



**DEFENSIVE COUNTERINFORMATION  
PLANNING, OPERATIONS AND ASSESSMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://afpubs.hq.af.mil>.

---

OPR: HQ USAF/XOIW (Sharon McMahon)

Certified by: HQ USAF/XOI  
(Maj Gen Glen D. Shaffer)

Pages: 23

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 US Air Force major commands (MAJCOMs) to include the National Guard Bureau (NGB), field operating agencies (FOAs) and direct reporting units (DRUs). Command-level instructions or supplements will provide additional guidance. **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. 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 requires integrated DCI operations and integrated assessments of the Air Force’s DCI capabilities. To provide the Air Force with a comprehensive, integrated DCI operational capability, this AFI assigns organizational responsibilities for DCI programs, activities and assessments.

<b>Chapter 1—DCI PLANNING, OPERATIONS AND ASSESSMENT</b>	<b>3</b>
1.1. General. ....	3
1.2. DCI Planning. ....	3
1.3. DCI Operations. ....	3
Figure 1.1. Defensive Counterinformation (DCI) .....	4
1.4. DCI Assessment. ....	4

1.5. Integration Activities. ....	4
<b>Chapter 2—RESPONSIBILITIES</b>	<b>5</b>
2.1. Commanders. ....	5
2.2. Headquarters Air Force. ....	5
2.3. Air Intelligence Agency. ....	9
2.4. MAJCOMs and NGB. ....	9
2.5. Specific MAJCOMs ....	10
2.6. FOAs and DRUs. ....	11
2.7. Wing/Base Commanders ....	11
<b>Chapter 3—DCI ASSESSMENT AND EVENT REPORTING PROGRAMS</b>	<b>12</b>
3.1. An integrated assessment program is required to provide the AF leadership the ability to evaluate and improve DCI programs, capabilities and readiness. Additionally, 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. Event reporting will provide the Air Force operational, communications and information, intelligence and law enforcement communities with comprehensive, integrated DCI information and a means to identify trends and operating thresholds on a continuing and timely basis. The reporting requirement in this AFI is exempt from licensing in accordance with paragraph 2.11.1. of AFI 33-324, <i>The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Collections.</i> ....	12
3.2. Basic Assessment Responsibilities ....	12
3.3. Assessment Metrics ....	12
3.4. Assessment Reporting ....	13
3.5. Event Reporting ....	13
<b>Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>	<b>15</b>
<b>Attachment 2—APPLICABLE GUIDANCE FOR DCI PROGRAMS AND SUPPORTING ACTIVITIES</b>	<b>20</b>
<b>Attachment 3—INSPECTION GUIDANCE</b>	<b>21</b>
<b>Attachment 4—FORMAT FOR ANNUAL DEFENSIVE COUNTERINFORMATION (DCI) ASSESSMENT REPORT</b>	<b>22</b>

## Chapter 1

### DCI PLANNING, OPERATIONS AND ASSESSMENT

**1.1. General.** Information superiority is a core competency of the Air Force. According to AFDD 1-1, *Air Force Basic Doctrine*, Information Operations is the aerospace function that establishes information superiority. Increasing reliance on information and information systems to conduct air and space operations presents the Air Force with new opportunities as well as new vulnerabilities. Combined with counterair and counterspace operations, counterinformation operations create an environment where friendly forces conduct operations with requisite freedom of action while denying unauthorized persons the capability to interfere with or disrupt that freedom of action. Counterinformation, like counterair and counterspace, consists of both defensive and offensive aspects. DCI planning, operations and assessment will be conducted to ensure maximum integration with all other warfighting missions and activities conducted by the Air Force. The programs and activities associated with DCI involve a wide range of organizations throughout the Air Force. This AFI is not intended to duplicate or interfere with management of those functional programs or activities contributing to DCI operations. Rather, this AFI provides the necessary implementation guidance to provide comprehensive, integrated DCI planning, operations and assessment.

