DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

AFI10-1701_AFGM2016-01
12 MAY 2016

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1480 Air Force Pentagon
Washington, DC 20330-1480

SUBJECT: Air Force Guidance Memorandum 1 to AFI 10-1701, *Command and Control for Cyberspace Operations*

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately changes Air Force Instruction 10-1701, *Command and Control for Cyberspace Operations*, 5 March 2014. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with (IAW) AFI 33-360, *Publications and Forms Management*. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

As a result of the publication of AF Policy Directive 17-2, *Cyberspace Operations*, which supersedes AFPD 10-17, *Cyberspace Operations*, dated 31 July 2012; AFI 10-1701 is hereby renumbered as AFI 17-201. This Memorandum is a renumbering of AFI 10-1701 only; the title and content remain unchanged. I hereby direct the Office of Primary Responsibility (OPR) for AFI10-1701 to conduct a special review in accordance with AFI33-360 to align its content with AFPD17-2. This will result in a rewrite or rescind action of AFI10-1701.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon rescinding or rewrite of AFI 10-1701, whichever is earlier**.**

WILLIAM J. BENDER, Lt Gen, USAF
Chief of Information Dominance and Chief
Information Officer

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-1701

5 MARCH 2014

Operations

COMMAND AND CONTROL (C2) FOR CYBERSPACE OPERATIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: AF/A3CS/A6CS

Certified by: AF/A3C/A6C
(Maj Gen Earl D. Matthews)

Pages: 15

This Instruction implements Air Force Policy Directive (AFPD) 10-17, *Cyberspace Operations*, and provides guidance for command and control of activities covered in AFI 33-115, *AF IT Services* and supporting Methods and Procedures Technical Orders (e.g., Vulnerability Management MPTO, etc.). This AFI introduces the term *AF Information Networks (AFIN)* as a replacement for the previously-used term AF-GIG. The AFIN is defined as the globally interconnected, end-to-end set of Air Force information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy-makers, and support personnel, including owned, leased and contracted communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. The terms AF Network (AFNET) and AF Network-Secure (AFNET-S) are introduced to refer to the Air Force's underlying Non-Secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet). This publication applies to all military and civilian AF personnel, members of the AF Reserve Command (AFRC), Air National Guard (ANG), third-party governmental employee and contractor support personnel in accordance with appropriate provisions contained in memoranda support agreements and AF contracts. Violations shall serve as a basis for denying individual's access to the AFIN. 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*, Table 1.1 for a description of the authorities associated with the Tier numbers. Requests for waivers must be submitted through HQ AFSPC/A3 to the OPR listed above for consideration and approval. 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 Form 847s from the field through the appropriate functional's chain of

command. This publication may be supplemented at any level, but all direct Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AF Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in the AF Records Information Management System (AFRIMS).

1. General.

1.1. In accordance with AFPD 10-17, the Commander, AF Space Command (AFSPC/CC) is responsible for the overall command and control, security and defense of the AFIN. AFSPC/CC is responsible for the command, control, implementation, security, operation, maintenance, sustainment, configuration, and defense of the AFNET/AFNET-S. Cyber orders issued by AFSPC/CC or his/her delegated representative are military orders issued by order of the Secretary of the Air Force.

1.2. The Unified Command Plan gives the Commander, U. S. Strategic Command (CDRUSSTRATCOM) responsibility to direct operations and defense of the Department of Defense (DoD) Information Networks (DoDIN). CDRUSSTRATCOM, either directly or via Commander, U.S. Cyber Command (USCYBERCOM), issues such orders as required to operate and defend the DoDIN and direct other cyberspace operations as required in support of requesting Combatant Commanders (CCDRs). 24 AF (AFCYBER) is the AF component to USCYBERCOM and, as such, is responsible for ensuring assigned/attached AF forces perform the missions and tasks assigned by USCYBERCOM.

1.3. Command and Control, General.

1.3.1. Classified processes governing C2 of AF offensive and defensive cyberspace operations conducted by AF Cyber Mission Forces are addressed in a classified CJCS Execute Order (title classified) issued on 21 Jun 13.

