

1 JANUARY 2003



Operations

**DEFENSIVE COUNTER INFORMATION  
PLANNING, OPERATIONS AND ASSESSMENT****COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: 50 SCS/SCBI (Ms. Sheila Y. Wood)

Certified by: 50 SCS/CC (Lt Col Michael J. Clark)

Pages: 10

Distribution: F

---

This instruction implements Air Force Policy Directive (AFPD) 10-20, *Air Force Defensive Counterinformation (DCI) Operations*. It establishes Air Force guidance regarding the integrated planning, operation and assessment of DCI operations and supporting activities. It applies to all organizations assigned or attached to 50 SW, participating tenant organizations, all civilian personnel, and Air Force contractors (when included as part of the associated contract) who use, operate, or manage Air Force Automated Information Systems (AIS). **Attachment 1** lists references, acronyms and definitions used in this instruction.

According to AFDD 2-5, *Information Operations*, DCI includes those actions that protect information, information systems and information operations from any unauthorized source. AFDD 2-5 also states, "DCI is the Air Force's overall top priority within the information warfare arena." The principal DCI programs include information assurance (IA), operations security (OPSEC), counterdeception, counterintelligence, counterpropaganda and electronic protection (EP). In addition, numerous other activities such as acquisition, procurement, force protection and security programs support Air Force DCI operations. In order for DCI to be effective, close coordination among disparate communities and organizations that conduct or support the diverse set of disciplines and activities associated with DCI operations is required. AFPD 10-20, *Air Force Defensive Counterinformation Operations*, AFI 10-2001, *Defensive Counterinformation Planning, Operations and Assessment* and AFSPCI 10-201 require integrated DCI operations and integrated assessments of the Air Force's DCI capabilities. This guidance is used to provide the 50th Space Wing with a comprehensive, integrated DCI operational capability; this 50 SWI assigns organizational responsibilities for DCI programs, activities and assessments.

**1. Purpose.** This instruction gives the directive requirements for DCI disciplines as outlined in AFPD 10-20, *Air Force Defensive Counterinformation Operations*; AFI 10-2001, *Defensive Counterinformation Planning, Operations and Assessment*; and AFSPCI 10-201, *Defensive Counterinformation Operations*, which implements the Wing DCI Operations program. Compliance with this Instruction ensures a centralized and integrated DCI function and ultimately satisfies the policy directive (AFPD 10-20) to maintain a

transparent infosphere that must provide accurate, timely and secure information in any required form, at any time and place.

**2. Integration Activities.** The conduct of the 50 SW DCI operations requires coordination with all 50 SW units. All 50 SW units, including Geographically Separated Units (GSUs), will work closely to understand and address the linked challenges in protecting information, information systems, and 50 SW mission systems and sharing of best practices as addressed in AFD 10-20. Reporting of system changes, deficiencies, or degradations on a day-to-day basis will be coordinated through the 50th Space Wing Network Control Center (NCC) facilitating open communication and dialogue between ALL units and NCC Information Warfare (IW)/DCI lead, located in the NCC, who in turn will coordinate assessments with functional elements. (*Attachment 2, Flow Chart*)

**3. Structure.** DCI resides in the wing information operations office. This policy defines the roles and responsibilities of affected wing DCI members, which include Information Assurance, OPSEC Officer, AFOSI, Intelligence Flight, 50 SFS and Electronic Protection Officer.

#### **4. General Roles and Responsibilities**

4.1. The Wing Commander ensures the Wing Information Operations (IO) Officer is designated.

**4.2. The IO Officer is the 50th Maintenance Group Commander.**

4.2.1. The IO Officer is the wing representative responsible for day-to-day issues of DCI according to applicable directives. The IO Officer is functionally responsible to the wing commander, reviews all DCI issues and recommends actions to 50 SW/CC.

4.2.2. Support Agreements: The IO Officer acts as the Functional Area Agreement Coordinator (FAAC) and ensures 50 SW GSUs are afforded the IO support necessary to ensure DCI implementation.

4.2.3. Contracts: Each contract in support of 50 SW operations requires DCI government representation during the contract development and source selection process. The IO Officer is assigned as Office of Collateral Responsibility (OCR), and maintains cognizance and provides advice throughout the life of the contract.