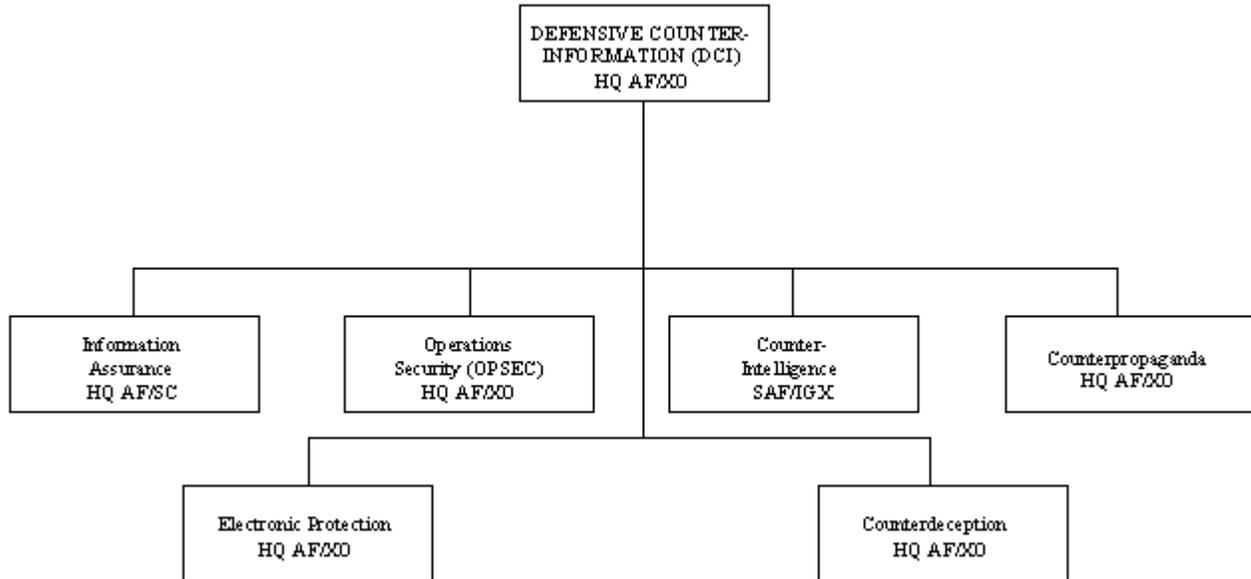
**1.2. DCI Planning.** Joint Publication 3-13, *Information Operations*, and AFD 10-20 require commanders to incorporate DCI operations throughout the spectrum of mission operations from peace to warfare. As part of the larger Air Force, Department of Defense, and national information infrastructures, commanders at all levels must protect their information, information infrastructures and information centers of gravity. DCI involvement should incorporate an operational risk management (ORM) process by which commanders assess and address risks posed to their information and associated infrastructures. In order to achieve these goals, commanders and planners must identify mission critical information and information systems, conduct vulnerability assessments on those systems, develop and implement plans to mitigate risk, include these activities in exercise planning and implementation, and include DCI considerations into the acquisition and procurement planning cycles

**1.3. DCI Operations.** The Air Force must organize, train and equip its forces to conduct DCI operations across the entire Air Force and at all organizational levels. Although DCI is an operational mission, it presents unique requirements as compared to traditional Air Force missions. Commanders rely on information to make decisions affecting operations both in crisis and in periods of relative peace. Therefore, the different organizations and functional areas conducting DCI must operate at all times. This means that functional areas, units and installations not normally associated with a warfighting mission now have a direct role in the conduct of operations. Furthermore, the reporting of events and the status of current resources available to conduct the mission, must be reported across the board and fused together to provide high-level decision-makers with an accurate picture of the Air Force enterprise. The Air Force will use existing mechanisms to assess readiness to include the Status of Resources and Training System (SORTS), exercises and inspection programs.

1.3.1. The ability of the Air Force to conduct DCI operations involves a wide range of programs and supporting activities. **Figure 1.1.** displays the DCI programs and associated OPRs. Definitions of each program are provided in **Attachment 1**. The Information Warfare Flights (IWFs) assigned to the aerospace operations centers are the CSAF-approved means for planning and integrating AF DCI capabilities for the warfighter. The functional OPRs for other core DCI disciplines provide AF DCI

capabilities to the warfighter as well. Specific policy and guidance for the conduct of activities associated with each program is listed in [Attachment 2](#).

**Figure 1.1. Defensive Counterinformation (DCI)**



1.3.2. The effective conduct of DCI operations also requires the integration of numerous supporting activities. The following activities have a significant influence on AF DCI operations: Force Protection, Antiterrorism, Industrial Security, Public Affairs, Contracting and Legal. Effective employment of Air Force DCI operations requires policy, guidance and ensuring that units associated with these supporting activities recognize their interrelationship with DCI processes.

**1.4. DCI Assessment.** A comprehensive report on the overall health of the DCI mission is submitted annually to AF/XO IAW AFPD 10-20. The DCI assessment report serves three purposes. First, it provides the Air Force leadership an ability to identify, understand and track DCI capabilities and readiness. Secondly, it serves as a guide to future investment and programming support for the overall DCI effort. Finally, it documents lessons learned and best practices throughout the Air Force and other organizations. [Chapter 3](#) of this AFI provides detailed guidance on the DCI assessment program.

**1.5. Integration Activities.** The conduct of DCI operations requires coordination with the legal community, AF/SC, AFOSI, the other services, the Joint Staff, the Office of the Secretary of Defense, and other US government organizations such as the National Infrastructure Protection Center. Additionally, the Air Force, in partnerships with the private sector, will work closely to understand and address the linked challenges in protecting information and information systems and sharing best practices as addressed in AFPD 10-20.

## Chapter 2

### RESPONSIBILITIES

**2.1. Commanders.** Commanders are responsible for DCI implementation, posture and operations within their commands, as addressed in AFDD 2-5 and AFPD 10-20. Additionally, they are responsible for enforcing DCI policies and directives. Commanders must:

2.1.1. Plan, prioritize and program DCI activities of their commands.

2.1.1.1. Ensure awareness of unit DCI activities of their commands. For example:

2.1.1.1.1. Information Assurance - Ensure systems (e.g., encryption, firewalls, anti-virus applications) and procedures (e.g., password management, COMSEC, INFOCON) are in place to guarantee availability, integrity, authenticity, confidentiality and nonrepudiation of information services.