1.3.2. When necessary to respond to a critical cyber event, as declared by CDRUSSTRATCOM or CDRUSCYBERCOM, AFSPC/CC, his/her delegated representative, or 24 AF/AFCYBER/CC may request applicable AF forces (e.g., Communications Focal Point (CFP) personnel within a Communications Squadron, etc.) be attached for tactical control to 24 AF/AFCYBER for the duration of the event. Due to the immediate nature of most cyber events, approval of the attachment will likely be

granted/transmitted verbally or electronically with hard copy orders to follow, per guidance in AFI 38-101, *Air Force Organization*.

1.3.3. All cyber orders must be complied with in the timeline directed. See section 2.2.2 for temporary relief from orders.

1.4. USSTRATCOM/USCYBERCOM issues orders via various formats that include but are not limited to Tasking Orders (TASKORDs) and Operation Orders (OPORDs). Orders received from USCYBERCOM will be relayed promptly, where applicable, through AFCYBER/CC or from his/her delegated representative to the 624 Operations Center (OC) to the tasked units. The 624 OC will relay USCYBERCOM orders to the appropriate units utilizing Cyber Tasking Orders (CTOs), Cyber Control Orders (CCOs), Time Compliance Network Orders (TCNOs), Maintenance Tasking Orders (MTOs), or Special Instructions (SPINS); hereafter referred to as cyber orders. AFCYBER/CC, through the 624 OC, may add AF-specific tasks to an OPORD; however, the original OPORD must remain intact.

1.4.1. Compliance with cyber orders is mandatory. Commanders shall ensure compliance with orders issued pursuant to this instruction and hold personnel and organizations accountable for the consequences of non-compliance **(T-2)**.

1.4.1.1. Military personnel and civilian employees may be subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk information and information systems by failure to comply with cyber orders issued by AFSPC/CC or his/her delegated representative.

1.4.1.2. Defense contractors are responsible for ensuring employees perform in accordance with the terms of the contracts and applicable directives, laws, and regulations. Violations by contractor personnel will be reported to contracting officers for disposition in accordance with the Federal Acquisition Regulation and applicable contract provisions. Future contracts shall include terms that alert contractors that noncompliance may serve as the basis for revoking access to the AFIN for individual violators, and that noncompliance will be a factor considered in contract performance evaluations **(T-2)**.

1.4.2. Prior to the implementation of this AFI, orders affecting the AFIN were a function of Air Force Network Operations (AFNETOPs). AFNETOPs orders issued prior to the issuance of this AFI remain valid, but orders issued after the date of this instruction will be issued by AFSPC/CC, his/her designated representative, or 24 AF/AFCYBER/CC.

1.5. Types of Orders.

1.5.1. AF CTO. AF CTOs are operational type orders issued to perform specific actions at specific time frames in support of AF and Joint requirements. AF CTOs are generally derived from USCYBERCOM orders and issued by AFCYBER via the 624 OC. AFSPC/CC or his/her delegated representative will issue AF CTOs directly (via 24 AF and the 624 OC) to direct the execution of cyberspace operations to protect and defend the AFIN.

1.5.2. AF CCO. CCOs are used to build/shape the portion of cyberspace to be employed in support of a Combatant Command (CCMD) operation or in response to adversary actions.

1.5.3. AF TCNO. TCNOs are orders issued to direct the immediate patching of information systems to mitigate or eliminate exploitation vulnerabilities. These orders have a significant implication if not accomplished in a timely manner.