4.2.4. The IO Officer ensures a dedicated DCI Program Manager is designated.

**4.3. Wing DCI Program Manager.**

4.3.1. The Wing DCI Program Manager is responsible for carrying out DCI functional responsibilities.

4.3.2. The DCI Program Manager will:

4.3.2.1. Conduct and document periodic meetings with all DCI Program element OPRs.

4.3.2.2. Be responsible for compiling the wing's annual DCI report and disseminating as required.

4.3.2.3. Review all DCI AF instructions, policies, and directives to ensure they are current and applicable.

4.3.2.4. Report directly to the IO Officer any issues or events as they arise during day-to-day

operations.

4.3.2.5. Ensure DCI representation at wing stand-up. The DCI Program Manager or one of the DCI element OPRs in attendance will satisfy this requirement.

4.3.2.6. Ensure DCI education, training, and awareness for 50 SW populous.

4.4. **DCI Program Element OPRs** are identified as IA, OPSEC, IN, OSI, SFS, EP, and NCC IW/DCI lead. In addition to each OPR being a member of the wing the threat working group (TWG), the following individual responsibilities are identified:

4.4.1. Wing/Base IA will perform annual IA assessments as required on behalf of the Wing Commander. OCONUS GSUs are scheduled biennially. The assessments will be used to compile the annual DCI status report in accordance with Attachment 6, AFI 10-2001.

4.4.2. OPSEC is an integrated section of DCI operations. It provides a means of detecting and controlling an adversary's actions on our military information functions and assists in protecting our DCI capabilities and intentions from adversary knowledge and attack. While OPSEC is not a security program, it should be coordinated with security disciplines (physical security and information assurance) to ensure that all aspects of sensitive activities are protected. Group/Unit OPSEC Monitors will serve as DCI points of contact. Parent organizations will ensure GSUs are incorporated into DCI activities.

4.4.2.1. 50 SW OPSEC Officer will maintain a list of groups/units DCI/OPSEC Monitors, and provide required training. In addition, he will disseminate education and awareness materials to unit DCI monitors and participate in web page review process.

4.4.3. 50 OSS/IN is an integral part of the Wing DCI program and shall provide the IO Officer and IA Office with timely, accurate, tailored intelligence on foreign threats to 50 SW and SAFB information and information systems.

4.4.3.1. 50 OSS/IN will review all suspected and confirmed information attacks on wing and base information and information systems to look for information of value to intelligence efforts, and will submit requests for intelligence information on those incidents that appear to be foreign or international in nature.

4.4.4. The AFOSI is the sole Air Force agency authorized to conduct counterintelligence activities and operations (Executive Order 12333 and AFD 71-1). For example, AFOSI prepares annual counterintelligence threat assessments (TA) to USAF personnel and resources for all areas with a significant USAF presence. TAs may be requested for any area. The annual TA for AFSPC units are revalidated at intervals during the year and will be expressly revalidated if requested by MAJCOM, or if world or local circumstances dictate. AFOSI is responsible for collecting, analyzing, disseminating intelligence and terrorist threat information, as well as conducting associated investigations. AFOSI is also responsible for conducting counterintelligence threat briefings to both specialized and general audiences. Serves as POC for antiterrorist threat. The AFOSI Detachment:

4.4.4.1. Manages the overall counterintelligence program/function for wing-level and below.

4.4.4.2. Coordinates with 14 AF and AFSPC for training, external agency sponsored surveys and wing-level issues.

4.4.4.3. Develops annexes or provides inputs for 14 AF and wing-level CONOPS when

required.

4.4.4.4. Develops and/or disseminates wing/unit level counterintelligence documentation as necessary.

4.4.5. 50 SFS is responsible for Personnel Security, Information Security, Law Enforcement, and Force Protection programs. 50 SFS participates in mission security area planning for all 50 SW missions and programs for security facilities, equipment and manpower. 50 SFS is responsible for physical security of Schriever AFB facilities to include protection of critical information systems in support of DCI. Also, the 50 SW Antiterrorism/Force Protection (AT/FP) NCO is lead for threat working group.

4.4.6. NCC Information Warfare/DCI Lead is the liaison between units and functional elements in assessing systems change in status and determining whether an event report should be generated. As such, this position shall:

4.4.6.1. Be responsible for knowing 50 SW mission “Systems” architecture (location, mission impact, alternate routing of systems, etc.).