2.1.1.1.2. OPSEC - Ensure OPSEC procedures (identification of critical information, scheduling and results of surveys/assessments, effectiveness of applied countermeasures) are implemented.

2.1.1.1.3. Electronic Protection - Ensure Electronic Protection safeguards (threat system detection capabilities, friendly system limitations and vulnerabilities, alternate countermeasures) are implemented.

2.1.1.2. Ensure operational and exercise planning includes identification and risk assessment of friendly information centers of gravity (COGs).

2.1.1.3. Integrate Operational Risk Management (ORM) to develop courses of action to mitigate vulnerabilities of these critical friendly information COGs. See AFI 90-901, *Operational Risk Management (ORM)*.

2.1.1.4. Periodically test an organization's ability to protect information COGs via the unit's exercise program.

2.1.2. Ensure DCI programs (especially information assurance, counterintelligence, and OPSEC) and supporting activities (such as physical security and critical infrastructure protection) provide AF units adequate protection and are conducted in an integrated fashion.

2.1.3. Ensure personnel receive sufficient training to support unit DCI responsibilities and missions.

2.1.4. Evaluate and report overall unit DCI readiness via SORTS system and provide inputs to other DCI assessments. For functional communities reporting via SORTS, these inputs will be leveraged to produce an overall DCI readiness assessment.

**2.2. Headquarters Air Force.** Headquarters Air Force will establish guidance and direction for DCI planning, operations and assessments. Additional guidance may be developed by Field Operating Agencies or designated lead commands.

2.2.1. AF/XO has overall responsibility for development and implementation of policy and guidance for DCI operations. AF/XO will:

2.2.1.1. Provide functional management for four of the six core DCI programs--OPSEC, counter-deception, counterpropaganda and electronic protection.

2.2.1.2. Ensure integration of DCI programs and activities into SORTS and Operational Report (OPREP) systems.

2.2.1.3. Ensure all AF organizations responsible for DCI programs and supporting activities are included in DCI operations.

2.2.1.4. Advocate MAJCOM DCI priorities during planning, programming and budgeting system (PPBS) deliberations.

2.2.1.5. Ensure total force DCI capabilities include appropriate programs and readiness across active duty, Air Force Reserve and Air National Guard (ANG) forces.

2.2.1.6. Ensure adequate interface with legal community, AF/SC, AFOSI and organizations external to the Air Force.

2.2.1.7. Manage implementation of AF responsibilities as directed by the Chairman, Joint Chiefs of Staff's DOD Information Operations Condition (INFOCON) system. Details of the implementation of the INFOCON system are addressed in draft AFI 10-2002, *Air Force Information Operations Condition (INFOCON) Implementation*.

2.2.1.8. Chair an annual DCI conference. Attendees should include Air Staff, MAJCOM and functional representatives. The conference agenda should clearly identify goals such as reviewing new policies and procedures, developing new tactics, discussing annual DCI assessment, etc.

2.2.1.9. Ensure Air Force career field managers and MAJCOM functional managers identify DCI training requirements as appropriate to the career fields.

2.2.1.10. Ensure DCI training efforts are properly resourced.

2.2.1.11. In coordination with SAF/AQ, AF/SC, AFRC and NGB, ensure procurement and modernization efforts include measures and technologies to protect networks and communications against intrusion, jamming, spoofing, deception, etc.

2.2.2. AF/SC has overall responsibility for Information Assurance. Information Assurance, a vital component of the Air Force's operational readiness, ensures continuous and dependable information services. Information Assurance depends on the continuous integration of personnel, operational and technical capabilities to guarantee availability, integrity, authenticity, confidentiality and nonrepudiation of information services, while providing the means to efficiently reconstitute these vital services following disruptions of any kind, whether from an attack, natural disaster, equipment failure, or operator error. In an assured infrastructure, warfighters can leverage the power of the Information Age. AF/SC will:

2.2.2.1. Provide functional management for the information assurance program.

2.2.2.2. Develop and implement policy and guidance for the operation of Air Force information systems. AF/SC optimizes the balance between information assurance and control of information flow by integrating architectures, strategies, resources, plans and operational procedures. Cooperative information assurance and other DCI activities are developed to best support the delivery of information services and overall warfighting.

2.2.2.2.1. The Network Operations and Security Center (NOSC) is the conduit between the Air Force Network Operations Center (AFNOC) and the Network Control Center. It provides commanders visibility into the network to achieve operational objectives. The NOSC exer-

cises command and control over its networks and mission systems. The NOSC performs MAJCOM enterprise management, helps achieve information assurance, and provides MAJCOM network visibility for timely situational awareness.

2.2.2.3. As the Air Force lead for critical infrastructure protection, coordinate identifying critical information processes and associated infrastructures.

2.2.2.4. SC or A-6, as appropriate, will advise the AF/XO or A-3 at each appropriate command level (AF, MAJCOM, AFFOR, NAF, or base) on associated impacts of INFOCON changes.