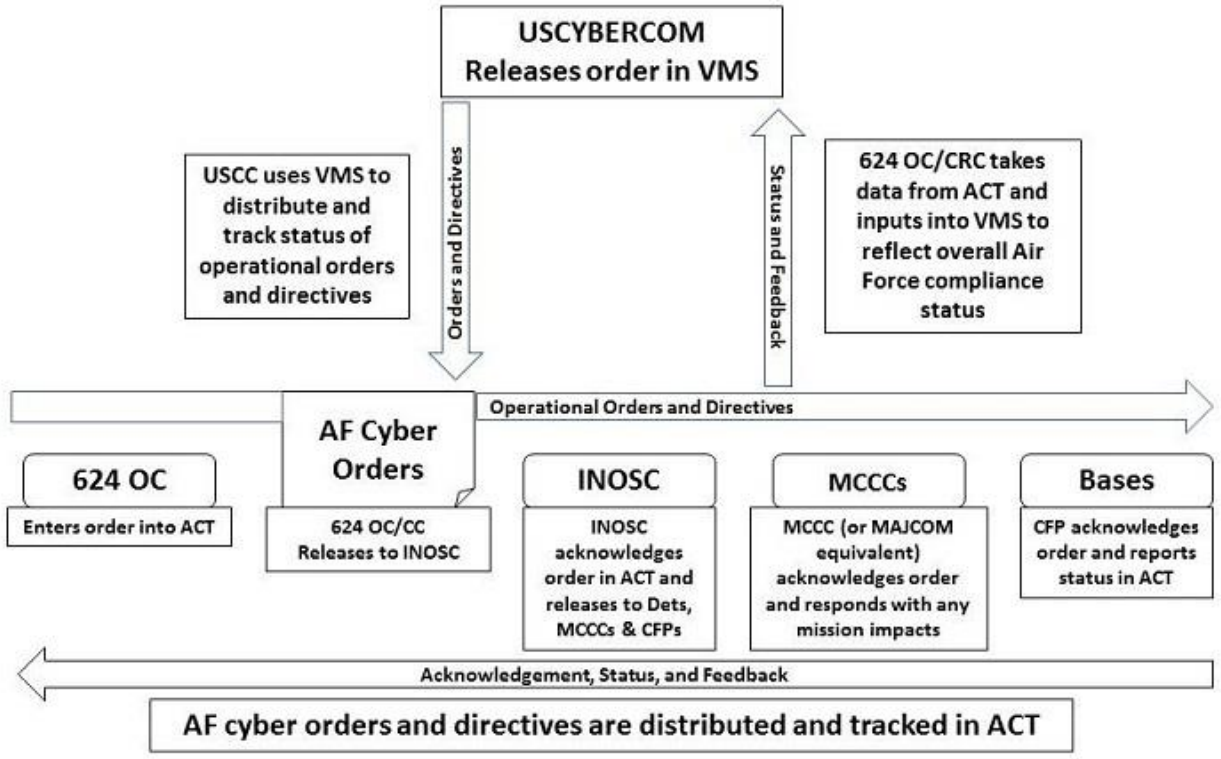
1.5.4. AF MTOs. MTOs are routine tasks that enhance network security with a medium to low risk associated with the task.

1.5.5. AF SPINS. SPINS provide amplifying instructions for planning, execution, and assessment of AF CTOs and CCOs.

1.5.6. C4 NOTAMs. Command, Control, Communications, and Computers Notices to Airmen (C4 NOTAMs) are used to disseminate network information that does not direct specific action to be taken or compliance to be tracked.

1.6. AF Cyber Orders Flow Process. Figure 1 graphically depicts the flow of cyber orders.

Figure 1. The AF Cyber Orders Flow Process



1.6.1. Cyber Orders Distribution. Applicable cyber orders are distributed by the 624 OC to major commands (MAJCOMs), field operating agencies (FOAs), direct reporting units (DRUs), MAJCOM Communications Coordination Centers (MCCCs), AF Component Commands and associated Air Operations Centers (AOCs) and AFFOR Communications Control Centers (ACCCs) for actions affecting assets (e.g., personnel, information systems, etc.) not under the direct control or ownership of 24 AF. For purposes of this Instruction, the term MCCC also includes organizational structures established at the discretion of a MAJCOM which perform the same functions as an MCCC.

1.7. Operational Reports (OPREP). All commanders are required to release OPREPS in accordance with AFI 10-206, *Operational Reporting*. Various cyber events/incidents, especially those impacting mission readiness/capability, will require an OPREP **(T-2)**.

2. Roles and Responsibilities.

2.1. Commander, Air Force Space Command (AFSPC/CC). In accordance with AFPD 10-17, AFSPC/CC is responsible for the overall command and control, security and defense of the AFIN. AFSPC/CC is responsible for the command, control, implementation, security, operation, maintenance, sustainment, configuration, and defense of the AFNET/AFNET-S. These day-to-day authorities may be delegated.

2.2. Commander, Twenty-Fourth Air Force (24 AF (AFCYBER)/CC). 24 AF is the Air Force component to USCYBERCOM. 24 AF/CC, when acting as AFCYBER/CC or when executing authorities delegated by AFSPC/CC, will:

2.2.1. Issue cyber orders as needed for the operation, defense, maintenance and control of the AFIN to Major Commands (MAJCOMs), wings, Integrated Network Operations and Support Centers (I-NOSCs), and CFPs via the 624 OC.

2.2.2. Within established criteria, approve or deny requests from affected organizations for relief from execution of cyber orders if such orders might degrade or impact any unit's ability to successfully complete assigned missions.