4.4.6.2. Be responsible for knowing 50 SW information infrastructure vulnerabilities and how to guard against those vulnerabilities.

4.4.6.3. Attend appropriate training/seminars/conferences, as the IO Officer deems necessary in order to perform proficiently in required duties.

4.4.6.4. Work on a day-to-day basis with functional elements on implementing response to events.

4.4.6.5. Ensure checklists from each functional element are updated and maintained in the NCC.

4.4.6.6. Be responsible for “network defender” training in DCI.

4.4.6.7. Shadow any blue team/red team function to analyze response to events. Will implement any recommended action when appropriate.

4.4.6.8. Be responsible for assessment of events and reporting directly to the Wing DCI program manager/IO Officer for compiling data for DCI event report.

4.4.7. **Wing Electronic Protection Point of Contact (POC)** coordinates with 14 AF and HQ AFSPC for training, external agency sponsored surveys and wing-level issues. Develops annexes or provides inputs for 14 AF and wing-level CONOPS when required. Writes wing-level electronic protection documentation as required. Advocates electronic protection awareness throughout wing.

4.5. **Group/Unit Commanders** will ensure current group/unit DCI/OPSEC Monitor are appointed. Appointment letters will be addressed to wing OPSEC Officer. (*Attachment 3, Unit DCI Inspection List*)

4.6. **Group DCI/OPSEC Monitors** will be POC for the DCI Program Manager and act as liaison for all DCI disciplines and efforts for their respectable unit. Additionally, they are required to ensure DCI training materials are presented to units at least on an annual basis. The Wing OPSEC officer will provide the materials.

**5. DCI Assessment Reporting** . An integrated assessment program is required to provide 50 SW leadership the ability to evaluate and improve 50 SW DCI program capabilities and readiness. This integrated assessment system will provide the basis for an annual report assessing the overall health of the DCI mission area as required in AFPD 10-20.

5.1. All assessment reporting will follow the guidelines provided by AFI 10-2001 para. 3.4.1 thru 3.4.4.

5.2. DCI Event Reporting. DCI events include attempted or actual intrusions into 50 SW information systems and espionage—to include industrial espionage, spectrum interference incidents, detected adversarial psychological operations deception efforts, and physical attacks on the information infrastructure.

5.3. All event reporting will follow the guidelines provided by AFI 10-2001 para. 3.5 thru 3.5.4.

5.4. In addition to the guidelines stated above, the 50 SW functional elements will assess responsible areas, and submit findings to DCI program manager to compile annual report to be forwarded to 14 AF and AFSPC.

**6. DCI Training** requirements are as follows:

6.1. Wing DCI program OPRs will attend AF Information Warfare Applications Course at Maxwell AFB, AL.

6.2. DCI Program OPRs will assist DCI Program Manager in developing education & awareness material for wing populace.

**7. DCI Supporting Activities** . Many activities play important roles in supporting the conduct of DCI operations. While not directly identified as core DCI program OPRs, these activities must be integrated as part of the overall 50 SW program to ensure maximum DCI effectiveness. 50 SW specific DCI supporting activities are listed below:

50 CE – Civil Engineer (Base Infrastructure, HVAC, Electricity)

50 OG - Operational Reporting, Status of Resources and Training (SORTS), *Wing Operations Center*

XP - Acquisition and Procurement, Contracting, War Plans

JA - Legal

IG - Inspection Policy, Exercises

PA - Public Affairs

LARRY D. JAMES, Colonel, USAF  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****Abbreviations and Acronyms***

**AF**—Air Force  
**AFB**—Air Force Base  
**AFI**—Air Force Instruction  
**AFOSI**—Air Force Office of Special Investigations  
**AFPD**—Air Force Policy Directive  
**AFSPC**—Air Force Space Command  
**AFSPCI**—Air Force Space Command Instruction  
**AIA**—Air Intelligence Agency  
**AIS**—Automated Information Systems  
**AT/FP**—Antiterrorism/Force Protection  
**COMSEC**—Communications Security  
**CONOPS**—Concept of Operations  
**DCI**—Defense Counterinformation  
**EP**—Electronic Protection  
**GSU**—Geographically Separated Unit  
**HQ**—Head Quarters  
**IN**—Intelligence Flight (50 OSS/IN)  
**INFOCON**—Information Condition  
**IO**—Information Operations  
**IW**—Information Warfare  
**NCC**—Network Control Center  
**OCR**—Office of Collateral Responsibility  
**OPR**—Office of Primary Responsibility  
**OPSEC**—Operations Security  
**OSS**—Operations Service Squadron  
**POC**—Point of Contact  
**SF**—Security Forces  
**SW**—Space Wing  
**TA**—Threat Assessment