2.2.2.5. As the Air Force functional manager for information assurance and security awareness training and education, integrate programs into cooperative efforts across the DCI community to improve the overall availability of critical information across a spectrum of operations from day-to-day to warfighting.

2.2.2.6. Lead and advocate coordination and development of information infrastructure and associated information assurance programs within the PPBS.

2.2.3. SAF/IG, as the functional manager for counterintelligence, is accountable for the execution of these responsibilities through the Commander, Air Force Office of Special Investigations (AFOSI). As the functional manager, SAF/IG, at the Air Staff level will:

2.2.3.1. Advocate for resources for counterintelligence during the PPBS, through the SAF/IGX Program Element Monitor and the AF corporate process.

2.2.3.2. Inform senior leaders on significant counterintelligence investigations by the dissemination of "Items" and briefings.

2.2.3.3. Provide policy concerning counterintelligence.

2.2.3.4. AFOSI. The AFOSI will play a central role in embedding its counterintelligence capabilities into the AF DCI program. Specific responsibilities include:

2.2.3.4.1. Provide worldwide capability with the full range of counterintelligence services to include but not limited to the following: investigations, operations against foreign intelligence services, collections, analysis, threat assessments, HUMINT vulnerability assessments, studies, defensive briefings, support to technology protection, protective service operations, and liaison.

2.2.3.4.2. Identify specific roles and responsibilities for counterintelligence support.

2.2.3.4.3. Establish counterintelligence requirements of DCI and prioritize requirements to enhance CI RDT&E and procurement to correct overall CI program deficiencies.

2.2.3.4.4. Identify procedures to import counterintelligence threat considerations to the AF INFOCON system.

2.2.3.4.5. Support DCI annual program assessments and DCI event reporting.

2.2.3.4.6. Develop DCI inspection checklist for AFOSI/IG inspection programs.

2.2.3.4.7. Provide exercise support to AF commanders and planners to include counterintelligence red teaming capabilities.

2.2.3.4.8. Manage the DoD Computer Forensic Laboratory and DoD Computer Investigations Training Program to provide digital forensic analysis and trained computer crime investigators to support counterintelligence investigations and operations.

2.2.4. Other HQ Air Force Responsibilities. Designated organizations responsible for specific DCI programs and supporting activities will provide assistance to AF DCI planning, operations and assessment capabilities. Such organizations will participate in DCI policy and planning meetings, ensure coordination with AF/XO and develop new or changed guidance to enable comprehensive integration of DCI. Per AFPD 10-20, all AF policy directives pertaining to DCI operations will be reviewed IAW AFI 33-360 V1, *Publications Management Program*, by OPRs and, as necessary, updated or changed to reflect DCI considerations. Specific HQ Air Force organizations responsible for DCI-related activities include:

2.2.4.1. Core DCI Disciplines. In addition to the core programs identified as AF/XO and SC responsibilities, SAF/IGX is the functional manager for counterintelligence (AFOSI is the Field Operating Agency). Functional managers for core DCI programs will ensure the establishment and implementation of effective DCI operations. At a minimum, this will include:

2.2.4.1.1. Develop and implement an AFI outlining the core DCI program and organizational responsibilities.

2.2.4.1.2. Develop and implement metrics, analyses and support for MAJCOM IG activities required for DCI assessment.

2.2.4.1.3. Establish Air Force self-inspection checklists for applicable DCI activities.

2.2.4.1.4. Work with appropriate organizations and career field managers to establish requirements for ensuring awareness, training and education necessary to conduct applicable DCI operations.

2.2.4.1.5. Develop and implement, in close coordination with Air Intelligence Agency (AIA), procedures to enable fused DCI event reporting and analysis.

2.2.4.1.6. Develop and implement, in close coordination with AIA, procedures to enable a fused annual assessment of AF DCI operations.

2.2.4.2. DCI Supporting Activities. Many activities play important roles in supporting the conduct of DCI operations. While not directly identified as core DCI programs, these activities must be integrated as part of the overall AF program to ensure maximum DCI effectiveness. HQ USAF OPRs for specific DCI supporting activities are listed below:

SC/IL/XO - Critical Infrastructure Protection

XOF - Force Protection, Physical Security, Personnel Security, Industrial Security, Information Security, and Acquisition Security

XOI - Special Technical Operations

XOR - Operational Requirements

XOO – Operational Reporting, Readiness (SORTS) and Exercises

XOP - War Plans

AQ – Acquisition and Procurement, Contracting

GC and JA - Legal

IGI - Inspection Policy

PA - Public Affairs

AF/RE & NGB - Air Reserve Component Support

**2.3. Air Intelligence Agency.** Air Intelligence Agency, a primary subordinate unit of the Air Combat Command, will play a central role in the management of the AF DCI program. Specific responsibilities include:

2.3.1. Establish and implement the counterdeception and counterpropaganda programs as addressed in AFPD 10-20.

2.3.2. Conduct vulnerability assessments and provide exercise support to AF commanders and planners. This would include the Telecommunications Monitoring and Assessment Program (TMAP), presently conducted by Electronic Systems Security Assessment (ESSA). Additional details on the AF DCI vulnerability assessment activity will be provided in AFI 10-2004, *Air Force Defensive Counterinformation Red Team and Vulnerability Assessments*, currently under development.