2.2.3. Represent AF equities to USCYBERCOM/USSTRATCOM when direction for operation and defense of the AFIN would degrade or impact any AF unit's ability to successfully complete assigned missions. 24 AF/CC (AFCYBER) will coordinate with USCYBERCOM/USSTRATCOM on behalf of affected organizations to resolve such issues.

2.2.4. Coordinate with affected AF organizations and CCDRs DoDIN Operations/defensive cyberspace operations (DCO) organizations to resolve conflicts between USCYBERCOM/USSTRATCOM or AF direction and CCDR direction for AFIN resources supporting CCDR missions.

2.2.5. Present forces to USCYBERCOM and other CCDRs as required in support of cyberspace operations as directed.

2.3. 624th Operations Center (624 OC). The 624 OC is the 24 AF/AFCYBER operations center responsible for issuing cyber orders as directed by 24 AF/AFCYBER/CC. The 624 OC will:

2.3.1. Manage an Air Force-wide tasking system for AF cyber orders as needed. As directed by AFSPC/CC, or if authority has been delegated, by 24 AF (AFCYBER)/CC, the 624 OC will relay USCYBERCOM orders as adopted AF cyber orders to all AF units **(T-2)**.

2.3.2. Relay Air Force and USCYBERCOM cyber orders to appropriate Air Force/AFCYBER units. 624 OC will generate applicable cyber orders to direct AF implementation; however, the original USCYBERCOM orders must remain intact. 624 OC acknowledges receipt of USCYBERCOM orders on behalf of AFCYBER **(T-2)**.

2.3.3. Oversee compliance with AF and USCYBERCOM cyber orders and relay status of those orders to 24 AF/AFCYBER/CC and USCYBERCOM as directed **(T-2)**.

2.3.4. Process requests for relief from AF cyber orders and advise the releasing authority on whether to grant, deny or seek further guidance/direction from USSTRATCOM/USCYBERCOM or AFSPC/CC. If such relief is granted, the 624 OC will immediately and concurrently notify affected organizations **(T-2)**.

2.4. 83rd Network Operations Squadron (NOS), 561st NOS, and 299th Network Operations Security Squadron (NOSS). NOSs receive and disseminate cyber orders from the 624 OC. The NOS unit structure contains the Integrated Network Operations Support Center (I-NOSC) and Enterprise Service Unit (ESU) flights/missions.

2.4.1. Relay, execute, and track cyber orders to affected MAJCOMs, MCCCs, ACCCs, and installation communications units. MAJCOMs, MCCCs and ACCCs pass applicable orders to their installation communications units at MAJCOM discretion or if not already received from the appropriate NOS **(T-2)**.

2.4.2. Coordinate with MAJCOMs, MCCCs, and ACCCs on operational impacts and Plans of Action and Milestones (POA&M) to mitigate risk to the AFIN when compliance with cyber orders cannot be achieved as directed **(T-2)**.

2.4.3. Advise MCCCs, ACCCs, and 624 OC on requests for relief. MCCCs/ACCCs will communicate with their subordinate installation communications units.

2.4.4. The 299 NOSS interfaces with the 624 OC and performs I-NOSC functions for the ANG. In addition to I-NOSC responsibilities the 299 NOSS also acts as the Enterprise Services Unit (ESU), Enterprise Service Desk (ESD) and MCCC for the ANG. 299 NOSS will continue to facilitate the integration of the ANG into the AFIN and work with ANG units to baseline and standardize their systems and equipment in accordance with AF/AFSPC/24 AF AFIN guidance. 299 NOS will:

2.4.4.1. Relay, execute and track cyber orders to ANG CFPs **(T-2)**.

2.4.4.2. Report status of compliance with orders to the 624 OC **(T-2)**.

2.4.4.3. Coordinate with ANG CFPs on operational impacts and POA&M to mitigate risk to the AFIN when relief of orders is granted **(T-2)**.