**TWG**—Threat Working Group

*Terms*

**Blue Team**—*See Scopenet*

**Counterdeception**—Efforts to negate, neutralize, and diminish the effects of, or gain advantage from, a foreign deception operation. Counter deception does not include the intelligence function of identifying foreign deception operations. (JP 1-02)

**Counterinformation**—Counterinformation seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force. (AFDD 1-2)

**Counterintelligence**—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

**Defensive Counterinformation**—Activities, which are conducted to protect and defend friendly information and information systems. Also called DCI. (AFDD 1-2)

**Electronic Protection**—That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. (JP 1-02)

**Electronic Warfare**—Any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack the enemy. (JP 1-02)

**Force Protection**—Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence and other security programs. See also combating terrorism; operations security; physical security; security; terrorism. (JP 1-02)

**Information**—1. Facts, data, or instructions in any medium or form. 2. That meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

**Information Assurance**—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (AFDD 2-5)

**Information Operations**—Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare and are conducted throughout all phases of an operation and across the range of military operations. (JP 1-02)

**Information Superiority**—That degree of dominance in the information domain, which permits the conduct of operations without effective opposition. See also **information operations. (Not IS)** (AFDD 2-5)

**Information System**—The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

**Information Warfare**—Information operations conducted during time of crisis or conflict to achieve or

promote specific objectives over a specific adversary or adversaries. Also called **IW**. See also **crisis; information; information operations; operation**. (JP 1-02)