2.3.3. Support Air Force and MAJCOM-level exercise programs through provision of ESSA and DCI red teaming capabilities. Additional detail on AIA's red teaming role in AF's DCI program will be provided in AFI 10-2004 currently under development.

2.3.4. Integrate reporting for event and annual DCI assessments as detailed in [Chapter 3](#).

2.3.5. Provide a center for fused DCI event reporting and analysis.

2.3.6. In conjunction with AFOSI, provide an annual overall Air Force DCI threat assessment including known DCI-related vulnerabilities and recommended countermeasures.

2.3.7. Provide training for IWFs, and other organizations as applicable, to integrate DCI operations.

**2.4. MAJCOMs and NGB.** MAJCOMs and NGB play a critical role in orchestrating DCI operations and are responsible for ensuring all supporting units establish a DCI program. Additionally, MAJCOMs and NGB will provide policy, oversight, implementing instructions, supplements and guidance as it applies to DCI. At a minimum, MAJCOM/NGB guidance must:

2.4.1. Identify roles and responsibilities for the six DCI programs at MAJCOM, NAF, unit and other levels to include tenant units. Additionally, identify roles and responsibilities at the centers such as the Space Warfare Center and the Aerospace Command and Control & Intelligence, Surveillance and Reconnaissance Center and gained AFRC/ANG units.

2.4.2. Develop roles and responsibilities for operational planning, exercises and supporting activities involving DCI.

2.4.3. Establish requirements for DCI capabilities and prioritize requirements to correct DCI R&D, procurement or program deficiencies.

2.4.4. Identify procedures to implement the Air Force INFOCON system and the DCI-related OPREP reporting.

2.4.5. Conduct DCI annual program assessments and DCI event reporting down to unit level. Perform DCI-specific assessments in conjunction with existing assessment activities (e.g. force protection, vulnerability assessments, information assurance assessment program, etc.).

2.4.6. Establish self-assessment checklists for core DCI programs and supporting activities as deemed applicable to the MAJCOM and NGB mission.

2.4.7. IAW AFI 90-201, Inspector General Activities, inspection programs will take an integrated approach to DCI operations as directed by AFPD 10-20. Areas of interest will include commander's involvement, the integration of DCI into plans and operating procedures, training, requirements documentation, and annual assessment. These programs will ensure assessment of DCI operations as part of compliance inspections per AFI 90-201. MAJCOMs and NGB will coordinate with their respective IG team to ensure DCI evaluation criteria are current and IAW any unique guidance from the commander.

2.4.8. With CINCs and other services, develop joint and combined tactics and plans for use of DCI capabilities.

2.4.9. Establish a single MAJCOM POC under Operations (DO equivalent) for its DCI program who will:

2.4.9.1. Integrate all activities related to DCI.

2.4.9.2. Develop DCI inspection checklists for MAJCOM and NGB IG inspection programs. A detailed inspection checklist is provided in [Attachment 3](#) as a guideline.

2.4.9.3. Interface with AF/XOI, AFOSI, AF/SC, MAJCOM/SC and AIA for reporting and assessments.

2.4.9.4. Interface with MAJCOM/SC and AIA for exercise support.

2.4.10. Participate in the annual AF DCI conference.

2.4.11. Ensure all DCI event reports are forwarded to AIA's DCI Fusion Center. Reporting details are provided in [Chapter 3](#).

## 2.5. Specific MAJCOMs

2.5.1. Air Combat Command, Air Force Space Command, Air Force Special Operations Command, Air Force Reserve Command, Pacific Air Forces and United States Air Forces in Europe will implement, as applicable, AIA's framework for developing and operationalizing the constructs of counter-deception and counterpropaganda as directed by AFPD 10-20.

2.5.2. Air Education and Training Command will, at the direction of the responsible career field functional manager (CFM) and upon completion of course resourcing, develop and incorporate DCI curriculum into existing or new courses which have been identified with DCI training/education requirements by the CFM. The program will:

2.5.2.1. Develop DCI training in selected officer and enlisted initial skills and supplemental training in response to stated requirements as identified and resourced by the responsible career field functional managers.

2.5.2.2. Develop new training courses relating to DCI from stated training requirements as determined, identified and resourced by the responsible career field functional managers.

2.5.2.3. Foster required knowledge of Air Force DCI programs and operations through professional military education when deemed appropriate.

**2.6. FOAs and DRUs.** At the base/installation level, FOAs and DRUs will comply with host MAJCOM and Wing guidance, as necessary. FOAs and DRUs are not required to develop independent DCI programs; however, they must fulfill their information assurance and OPSEC responsibilities. FOAs with specific DCI roles, particularly AIA and AFOSI, are addressed elsewhere in this AFI or in the appropriate DCI program or supporting activity guidance.