2.4.4.4. Advise ANG CFPs and the 624 OC on requests for relief **(T-2)**.

2.5. MAJCOMs, MCCCs, ACCCs, Wings, CFPs, and Program Management Offices (PMOs).

2.5.1. Organizational commanders will ensure cyber orders are disseminated to and executed by their subordinate units **(T-2)**. Commanders or their designated representatives may request relief from cyber orders due to operational impacts via 24 AF/AFCYBER-defined orders relief processes **(T-2)**. However, the request does not relieve commanders from implementing cyber orders when capable. Wing Commanders (or equivalent) will keep their respective MAJCOM, MCCCs and ACCCs informed of such requests for relief and expected operational impact if relief is not granted. Wing Commanders over tenant units with operational impact to unique mission systems will

request relief through the owning MAJCOM/organization, keeping host base CFP informed **(T-2)**.

2.5.2. MAJCOMs and wings will not normally relay cyber orders to subordinate CFPs. MCCCs and CFPs will receive these orders simultaneously via the 624 OC and supporting I-NOSC. This is only to prevent redundant tasking to the CFPs and does not preclude any commander in the CFPs chain of command from exercising their inherent command authorities. MCCCs will receive cyber orders from the 624 OC and the appropriate I-NOSC and may send them to their installation communications units if not already received from the appropriate NOS.

2.5.3. MAJCOM Communications Coordination Centers. MCCCs provide MAJCOM Commanders and the 624 OC with situational awareness of MAJCOM-unique functional system availability (if applicable) and of compliance with network taskings. In some cases, MCCCs maintain MAJCOM unique functional systems. MCCCs will:

2.5.3.1. Track, assign, and monitor cyber orders issued through the 624 OC and I-NOSCs.

2.5.3.2. Advise the MAJCOM CC on completion of cyber orders or inability to complete assigned tasks pertaining to AFNET, PMO, and MAJCOM-unique systems as required/directed by the MAJCOM/CC.

2.5.3.3. Provide updates on MAJCOM unique network health/status and operational impact to the 624 OC.

2.5.3.4. Advise MAJCOM/CCs, I-NOSC, and 624 OC, on operational impacts of cyber orders to component missions.

2.5.3.5. Coordinate conflicting guidance with I-NOSCs and CCDR DCO organizations.

2.5.3.6. Coordinate Plans of Action and Milestones (POA&M) with I-NOSCs and CCDR DoDIN Ops/DCO organizations to resolve operational impact issues when relief of orders is granted. Ensure POA&Ms are completed for any requests for relief and ensure POA&Ms remain updated and current until compliance with the orders is achieved.

2.5.3.7. Provide situational reports (SITREPS) to their CCDR, MAJCOM and 624 OC related to outage and other network events impacting the AFIN and/or the MAJCOM mission. This requirement does not replace any requirement for OPREP reporting outlined in AFI 10-206.

2.5.4. AFFOR Communications Control Centers. ACCCs support numbered Air Forces (NAF) in their AF and Service component responsibilities. ACCCs provide a similar capability as MCCCs and will:

2.5.4.1. Comply with cyber orders issued by the 624 OC and I-NOSCs.

2.5.4.2. Report completion of cyber orders or inability to complete assigned tasks to the I-NOSCs and 624 OC and their respective MCCC and wing.

2.5.4.3. Provide updates on component unique network activity, health/status, and operational impact to the 624 OC, if applicable.

2.5.4.4. Advise commanders, MCCCs, and 624 OC, on operational impacts of cyber orders to component missions.

2.5.4.5. Coordinate conflicting guidance with I-NOSCs and CCDR DoDIN Ops/DCO organizations.

2.5.4.6. Coordinate POA&Ms with I-NOSCs and CCDR DoDIN Ops/DCO organizations to resolve operational impact issues when relief of orders is granted. Ensure POA&Ms are completed for any requests for relief and ensure POA&Ms remain updated and current until compliance with the orders is achieved.

2.5.4.7. Provide SITREPs to their component and the 624 OC related to outage and other network events impacting the AFIN or the supported CCMD mission.

2.5.5. Communication Focal Points. The base CFPs monitor performance of the local network and serve as the conduit for implementing cyber orders. CFPs will:

2.5.5.1. Direct applicable personnel (e.g., Client System Support Technicians, Functional System Administrators, etc.) to implement cyber orders issued through the 624 OC and I-NOSCs or through the MAJCOMs (e.g. MCCC or similar structure). Provide compliance tracking for all orders that cannot be monitored or tracked electronically **(T-2)**.

2.5.5.2. Report completion of cyber orders or inability to complete assigned tasks that are not electronically visible to their respective wing and MCCC/ACCC. The MCCC/ACCC will report through the appropriate I-NOSC to the 624 OC **(T-2)**.