**Infosphere**—Reference AAFP 33-2.

**Operations Security**—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called **OPSEC**. (JP 1-02)

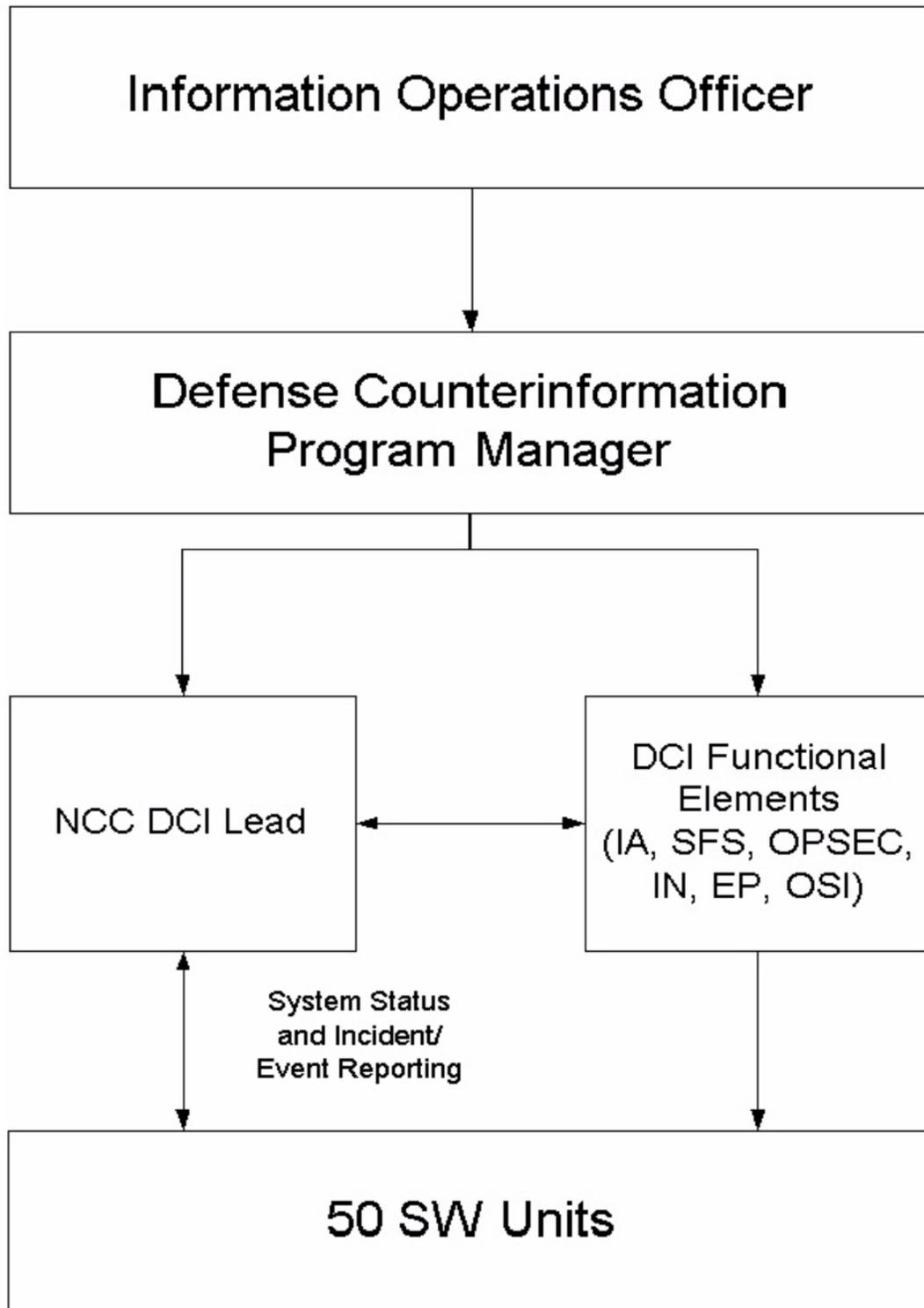
**Red Team**—Independent and threat-based (postulated and/or known) effort that is employed to improve the readiness and defensive capabilities of DoD components. IO Red Team is an interdisciplinary, simulated opposing force that utilizes active and passive, technical and non-technical capabilities on a formal, time-bounded tasking to expose and exploit IO vulnerabilities of friendly forces. (DOD 3600.4-M)

**Scopenet**—Ten, four-person teams from AFCA's global connectivity directorate that travels to more than 110 sites annually to tune networks for optimum performance. They also enhance network security; improve network operations management; train and mentor technical personnel; identify and share best practices; and as required, respond to emergency situations.

([http://www.af.mil/news/Mar2001/n20010314\\_0360.shtml](http://www.af.mil/news/Mar2001/n20010314_0360.shtml))

Attachment 2

FLOW CHART



Attachment 3

UNIT DEFENSIVE COUNTERINFORMATION INSPECTION CHECKLIST

<i>Unit Defensive Counterinformation Inspection Checklist</i>			
<b>Section I. Applies to all host and tenant organizations:</b>			
<b># - Identifies critical questions</b>	<b>Last Inspected:</b>	<b>C/L Date SEP 2002</b>	
<b><i>ADMINISTRATIVE</i></b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>
#1. Are unit personnel aware and trained on their responsibilities of Defensive Counterinformation (DCI)? (50 SWI 10-226, Para. 4.6.)			
#2. Has a unit DCI/OPSEC Monitor been designated in writing and a copy of the letter sent to wing OPSEC officer? (50 SWI 10-226, Para. 4.5.)			
3. Are users of Information Systems (IS) able to identify and report anomalies, intrusions, and incidents? (50 SWI 10-226, Para. 5.2.)			
4. Are Incident reporting procedures established? Do the procedures include notifying the 50 SW NCC? (50 SWI 10-226, Para. 2. & Attachment 2)			
5. Have means been incorporated to protect, detect and react to intrusions and probes to your information systems? (IS Certification & Accreditation Package/System Security Authorization Agreement)			
6. Have restoration capabilities been established for IS? (IS Certification & Accreditation Package/Security Authorization Agreement)			
7. Are all equipment needs, deficiencies, and shortfalls identified? (IS Certification & Accreditation Package/Security Authorization Agreement)			
8. Are implementation procedures for INFOCONS established, understood and applied correctly when determined appropriate? (AFSPC VAN MSG R051903Z)			