Information Conditions (INFOCON)

Proficiency Code: A

The *INFOCON* system is a commander‘s alert system that establishes a uniform process for posturing and defending against malicious activity targeted against U.S. DoD information systems and networks. The *INFOCON* system was developed for U.S. DoD information systems and networks. However, it is acknowledged that U.S. involvement in future conflicts will likely be within a Combined operations environment. This implies that the success of the Warfighting operations will depend greatly on the ability of the U.S. and allied/coalition partners to ensure continued availability and access to critical mission and support information systems and information networks.

The *INFOCON* system is a commander‘s alert system, characterized by five progressive levels of threats to information networks, and a series of increasing defensive measures that apply to information systems and, to a lesser extent, users of these systems. Specific features assist the commander in using the *INFOCON* system. A risk mitigation tool aids the commander in proactively declaring postures *and* directing defensive actions based on advanced indications and warning of hostile activity. The *INFOCON* system also guides the commander in identifying the *INFOCON* posture in the event predictive intelligence is not possible. The uniform application of defensive measures promotes predictable responses to crises and provides timely, accurate, and clear direction to commanders. Flexibility is built into the *INFOCON* system to allow additional specific actions to be mandated, based on the threat. Thus, the *INFOCON* system provides a range of defensive measures that support operations at all levels of conflict, peacetime operations through combat operations, and back to restoration of peace. The *INFOCON* system pertains to all information systems and networks, including interconnections between public and coalition networks.

The *INFOCON* strategy is 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. CDRUSSTRATCOM directs changes in the global *INFOCON* status, while changes in local or regional *INFOCON* status will be more actively managed by commanders at all levels (e.g., base, post, camp, station, major command) using a framework of standardized measures. *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 that every commander must make. The *INFOCON* are supplemented by Tailored Readiness Options (TROs), which are applied in order to respond to specific intrusion characteristics or activities, directed by CDRUSSTRATCOM or commanders. The *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 170 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.

Posture Levels:

a. 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.

b. *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. 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.

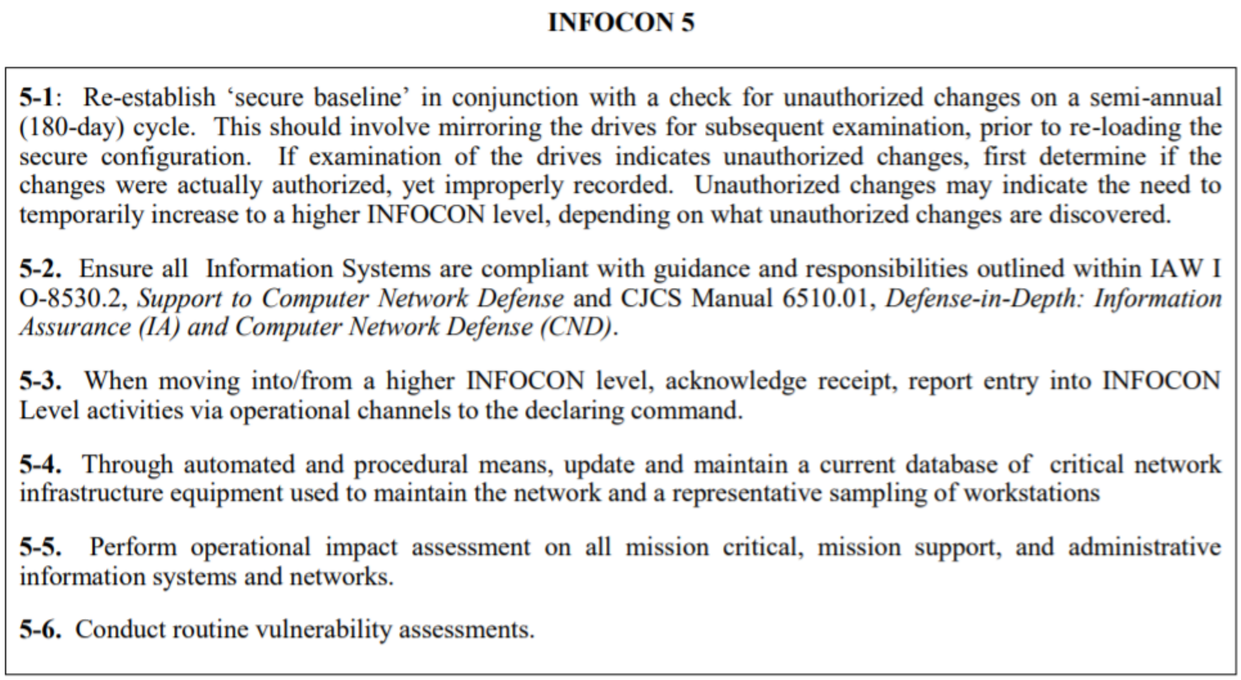
c. INFOCON 3. INFOCON 3 further increases NetOps readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to end-users is minor.

d. 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. Impact to endusers could be significant for short periods, which can be mitigated through training and scheduling.

e. 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. Currently, 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.