2.5.5.3. Provide local commanders with situational awareness of their ability to support all required mission areas at their fixed base or deployed location.

2.5.5.4. Coordinate with their parent wing and their respective MCCC/ACCC on operational impacts and POA&Ms to mitigate risk to the AFIN when relief of orders is granted. Ensure POA&Ms are completed for any requests for relief and ensure POA&Ms remain updated and current until compliance with the orders is achieved.

2.5.5.5. CFPs will provide support to tenant organizations of other Services in accordance with the provisions of the applicable Host-Tenant Support Agreement (T-2).

2.5.6. Program Management Offices (PMOs) or PMO-like entities. PMOs or PMO-like entities manage the acquisition and sustainment of information technology, including National Security Systems (NSS). PMO's engineer and deliver platform information technology, automated information systems (AIS), and outsourced information technology (IT). These deliveries may be systems and/or applications based on commercial-off-the-shelf or government-off-the-shelf systems, or a hybrid of each. PMOs ensure compliance with all relative directives and orders. Due to operational/contractual issues, additional testing/validation of software and security updates for PMO systems may be required to ensure engineering, interoperability, and mission functionality is not jeopardized. PMOs will:

2.5.6.1. Comply with cyber orders issued by 624 OC, via the parent MAJCOM/Wing, affecting program systems for which the PMO is responsible.

2.5.6.2. Request relief from cyber orders due to operational impacts, through the appropriate MAJCOM/MCCC to the 624 OC. Systems which cannot meet compliance within six months will be further evaluated for risk to the AFIN, impact to AF missions if quarantined or disconnected from the AFIN, and cost to implement the orders. Within established criteria, 24 AF/CC may accept the risk, require the PMO to implement additional risk mitigating actions and/or recommend to the AFSPC/CC, as the AF DAA, that the system be quarantined or disconnected from the AFIN. Recommendations for quarantine or disconnection due to unacceptable risk may result in a Denial of Authorization to Operate (DATO), per AFI 33-210, *Air Force C&A Process*.

2.5.6.3. Report status of compliance with orders to the appropriate wing, MCCC/ACCC, and to 624 OC.

2.5.6.4. Coordinate POA&Ms through the appropriate wing and/or MCCC/ACCC to the 624 OC on operational impacts and to mitigate risk to the AFIN if relief of orders is granted. Ensure POA&Ms are completed for any requests for relief and ensure POA&Ms remain updated and current until compliance with the orders is achieved. In any case, relief from orders will be governed by the provisions of paragraph 2.5.7.2 above.

2.5.6.5. Update program Technical Orders (TO) as required maintaining compliance with cyber orders. Issue Time Compliance Technical Orders (TCTOs) independent of cyber orders when needed to update TOs in the field pending formal TO change releases.

2.5.6.6. Provide SITREP to the MCCC/ACCC, wing and 624 OC related to outage and other network events impacting the AFIN and/or the MAJCOM mission.

3. Authorized Service Interruptions (ASI).

3.1. ASI Definition. ASIs are scheduled periods of network, equipment, or system downtime required to perform preventive maintenance actions, software or equipment upgrades or replacement, system reboots, etc. There are three defined types of ASIs.

3.1.1. Preventive Maintenance Inspection (PMI). PMI ASIs are required for any preventive maintenance actions accomplished on a recurring basis. Examples include routine maintenance of server equipment or server reboots required due to the application of TCTO/MTO-directed countermeasures.

3.1.2. Routine. Routine ASIs are required for any network system changes that will require an interruption of service to complete. Examples include service interruptions required to perform system/software upgrade, or to repair/replace faulty equipment.

3.1.3. Emergency. Emergency ASIs are for those ad hoc events which require an immediate service interruption to correct hazardous or degraded conditions where loss of human life or of Core Services (DCs, exchange, switches, routers) could occur through lack of immediate action. Examples of emergency outages include power problems, equipment malfunctions, imminent system failures, or any hazardous condition that requires immediate attention and cannot otherwise be scheduled as a routine service interruption.

3.2. Operational Reporting of Mission Impact. Organizations submit OPREPs related to outages IAW AFI 10-206.

3.3. ASI Approval Authority.

3.3.1. The AFSPC/CC or, when authority has been delegated, 24 AF/CC, is the approval authority for routine and emergency ASI requests associated with those AFIN links, nodes, functional systems, or services on the AFIN (1) directly supporting an active CCMD operation; (2) whose compromise or loss could affect national security; or (3) whose compromise or loss would degrade or disable critical C2 communications. The 624 OC is the focal point for the coordination of ASIs that must be approved by both the affected installation commander and the 24 AF/CC.

