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