## **2.7. Wing/Base Commanders**

2.7.1. Issue implementing supplements and other guidance as required.

2.7.2. Identify procedures for implementing AF INFOCON system and DCI related OPREP reporting.

2.7.3. Establish procedures for ensuring awareness, training, and education necessary to conduct DCI operations.

2.7.4. Establish procedures for conducting Wing DCI program assessments and DCI event reporting.

2.7.5. Establish a single wing/base DCI POC under Operations (DO equivalent) for its DCI program who will:

2.7.5.1. Integrate all activities related to DCI.

2.7.5.2. Interface with respective MAJCOM for reporting and assessments.

2.7.6. ANG DCI philosophy, organization, policy development, information dissemination and unique issues will be centrally managed by the NGB. Additionally, NGB will work in concert with gaining MAJCOMs to ensure oversight procedures and established MAJCOM-specific requirements are integrated into ANG wing/unit DCI programs. All DCI reports and assessments will be forwarded to gaining MAJCOMs and NGB for review and analysis.

## Chapter 3

### DCI ASSESSMENT AND EVENT REPORTING PROGRAMS

**3.1.** An integrated assessment program is required to provide the AF leadership the ability to evaluate and improve DCI programs, capabilities and readiness. Additionally, 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. Event reporting will provide the Air Force operational, communications and information, intelligence and law enforcement communities with comprehensive, integrated DCI information and a means to identify trends and operating thresholds on a continuing and timely basis. The reporting requirement in this AFI is exempt from licensing in accordance with paragraph 2.11.1. of AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Collections*.

#### **3.2. Basic Assessment Responsibilities**

3.2.1. AF/XO will ensure integration and advocate programmatic activity related to DCI assessments.

3.2.2. AIA will serve as the agent for collecting and providing event and annual DCI assessment reports. AIA will establish a single focal point for the collection of relevant DCI assessment information.

3.2.3. Functional managers for all DCI programs and supporting activities will develop appropriate metrics for assessment and identify shortfalls in their program's capabilities. The functional managers will also provide their respective DCI core discipline annual assessment input to the annual DCI assessment. For example, AF/SC, vice the MAJCOMs/FOAs/DRUs, will submit the IA input for the annual DCI assessment.

3.2.3.1. As applicable, AIA should leverage existing DCI core discipline metrics.

3.2.4. MAJCOMs and ANG will collect data required by AF and MAJCOM-specific instructions and provide MAJCOM-wide assessments to AIA. ANG assessments will focus on data not already reported directly to the MAJCOMs. MAJCOMs and ANG are only required to report data specifically identified in AFIs as reportable under the DCI assessment program.

3.2.5. Tenant FOAs, DRUs and other organizations will provide reports and information as directed by host MAJCOMs.

3.2.6. AIA will develop and publish an annual assessment report for functional OPRs coordination and AF/XO approval. This report may be sensitive or classified and should be marked accordingly.

#### **3.3. Assessment Metrics**

3.3.1. AF/XO will develop an integrated DCI assessment system based on input from the functional OPRs for DCI core programs and supporting activities.

3.3.2. AIA will consolidate a comprehensive list of DCI metrics developed by functional OPRs NLT 1 Nov of each year for use in the upcoming year's annual assessment. For example, metrics published in Nov 2000 will be used for data collection throughout 2001 and reported in the Jan 2002 DCI Assessment.

3.3.3. Functional OPRs will develop and annually update appropriate metrics. The updated metrics will be provided to AF/XOI.

3.3.3.1. These metrics will be provided to AIA by 1 Sep.

3.3.3.2. For each metric, the functional OPR will define the activity being measured; identify an OPR for ensuring proper measurement; describe the system by which the metric is assessed; and provide details on how measurements will be passed to HQ AIA/DO.

3.3.3.3. AF/XOI and functional OPRs will provide guidance to MAJCOMs, ANG, FOAs, and DRUs through AFIs and other means, as necessary, to define their roles and responsibilities in conducting metrics. AF/XOIW will convene and chair a working group of Air Staff functional managers to ensure that guidance to the field is consistent in format and content.

3.3.4. MAJCOMs, ANG, FOAs, and DRUs will provide information on metrics as directed by functional OPRs.

### 3.4. Assessment Reporting

3.4.1. AIA will:

3.4.1.1. Establish and publish a list of required reports in coordination with the functional OPRs and update it annually. In addition, AF/XOI and AIA may request other specific reports be passed as part of the DCI assessment program.

3.4.1.2. In coordination with Air Staff, MAJCOMs, ANG, HQ AFOSI, and HQ AFCA, compile DCI annual reporting data.

3.4.1.3. Provide a draft of the annual Air Force DCI assessment to AF/XOI by 15 March each year.

3.4.1.4. Provide the final annual Air Force DCI assessment to AF/XO by 1 May each year.

3.4.2. Each functional OPR will identify reports relevant to DCI activities and ensure they are passed to AIA to conduct integrated DCI assessments.

3.4.3. MAJCOMs and ANG will provide an annual assessment to AIA as part of the annual AF DCI assessment by 31 Jan each year. DCI report format is provided in [Attachment 4](#).

3.4.4. The final annual AF DCI assessment report will be disseminated by AF/XO to the MAJCOMs, ANG, intelligence, communications and information, and law enforcement units and other DCI operational entities (i.e., AFCERT, IWFs, AFNOC, etc.).