3.3.2. The installation commander is the approval authority for all PMI ASI requests that do not impact the AFNET/AFNET-S or meet the criteria specified in paragraph 3.3.1 **(T-2)**.

3.4. General ASI Coordination Guidance.

3.4.1. Service interruptions will be scheduled at a time that will have the minimum impact on operations **(T-2)**.

3.4.2. Requesting organizations must complete applicable local level coordination (e.g., major tenant unit commanders) on all ASIs prior to submitting the ASI request for approval.

4. Periods of Non-Disruption (PONDs).

4.1. PONDs are directed by USCYBERCOM to halt all maintenance actions within either a geographic or functional Area of Responsibility (AOR), or for very specific systems and or assets crossing one or more AORs. PONDS are intended to ensure commanders have full availability of critical C2 capabilities.

4.2. PONDs will only be issued to support real-world operations, crisis situations, and significant events that may negatively impact national security.

4.3. Requests for PONDs will be channeled through the ASI coordination chain to USCYBERCOM for final approval/disapproval.

BURTON M. FIELD, Lt Gen, USAF
DCS Operations, Plans & Requirements

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSI 3121.01B, *Standing Rules Of Engagement/Standing Rules For The Use Of Force For US Forces*, 13 June 2005 (Current as of 18 Jun 08)

CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, 9 February 2011

CJCSM 6510.01A, *Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)*, 24 Jun 09

CJCS Execute Order, *Title Classified*, 21 June 2013

DoDD O-8530.1-M, DoD *Computer Network Defense (CND) Service Provider Certification and Accreditation Process,* January 8, 2001

DoDD 3600.01, *Information Operations*, August14, 2006, with Change 1, 23 May 2011

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 November 2007

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

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

JP 1-02, *DoD Dictionary of Military and Associated Terms*, As Amended Through 15 May 2011

JP 3-12, *Cyberspace Operations (U)*, SECRET/REL USA, FVEY, 5 February 2013

AFDD 3-12, *Cyberspace Operations*, 15 July 2010, w/change 1, 30 November 2011

AFPD 10-17, *Cyberspace Operations*, 31 July 2012

AFI 10-206, *Operational Reporting*, 6 September 2011

AFI 10-701, *Operations Security,* 8 June 2011

AFI 10-710, *Information Operations Condition (INFOCON)*, 10 August 2006

AFI 33-150, *Management of Cyberspace Support Activities*, 30 November 2011

AFI 33-210, *Air Force C&A Process*, 28 Dec 2008

AFI 38-101, *Air Force Organization*, 16 Mar 11

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

TO 00-33A-1001, *General Communications Activities Management Procedures and Practice Requirements*, 1 December 2012

TO 00-33A-1109, *AF-GIG Vulnerability Management*, 9 January 2013

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

24 AF/CC—Commander, Twenty-Fourth Air Force

624 OC—624th Operations Center

ACCC—AFFOR Communications Control Centers

ACT—AFNETOPS Compliance Tracker

AFDD—Air Force Doctrine Document

AFFOR—Air Force Forces

AFI—Air Force Instruction

AFIN—Air Force Information Networks

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

ANG—Air National Guard

C2—Command and Control

C4 NOTAM—Command, Control, Communications, and Computer Notice to Airmen

CC—Commander

CCDR—Combatant Commander

CCO—Cyberspace Control Order

CCS—Command & Control Squadron

CDRUSCYBERCOM—Commander, United States Cyber Command

CDRUSSTRATCOM—Commander, United States Strategic Command

CFP—Communications Focal Point

CJCSI—Chairman, Joint Chiefs of Staff Instruction

C-MAJCOM—Component MAJCOM

C-NAF—Component NAF

CND—Computer Network Defense

CTO—Cyber Tasking Order

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDIN—Department of Defense Information Networks

