.

Table 6.4. (FOUO) Elements of TRO FOUR.

T4-01	Using automated means, test all network addresses for current antivirus (AV) signatures. Lock out all addresses where AV signatures cannot be verified.

6.2.5. (FOUO) TRO FIVE - Firewall signatures.

6.2.6. (FOUO) TRO SIX - Intrusion Detection System (IDS) rules.

6.2.7. (FOUO) TRO SEVEN - Access Control Lists.

Table 6.5. (FOUO) Elements of TRO SEVEN.

T7-01	Block all Port 25 TCP and UDP to non-mail servers
T7-02	Block inbound Port 80 TCP and UDP to non-mail servers

6.2.8. (FOUO) TRO EIGHT – Connectivity.

Table 6.6. (FOUO) Elements of TRO EIGHT.

T8-01	Disable Remote Maintenance
T8-02	Disable dial-in access
T8-03	Disable shares

6.2.9. (FOUO) TRO NINE – Logging.

Table 6.7. (FOUO) Elements of TRO NINE.

T9-01	Offload logging of domain controllers to external storage

6.2.10. (FOUO) TRO-TEN - Load Control.

Table 6.8. (FOUO) Elements of TRO TEN.

T10-01	Implement Minimize
T10-02	Disable outbound Port 80 for non-essential users
T10-03	Disable FTP for non-essential users

CORT O. HACKER, Major, USAF
Command Secretariat

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSM 3402.01B, (S) *Alert System of the Chairman of the Joint Chiefs of Staff* (U), 1 November 2000

CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*, 25 March 2003

CM-510-99, CJCS Memorandum, *Information Operations Condition (INFOCON)*, 10 March 1999

DoDD O-8530.1, *Computer Network Defense (CND)*, 8 January 2001

DoDI O-8530.2, *Support to Computer Network Defense (CND)*, 9 March 2001

NetOps CONOPS, *Joint Concept of Operations for Global Information Grid NetOps*, 15 August 2005

Abbreviations and Acronyms

AIS—Automated Information Systems

BDC—Backup Domain Controller

CDRUSSTRATCOM—Commander, United States Strategic Command

CJTF-GNO—Commander, Joint Task Force for Global Network Operations

CNA—Computer Network Attack

CND—Computer Network Defense

CNE—Computer Network Exploitation

CNEC—Computer Network Event Conference

COI—Community of Interest

DNS—Domain Name Server

DoD—Department of Defense

FOUO—For Official Use Only

FTP—File Transfer Protocol

GIG—Global Information Grid

GNO—Global Network Operations

IA—Information Assurance

IAW—In Accordance With

IC—Intelligence Community

IC-IRC—Intelligence Community Incident Response Center

INFOCON—Information Operations Condition

IP—Internet Protocol

IS—Information System

IT—Information Technology

JS/J-3—Joint Staff Director for Operations

JTF-GNO—Joint Task Force for Global Network Operations

NetOps—Network Operations

NIPRNET—Non-classified Internet Protocol Routing Network

OPSEC—Operations Security

OPTEMPO—Operational Tempo

PDC—Primary Domain Controller

SD—Strategic Command Directive

SIPRNET—Secret Internet Protocol Router Network

SITREP—Situation Report

TCP—Transmission Control Protocol

TRO—Tailored Readiness Option

UDP—User Data Protocol

U.S.—United States

USSTRATCOM—United States Strategic Command

Terms

Access—Opportunity to make use of an information system (IS) resource.

Access Control—Limiting access to IS resources only to authorized users, programs, processes or other systems.

Accountability—Process of tracing IS activities to a responsible source.

Application—Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges.

Assurance—Measure of confidence that the security features, practices, procedures and architecture of an IS accurately mediate and enforce the security policy.

Audit—Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Availability—Timely, reliable access to data and information services for authorized users.

Baseline—Represents the most up to date operating system (patches, etc) that can be used to reload a system. As it applies to INFOCON, this is the latest known snapshot of the system including all approved changes.

Computer Emergency Response Team(s) (CERT)—CERTs are teams composed of personnel with technical expertise and organic equipment that may deploy to assist remote sites in the restoration of computer services. Services have formed CERTs as an operational organization for rapid response to both deployed and installation based Service forces. ***Note:*** Some teams may be referred to as Computer Security Incident Response Team(s) (CSIRT) or Computer Incident Response Team(s) (CIRT).

Computer Network Attack (CNA)—Operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Exploitation (CNE)—Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations.

Computer Network Defense (CND)—Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks. ***Note:*** The unauthorized activity may include disruption, denial, degradation, destruction, exploitation or access to computer networks, information systems or their contents or theft of information. CND protection activity employs information assurance protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, detection activities, including trend and pattern analysis, are performed by multiple disciplines within the DoD, e.g., network operations, CND Services, intelligence, counterintelligence and law enforcement. CND response can include recommendations or actions by network operations (including information assurance), restoration priorities, law enforcement, military forces and other U.S. Government agencies.

Data—Representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

Distributed Denial of Service (Attack)—Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.

DoD Information System—Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display or transmission of information. Includes AIS applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Enclave—Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.

Event—Occurrence, not yet assessed, that might effect the performance of an IS.

Firewall—System designed to defend against unauthorized access to or from a private network.

Global Information Grid (GIG)—Globally interconnected, end-to-end of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalitions, allied and non-DoD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

Incident—IS assessed occurrence having actual or potentially adverse effects on an IS.

Information—Any communications or representation of knowledge such as facts, data or opinion in any medium or form including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

Information Assurance (IA)—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of ISs by incorporating protection, detection and reaction capabilities.

Information Operations—Actions taken to affect adversary information and ISs while defending one's own information and ISs.

Information System (IS)—Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, display or transmission of information.

Intrusion—Unauthorized act of bypassing the security mechanism of a system.

Operating System—An integrated collection of routines that service the sequencing and processing of programs by a computer. ***Note:*** An operating system may provide many services, such as resource allocation, scheduling, input/output control and data management. Although operating systems are predominantly software, partial or complete hardware implementations may be made in the form of firmware.

Operations Security (OPSEC)—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) identify those actions that can be observed by adversary intelligence systems; b) determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and/or c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Password—Protected/private string of letters, numbers and special characters used to authenticate an identity or to authorize access to data.

Restoration—Action taken to repair and return to service, an impaired (degraded) or unserviceable telecommunications service or facility. ***Note:*** Permanent or temporary restoration may be accomplished by various means, such as patching, rerouting, substitution of component parts, etc.

Risk—Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability.

Secret Internet Protocol Router Network (SIPRNET)—Worldwide Secret level packet switch network using high-speed Internet protocol routers and high-capacity Defense Information Systems Network circuitry.

System Administrator—Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters and sound implementation of established IA policy and procedures.

Telecommunications—Preparation, transmission, communication or related processing of information (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electro-optical or electronic means.

Threat—Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

User—Individual or process authorized to access an IS.

Vulnerability—Weakness in an IS, system security procedures, internal controls or implementation that could be exploited.