### 3.5. Event Reporting

3.5.1. DCI events include attempted or actual intrusions into Air Force information systems, espionage (to include industrial espionage), spectrum interference incidents, suspected PSYOP or deception efforts, and physical attacks on the Air Force information infrastructure. This may also include TMAP-related events such as password disclosures or other events which may create a system vulnerability. DCI events can be identified as part of an in-house survey, IO Red Team or by any member of the unit that observes the activity during day-to-day operations. In some cases, these events will warrant being highlighted beyond the particular unit to enable damage control measures that can avoid potential exploitation by unauthorized persons and ensure future corrective measures are imple-

mented. Commanders will report events consistent with the guidance developed in accordance with section 3.2.3.3. of this AFI. The purpose of this reporting is to identify vulnerabilities and trends and to improve the service-wide DCI posture. Investigative information must be handled and communicated through existing channels IAW appropriate legal and OPSEC considerations.

3.5.2. MAJCOMs and ANG will forward event reports in a timely manner to AIA's DCI Fusion Center at [dcifuse@aia.af.mil](mailto:dcifuse@aia.af.mil) (NIPRNET) or [dcifuse@aiancc.aia.kelly.af.smil.mil](mailto:dcifuse@aiancc.aia.kelly.af.smil.mil) (SIPRNET). For those programs where reporting guidance already exists (information assurance, counterintelligence, OPSEC), follow normal reporting channels, adding AIA's DCI Fusion Center as an addressee (HQ AIA Kelly AFB TX//DCIFC//).

3.5.3. AIA will compile and analyze data on all DCI events and will provide fused reporting to AF command, intelligence, communications and information, and law enforcement channels and other DCI operational entities. Fused reports will be disseminated in a timely manner to ensure comprehensive DCI information is available to AF commanders on a continuous basis.

3.5.4. All DCI event collection and reporting is subject to Intelligence Oversight IAW DoD 5240.1R, Procedures Governing the Activities of DoD Intelligence Components that affect United States Persons.

ROBERT H. FOGLESONG, Lt General, USAF  
DCS/Air and Space Operations

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

AFPD 10-20, Air Force Defensive Counterinformation Operations

AFPD 10-24, AF Critical Infrastructure Protection

AFPD 33-2, Information Assurance

AFDD 1-1, Air Force Basic Doctrine

AFDD 2-5, Information Operations

AFI 10-201, Status of Resources and Training System

Draft AFI 10-2002, Air Force Information Operations Condition (INFOCON) Implementation

AFI 10-2004, Air Force Defensive Counterinformation Red Team and Vulnerability Assessments

AFI 33-115V1, Network Management

AFI 33-119, Electronic Mail (e-mail) Management and Use

AFI 33-129, Transmission of Information via the Internet

AFI 33-202, Computer Security

AFI 33-204, Information Protection Security, Awareness, Training and Education Program

AFI 33-205, Information Protection Metrics and Measurements Program

AFI 33-360V1, Publications Management Program

AFI 37-124, The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Collections.

AFI 71-101, V4, Counterintelligence

AFI 90-201, Inspector General Activities

AFI 90-901, Operational Risk Management Program

AFTTP 3-1, Air Force Tactics, Techniques and Procedures

CJCSI 6510.01B, Defensive Information Operations Implementation

CSCSI 6510.04, Information Assurance Readiness Metrics

DoD 3600.4-M, DoD Information Operations Red Teaming

DoD 5240.1R, Procedures Governing the Activities of DoD Intelligence Components that affect United States Persons