Structure:

a. *INFOCON* 5, NORMAL READINESS.



INFOCON 5

5-1: 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. Unauthorized changes may indicate the need to temporarily increase to a higher INFOCON level, depending on what unauthorized changes are discovered.

5-2. Ensure all Information Systems are compliant with guidance and responsibilities outlined within IAW I O-8530.2, *Support to Computer Network Defense* and CJCS Manual 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND).*

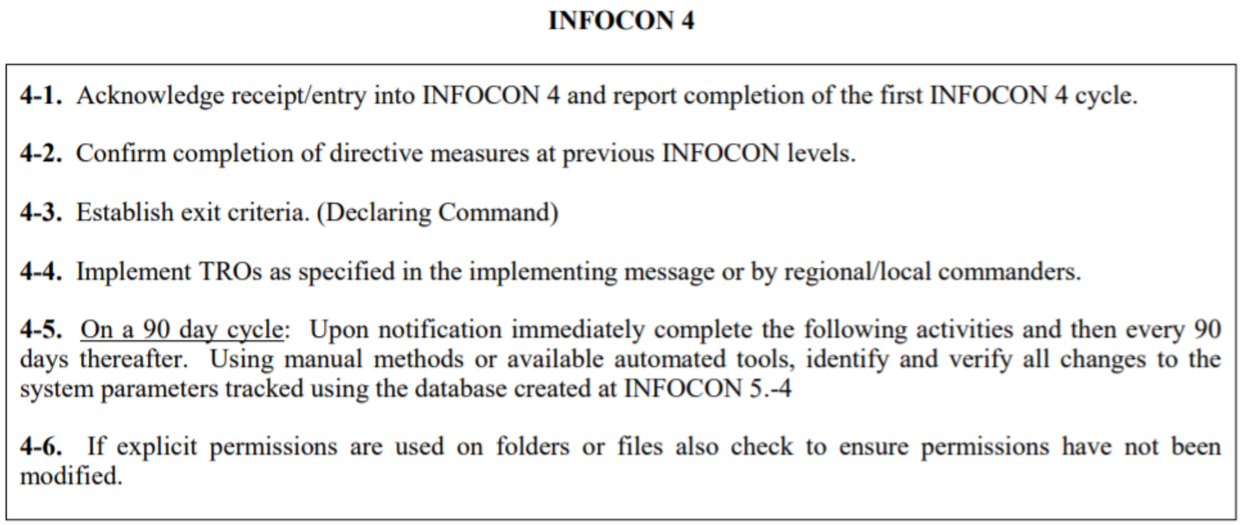
5-3. When moving into/from a higher INFOCON level, acknowledge receipt, report entry into INFOCON Level activities via operational channels to the declaring command.

5-4. Through automated and procedural means, update and maintain a current database of critical network infrastructure equipment used to maintain the network and a representative sampling of workstations

5-5. Perform operational impact assessment on all mission critical, mission support, and administrative information systems and networks.

5-6. Conduct routine vulnerability assessments.

b. *INFOCON* 4, INCREASED MILITARY VIGILANCE.



INFOCON 4

4-1. Acknowledge receipt/entry into INFOCON 4 and report completion of the first INFOCON 4 cycle.

4-2. Confirm completion of directive measures at previous INFOCON levels.

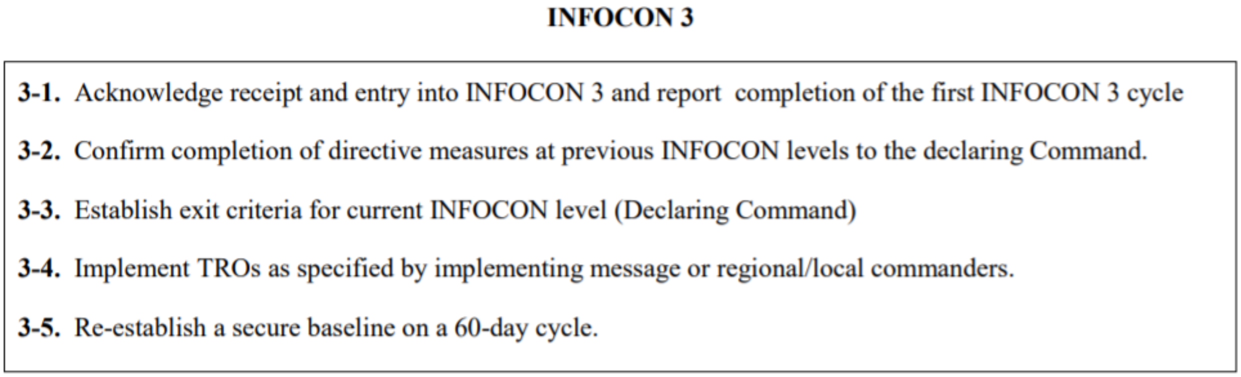
4-3. Establish exit criteria. (Declaring Command)

4-4. Implement TROs as specified in the implementing message or by regional/local commanders.

