

**BY ORDER OF THE COMMANDER  
56TH FIGHTER WING (AETC)**

**LUKE AIR FORCE BASE  
INSTRUCTION 10-710**



**19 JULY 2016**

**Operations**

**INFORMATION OPERATIONS  
CONDITIONS (INFOCON)**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available on the e-Publishing website at [www.e-Publishing.af.mil](http://www.e-Publishing.af.mil) for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: 56 CS/SCOSC

Certified by: 56 CS/CC  
(Maj Lewis G. Sorvillo)

Supersedes: LUKEAFBI 10-710, 4 May  
2009

Pages: 6

---

This instruction establishes procedures for implementation of Information Operations Condition (INFOCON). Program policy and requirements for all information systems, and provides responsibilities and guidance for establishing and managing the program. It applies to all military and civilian personnel on Luke Air Force Base (Luke AFB). The 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, to include computer and telecommunications networks and systems. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW AFMAN 33-363, *Management of Records*, and disposed of IAW the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, T-3”) number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. This publication may not be supplemented or further implemented/extended. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

## *SUMMARY OF CHANGES*

**This publication is substantially revised and must be completely reviewed.** Changes include paragraphs 2.4.1. and 2.4.2, updating Normal and Non-duty hour contact numbers. Updates Attachment 1, Glossary of References and Supporting Information.

### **1. RESPONSIBILITIES**

1.1. Wing Commander: During local INFOCON declaration, the 56th Fighter Wing Commander (56 FW/CC) has the overall authority for INFOCON implementation on Luke AFB and declares increases or decreases in INFOCON posture based on hostile network activity directed against the 56 FW and Luke AFB network resources.

1.2. Communications Squadron Commander: The 56th Communications Squadron Commander (56 CS/CC) is the wing Communications Systems Officer (CSO) and, when appropriate, is responsible for informing the 56 FW/CC of local or downward directed (AETC) INFOCON status updates.

1.2.1. For local or downward directed (AETC) INFOCON status updates, the CSO receives notification from the Communications Focal Point representative, and will contact the 56 FW/CC and 56th Fighter Wing Command Post (56 FW/CP) using reporting procedures appropriate for the level of threat.

1.3. Communications Focal Point (CFP):

1.3.1. The CFP is the overall point of contact for INFOCON and ensures unit Functional System Administrators (FSAs) and Client Support Administrators (CSAs) are kept informed of INFOCON status and threats to Luke AFB systems.

1.3.2. The CFP will:

1.3.2.1. Be the primary focal point for all INFOCON status reporting and will keep the CSO and 561st Network Operations Squadron (561 NOS) informed of compliance.

1.3.2.2. Prepare for round-the-clock operations when directed by the CSO.

1.3.2.3. Provide technical assistance to the group FSAs and CSAs.

1.3.2.4. Filter compliance and attainment status reports from FSAs/CSAs and document compliance of INFOCON checklists.

1.4. Network Operations Center (NOC):

1.4.1. The NOC implements general actions and/or specific measures to increase the security of the network. Additionally, the NOC provides technical advice and recommendations to the chain of command.

1.4.2. The NOC will:

1.4.2.1. Provide operational assessment to the CSO during all INFOCON status changes so he/she can properly brief the 56 FW/CC and obtain approval to release said changes.

1.4.2.2. Prepare for round-the-clock operations when directed by the CSO.

### 1.5. 56 FW/CP:

1.5.1. 56 FW/CP will inform base personnel of INFOCON status changes.

### 1.6. Functional System Administrator (FSA) and Client Support Administrator (CSA):

1.6.1. Network security is a collaborative effort that can impact all users. Through FSAs, CSAs and network users, unit commanders are responsible for implementing appropriate portions of the INFOCON checklists and/or any other security measures for their areas of responsibility. FSAs and CSAs must familiarize themselves and comply with this instruction. In addition, FSAs, CSAs and network users must understand that in times of increased threat, their ability to carry out routine duties maybe impacted by the need to protect mission critical systems (Attachment 3).

1.6.2. When directed, FSAs and CSAs will use the INFOCON checklists located on the 56 CS Share Point page: [https://luke.eis.aetc.af.mil/56MSG/CS/56\\_SCO/INFOCON/Forms/AllItems.aspx](https://luke.eis.aetc.af.mil/56MSG/CS/56_SCO/INFOCON/Forms/AllItems.aspx) and implement immediately upon notification.

1.6.3. Upon notification of INFOCON status change, the FSA/CSA will notify the CFP of acknowledgment of INFOCON status. When appropriate INFOCON checklist and/or any other specific security measure is complete, unit FSA/CSAs will notify the CFP of attainment or provide hourly updates until attainment is reached. In addition, FSAs/CSAs will notify unit Information System Security Officers (ISSO) of any actions required.

## 2. NOTIFICATION PROCEDURES

2.1. Technical reporting will be accomplished IAW INFOCON FSA/CSA checklists.

2.2. During Normal Duty Hours: The CFP and/or NOC will be notified by the Air Force Network Operations Center/Network Control Division (AFNOC/NCD), 561 NOS, or exercise official. The CFP will notify the CSO. The CSO will contact the 56 FW/CC and the 56 FW/CP. For local INFOCON status, based upon the recommendation from the CSO, the 56 FW/CC will determine the appropriate INFOCON level. After approval from 56 FW/CC to change INFOCON level, the 56 FW/CP will notify all units of the INFOCON level. Once units receive notification that an INFOCON level has been mandated, they will execute the appropriate checklist and/or security measures.