DRU—Direct Reporting Unit

ESD—Enterprise Service Desk

ESU—Enterprise Services Unit

FOA—Field Operating Agency

I-NOSC—Integrated NOSC

IT—Information Technology

JFC—Joint Force Commander

JP—Joint Publication

MAJCOM—Major Command

MCCC—MAJCOM Communications Coordination Center

MTO—Maintenance Tasking Order

NAF—Numbered Air Force

NOS—Network Operations Squadron

NOSC—Network Operations & Security Center

NOSS—Network Operations and Security Squadron

OC—Operations Center

OPORD—Operation Order

OPR—Office of Primary Responsibility

PMO—Program Management Office

POA&M—Plan of Actions and Milestones

SPINS—Special Instructions

TCNO—Time Compliance Network Order

TCTO—Time Compliance Technical Order

TO—Technical Order

USCYBERCOM—United States Cyber Command

VMS—Vulnerability Management System

Terms

Air Force Forces (AFFOR)— United States Air Force component command assigned to a Joint Force Commander (JFC) at the unified, sub unified, and Joint Task Force (JTF) level. AFFOR includes the COMAFFOR-cyberspace operations, his/her staff, 624 OC, and all Air Force forces and personnel assigned to attach to that Joint Force's Air Force component.

Air Force Information Networks (AFIN)— The globally interconnected, end-to-end set of Air Force information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy-makers, and support personnel, including owned and leased communications and computing systems and services,

software (including applications), data, security services, other associated services, and national security systems.

Air Force Network (AFNET)— The Air Force's underlying Nonsecure Internet Protocol Router Network (NIPRnet) that enables Air Force operational capabilities and lines of business, consisting of physical medium and data transport services. Includes transmission mediums, gateways, routers, switches, hubs and firewalls, and the functions required to support and enable the environment such as command and control, management, maintenance, network authentication, and defense. (AFSPC Commander's Intent)

Air Force Network—Secure (AFNET-S) - The Air Force's underlying Secure Internet Protocol Router Network (SIPRnet) that enables Air Force operational capabilities and lines of business, consisting of physical medium and data transport services. Includes transmission mediums, gateways, routers, switches, hubs and firewalls, and the functions required to support and enable the environment such as command and control, management, maintenance, network authentication, and defense. (AFSPC Commander's Intent)

Commander, Air Force Forces (COMAFFOR)— Designated whenever US Air Force forces are presented to a joint commander. In any operation, a COMAFFOR is designated from the US Air Force and serves as the commander of US Air Force forces assigned and attached to the Joint Force Air Component. (AFDD 2).

Communications Focal Point (CFP)— The **c**onsolidation of help desk, telephone trouble tickets and Maintenance Operations Center. This function tracks all communications systems/equipment outages and resides with the Client Service Center (CSC) work center.

Computer Network Defense (CND)— Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks. (JP 6-0). This term is being replaced by Defensive Cyberspace Operations (DCO).

Cyber (adj.)— Of or pertaining to the cyberspace environment, capabilities, plans, or operations. (AFPD 10-17)

Cyber Tasking Order (CTO)— An operational type order issued to perform specific actions at specific time frames in support of AF and Joint requirements.

Cyber Orders— A general term used to refer to the various types of orders issued for network operations and maintenance (CTOs, CCOs, SPINS, MTOs, etc).

Cyberspace— A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02)

Cyberspace Control Order (CCO)— Used to build/shape the portion of cyberspace to be employed in support of a CCMD operation or in response to adversary actions.

Cyberspace Operations— The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. (AFPD 10-17)

Cyberspace Support— Foundational, continuous or responsive operations in order to ensure information integrity and availability in, through, or from Air Force-controlled infrastructure and its interconnected analog and digital portion of the battlespace. (AFDD 3-12)

Department of Defense Information Networks (DoDIN)— The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (Joint Pub 3-12)

Department of Defense Information Networks Operations (DoDIN Ops)— Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (Joint Pub 3-12)

Information Operations (IO)— The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO. (JP 1-02)

Maintenance Tasking Order (MTO)— Routine tasks that enhance network security with a medium to low risk associated with the task.

Operation Order (OPORD). A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. (JP 5— 0)

Special Instructions (SPINS)—. Provide amplifying instructions for planning, execution, and assessment of AF CTOs and CCOs.

Time Compliance Network Order (TCNO)— A downward-directed operations, security or configuration management-related order issued by USCYBERCOM in an Operational Order (OPORD). TCNOs do not replace information conditions (INFOCONs), Operational Event/Incident Reports (OPREPs), SITREPs or Time Compliance Technical Orders (TCTO). The TCNO provides a standardized mechanism to issue an order.