4-5. 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.-4

4-6. If explicit permissions are used on folders or files also check to ensure permissions have not been modified.

c. *INFOCON* 3, ENHANCED READINESS.



INFOCON 3

3-1. Acknowledge receipt and entry into INFOCON 3 and report completion of the first INFOCON 3 cycle

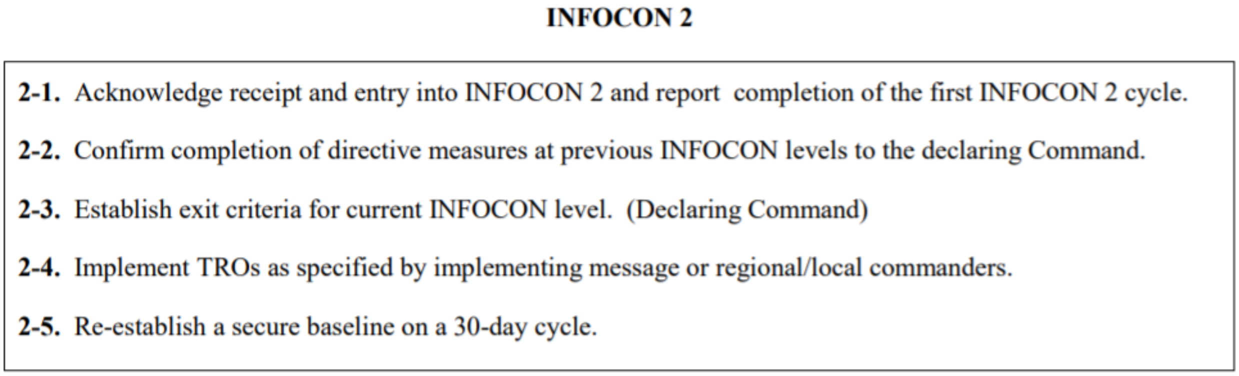
3-2. Confirm completion of directive measures at previous INFOCON levels to the declaring Command.

3-3. Establish exit criteria for current INFOCON level (Declaring Command)

3-4. Implement TROs as specified by implementing message or regional/local commanders.

3-5. Re-establish a secure baseline on a 60-day cycle.

d. *INFOCON* 2, GREATER READINESS.



INFOCON 2

2-1. Acknowledge receipt and entry into INFOCON 2 and report completion of the first INFOCON 2 cycle.

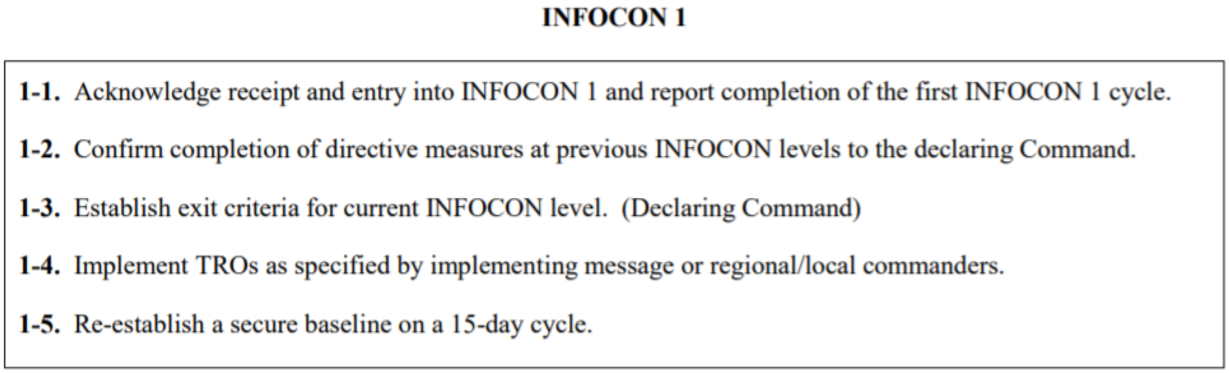
2-2. Confirm completion of directive measures at previous INFOCON levels to the declaring Command.

2-3. Establish exit criteria for current INFOCON level. (Declaring Command)

2-4. Implement TROs as specified by implementing message or regional/local commanders.

2-5. Re-establish a secure baseline on a 30-day cycle.

e. *INFOCON* 1, MAXIMUM READINESS.



INFOCON 1

1-1. Acknowledge receipt and entry into INFOCON 1 and report completion of the first INFOCON 1 cycle.

1-2. Confirm completion of directive measures at previous INFOCON levels to the declaring Command.

1-3. Establish exit criteria for current INFOCON level. (Declaring Command)

1-4. Implement TROs as specified by implementing message or regional/local commanders.

1-5. Re-establish a secure baseline on a 15-day cycle.