2.3. During Non-Duty Hours: The CFP and/or 56 FW/CP will be notified by AFNOC or 561 NOS. The 56 FW/CP will notify the 56 FW/CC and CSO.

2.4. The following telephone extension will be used for INFOCON reporting:

2.4.1. Normal duty hours: 6-4400, Option 8.

2.4.2. Non-duty hours: 6-4400, Option 7.

SCOTT L. PLEUS  
Brigadier General, USAF  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

CJCSI 6510.01E, Information Assurance and Support to Computer Network Defense, 9 Jun 2015

DODI 3600.2, Information Operations Security Classification Guidance, 28 Nov 05

DODD 3020.26, Department of Defense Continuity Programs, 9 Jan 2009

AFI 10-710, Information Operations Condition (INFOCON), 10 Aug 06

AFMAN 33-363, *Management of Records*, 1 March 2008

AFNetOps Security Classification Guide, 20 Apr 07

***Adopted Forms***

AF Form 847, *Recommendation for Change of Publication*;

***Abbreviations and Acronyms***

**AETC**—Air Education and Training Command

**AF**—Air Force

**AFI**—Air Force Instruction

**AFRIMS**—Air Force Records Information Management System

**CC**—Commander

**CFP**—Communications Focal Point

**CP**—Command Post

**CSA**—Client Support Administrator

**CSO**—Communications Systems Officer

**FSA**—Functional System Administrator

**FW**—Fighter Wing

**INFOCON**—Information Operations Condition

**ISSO**—Information System Security Officers

**NOC**—Network Operations Center

**RDS**—Records Disposition Schedule

## Attachment 2

### BASIC INFOCON PROCEDURES

**A2.1. DESCRIPTION:** The INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer and telecommunication networks and systems. While all communications systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and standoff capability make computer network attack (CNA) an attractive option to our adversaries at present. The DoD INFOCON criteria and response actions may be expanded at a later date to include all forms of information operations. CNA is defined as “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” INFOCON also outlines countermeasures to scanning, probing, other suspicious activities, unauthorized access, and data browsing. DoD INFOCON measures focus on computer network-based protective measures, due to the unique nature of CNA. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are 5 (normal activity), 4 (increased risk of attack), 3 (specific risk of attack), 2 (limited attack), and 1 (general attack). Countermeasures at each level include notifications, increased security practices, higher headquarters reporting, and higher INFOCON review.

#### **A2.2. DEFINITIONS:**

A2.2.1. INFOCON 5. Indicates no significant activity.

A2.2.2. INFOCON 4. A heightened threat of a possible information system attack related to regional events occurring that affect U.S. interests, or on-going or planned military operations/contingencies, or increased information system probes, scans, or other activities detected indicating a pattern of surveillance.

A2.2.3. INFOCON 3. Indications & Warnings (I&W) indicate the targeting of a specific system, location, unit or operation, or a major military operation or contingency is planned or on-going, or a significant level of network probes, scans or activities has been detected indicating a pattern of concentrated reconnaissance. Other actions could include attempted or successful network penetrations or denial of service attempts.

A2.2.4. INFOCON 2. Intelligence assessment(s) and reports indicate a limited attack has occurred. Information system attack(s) was detected with limited impact to DoD operations. Attack resulted in minimal success and was successfully counteracted with little or no data loss or systems compromised. Information system is still mission capable.

A2.2.5. INFOCON 1. Successful information system attack(s) detected and in progress which impact DoD operations. The attack(s) is widespread and undermines the ability of the targeted system(s) to function effectively and poses a significant risk of mission failure. Primary efforts must be focused on recovery and reconstitution of damaged mission critical systems and files.

## Attachment 3

## CRITICAL INFORMATION SYSTEMS

Table A3.1. Critical Information Systems and Responsible Organization.

<b><u>CRITICAL INFORMATION SYSTEMS</u></b>	<b><u>RESPONSIBLE ORGANIZATION</u></b>
Storage Area Network	56 CS/Network Operations
(Our connection to) Non-Secure Internet Protocol Router Network (NIPRNET)	56 CS/Network Infrastructure
(Our connection to) Secret Internet Protocol Router Network (SIPRNET)	56 CS/Network Infrastructure
Information Transfer Nodes (ITNs)	56 CS/Network Infrastructure
Boundary Systems	561 NOS
Cargo Movement Operations Systems (CMOS)	56 LRS
Logistics Module (LOGMOD-B)	56 LRS
Supply Asset Tracking System (SATS)	56 LRS
Fuels Automated System (FAS)	56 LRS
DEERS/RAPIDS	56 FSS
Deliberate and Crisis Action Planning and Execution Systems (DCAPES)	56 FSS
Military Personnel Data System (MILPDS)	56 FSS
Standard Procurement System (SPS)	56 CONS
Graduated Training Integrated Management System (GTIMS)	56 OSS
Armed Forces Health Longitudinal Technology Application (AHLTA)	56 MDG