[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@3ed1573679204f3e8bddd2053331c805?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

ref <https://militarybase.net/infocon/>

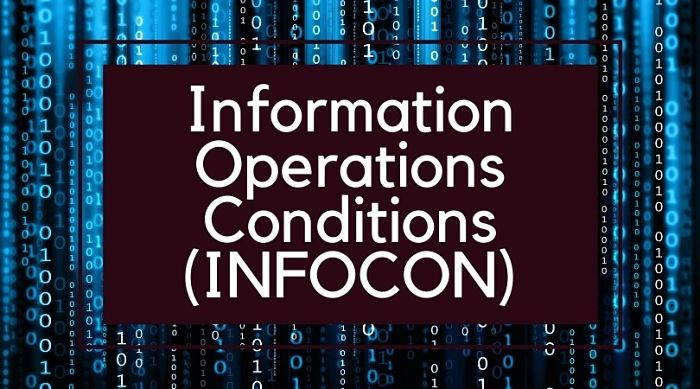
**[](https://militarybase.net/)**

Information Operations Conditions (INFOCON)

 by [Joe Wallace](https://militarybase.net/author/joe-wallace/)

The Information Operations Conditions, or INFOCON system is designed  to indicate the current level of response to threats against Department  of Defense computer networks, systems, and individual machines. It is  designed to present a “structured, coordinated approach to defend  against and react to adversarial attacks,” according to DoD sources.

INFOCON is similar in nature to [Force Protection Conditions or FPCON](https://militarybase.net/fpcon-levels/), but is applicable to networks rather than military bases. A Strategic  Command Directive DoD publication from 2006, notes that INFOCON strategy changed the DoD approach from a reactive system (reacting to threats  rather than “preventive medicine”) to a “readiness-based,” proactive  approach.



**How INFOCON works**

INFOCON has five levels (see below) ranging from normal conditions  all the way to responding to a general attack. Like FPCONs, these  conditions may vary from base to base, command to command, and even  between theatres of operations. There may be a military installation  operating under a higher INFOCON level than others elsewhere due to  specific threats or conditions that warrant the elevated levels.

INFOCONs are adjusted as conditions warrant, and they may not change  in sequential order. Instead, they are applied according to the nature  of the threat or potential threat.

The rules governing INFOCONs, again similar to FPCONs, will apply to  all military and civilian personnel working in an affected area. A good  example of how this policy is implemented can be found in a 2016 order  from the Luke Air Force Base 56th Fighter Wing Commander, which includes the following instructions:

“(INFOCONS apply) to all military and civilian personnel on Luke Air  Force Base”, noting that INFOCON recommends actions “to uniformly  heighten or reduce defensive posture, defend against computer network  attacks, and mitigate  sustained damage to the Luke AFB  information  infrastructure”.

DoD INFOCONs are used to focus on “computer network-based protective  measures”. Each level of INFOCON represents defensive measures taken  based on the risks presented “through the intentional disruption of  friendly information systems”.

What kinds of disruption? Any operation that may include attempts to:

* Disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks
* Scanning, probing, “other suspicious activities”
* Gain unauthorized access
* Perform unauthorized “data browsing”

**The Five INFOCON Levels**

**INFOCON 5:**No significant threats or activity.

**INFOCON 4:** A “heightened threat” of a possible  information system attack. This may be associated with localized events  or issues, military operations, and may also be assigned as the result  of “increased information system probes”, scans, or other attempts to  compromise a government network or communication system.

**INFOCON 3:** This level is necessary where there are  indications that a specific system, location, unit or operation may be  targeted. It may also be implemented during a major military operation.  Other things that can trigger INFOCON 3 or contingency include an  elevated level of network probes or scans. Any indication that there has been an increase or concentration in attempts (successful or not) or  surveillance may trigger INFOCON 3.

**INFOCON 2:** This level applies when a “limited  attack” has been launched against a government network or system.  INFOCON 2 is appropriate when there was limited success in an attack or  intrusion, with little or no data loss or system compromise. In these  scenarios the information system is still generally functional and  available for official use.

**INFOCON 1:**The condition required when there has  been a successful attack on an information system with a definite effect upon DoD missions or operations. Attacks under INFOCON 1 are generally  widespread, interfering with “the ability of the targeted system(s) to  function effectively,“ and creating risk of mission failure.

**Who Is Responsible For INFOCONs?**

INFOCONs require support from designated authorities in a government  computer network such as the Functional System Administrator (FSA) and  Client Support Administrator (CSA) or their equivalents.

Because network security relies on the cooperation of the most basic  end user all the way up to the FSA, CSA and above for a given system,  there are a series of checklists and procedures that each network will  adopt on the local level. In general, unit commanders “are responsible  for implementing appropriate portions of the INFOCON checklists and/or  any other security measures for their areas of responsibility” in many  cases.

Similar to FPCONs, the approved authority for setting and regulating  the conditions establishes the appropriate threat condition level, and  all who work with these networks will have their own marching orders. In the same way that an FPCON alters day to day activity with increased ID checks, searches and patrols, and enhanced force protection measures,  the computer network version of these protective conditions apply via  INFOCONs.

**Concepts That Inform INFOCONs**

The DoD Command Directive from 2006 about INFOCONs we mentioned at  the beginning of this article includes some general instructions about  dealing with cyber threats and intrusion attempts under INFOCON.

For example, the Command Directive indicates that when INFOCON levels must be changed due to increased threat levels, those increased levels  “should not result in a self-imposed denial of service, either to  specific users or to entire networks.” While responding to threats  during an elevated INFOCON situation, specific ports, IP addresses, or  other network features may need to be individually dealt with, they are  implemented only when necessary.

“As military operations continue to rely more and more on net-centric operations,” the Command Directive states, INFOCON measures must be  tied to operational activities of the affected commands.

And the awareness of threats from within an organization are not lost on military planners. INFOCON measures “should mitigate insider threats from both authorized and unauthorized users,” according to the 2006  directive.