JP 1-02, DoD Dictionary of Military and Associated Terms

JP 3-13, Joint Doctrine for Information Operations

PDD-63, Critical Infrastructure Protection

*Abbreviations and Acronyms*

**AC2ISRC**—Aerospace Command and Control & Intelligence, Surveillance, and Reconnaissance Center

**AF**—Air Force

**AFCA**—Air Force Communications Agency

**AFCERT**—Air Force Computer Emergency Response Team

**AFDD**—Air Force Doctrine Document

**AFFOR**—Air Force forces

**AFI**—Air Force Instruction

**AFNOC**—Air Force Network Operations Center

**AFOSI**—Air Force Office of Special Investigations

**AFPD**—Air Force Policy Directive

**AFRC**—Air Force Reserve Command

**AFSSI**—Air Force System Security Instruction

**AIA**—Air Intelligence Agency

**ANG**—Air National Guard

**C4**—Command, Control, Communications and Computers

**CFM**—Career Field Functional Manager

**CINC**—Commander in Chief

**CIP**—Critical Infrastructure Protection

**COG**—Center of Gravity

**COMPUSEC**—Computer Security

**COMSEC**—Communications Security

**DCI**—Defensive Counterinformation

**DoD**—Department of Defense

**DoDD**—Department of Defense Directive

**DRU**—Direct Reporting Unit

**EMSEC**—Emissions Security

**ESSA**—Electronic Systems Security Assessment

**EW**—Electronic Warfare

**FOA**—Field Operating Agency

**HQ**—Headquarters

**IA**—Information Assurance

**IAW**—In Accordance With

**IG**—Inspector General

**INFOCON**—Information Condition

**IO**—Information Operations

**IW**—Information Warfare

**IWF**—Information Warfare Flight

**MAJCOM**—Major Command

**NAF**—Numbered Air Force

**NGB** —National Guard Bureau

**NIPRNET**—Non-Secure Internet Protocol Network

**NOSC**—Network Operations and Security Center

**OPR**—Office of Primary Responsibility

**OPREP**—Operational Report

**OPSEC**—Operations Security

**ORM**—Operational Risk Management

**PPBS**—Planning, Programming and Budgeting System

**POC**—Point of Contact

**PSYOPS**—Psychological Operations

**SAF**—Secretary of the Air Force

**SATE**—Security Awareness, Training and Education

**SCI**—Sensitive Compartmented Information

**SIPRNET**—Secret Internet Protocol Network

**SORTS**—Status of Resources and Training System

**SWC**—Space Warfare Center

**TMAP**—Telecommunications Monitoring and Assessment Program

### *Terms*

**Computer Security.**—The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02)

**Communications Security.**—The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (JP 1-02)

**Counterdeception.**—Efforts to negate, neutralize, and diminish the effects of, or gain advantage from, a

foreign deception operation. Counterdeception 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)

**Counterpropaganda.**—Efforts to negate, neutralize, diminish the effects of, or gain advantage from foreign psychological operations or propaganda efforts. (AFDD 2-5)

**Critical Information.**—Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (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)

**Emission Security.**—The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. (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 combatting 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 Condition.**—Comprehensive defense posture and response based on the status of information systems, military operations and intelligence assessments of adversary capabilities and intent. (CJCS Memo, 10 Mar 99)

**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)

**Offensive Counterinformation.**—Offensive IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems. (AFDD 2-5)

**Operational Risk Management.**—The systematic process of identifying hazards, assessing risks, analyzing risk control measures, making control decisions, implementing risk controls, and supervising and reviewing the process. Commanders accept the residual risks. (AFDD 1-2)

**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)

## Attachment 2

### APPLICABLE GUIDANCE FOR DCI PROGRAMS AND SUPPORTING ACTIVITIES

**A2.1. Air Force DCS/Air and Space Operations (HQ USAF/XO).** As the OPR for Counterdeception; Counterpsychological Operations; Electronic Protection and OPSEC, AF/XO plans and employs these programs IAW new and existing doctrine, policy, and instructions and advocates funding for their support. Air Intelligence Agency will provide a framework for developing and operationalizing the constructs of Counterdeception and Counterpropaganda. Electronic Protection will be conducted and managed as part of the existing Electronic Warfare program which includes electronic attack, electronic protection and electronic support activities. OPSEC is a well established program and should be implemented in all functional areas.

**A2.2. Office of the Inspector (SAF/IG).** SAF/IGX is the OPR for Counterintelligence. The Air Force Office of Special Investigations (AFOSI), as a field operating agency under the direction and guidance of SAF/IG, performs as a federal law enforcement agency with responsibility for conducting criminal investigations, counterintelligence activities, and specialized investigative and force protection support for the Air Force.

**A2.3. Air Force Director of Communications and Information (HQ USAF/SC).** As the AF OPR for Information Assurance; Communications Security (COMSEC); Emission Security (EMSEC); Computer Security (COMPUSEC); and Security Awareness, Training and Education (SATE) policies, executes Information Assurance and administers the COMSEC and COMPUSEC programs for AF non-Sensitive Compartmented Information (SCI) command, control, communications and computer (C4) systems. HQ USAF/SC will also advocate funding to support these Information Assurance program components.

**Attachment 3****INSPECTION GUIDANCE**

**A3.1.** Inspectors, staff assistance visit team members, and units can follow this checklist when assessing DCI operations.

**A3.2.** Has a DCI program manager been appointed? (AFI 10-2001, para [2.4.9.](#))

**A3.3.** Are they from the Operations element? (AFI 10-2001, para [2.4.9.](#))

**A3.4.** Do they interface with HHQs and subordinate unit program managers?  
(AFI 10-2001, [2.4.9.3.](#))

**A3.5.** Have roles and responsibilities for the six DCI programs been identified. (AFI 10-2001, para [2.4.1.](#))

**A3.6.** Have roles and responsibilities been developed for operational planning, exercises and supporting activities involving DCI. (AFI 10-2001, Para [2.4.2.](#))

**A3.7.** Are self-assessment checklists established for core DCI programs and supporting activities as deemed applicable to the unit mission? (AFI 10-2001, [2.4.6.](#))

**A3.8.** Are unit DCI assessments conducted and forwarded to HHQs for inclusion in the annual Air Force DCI assessment? (AFI 10-2001, para 3.1.4.)

**A3.9.** Are DCI events documented and reported to AIA's DCI Fusion Center? (AFI 20-2001, para [3.4.2.](#))

**A3.10.** Have procedures been identified to implement the Air Force INFOCON system and the DCI-related OPREP reporting? (AFI 10-2001, para [2.4.4.](#))

**Attachment 4****FORMAT FOR ANNUAL DEFENSIVE COUNTERINFORMATION (DCI)  
ASSESSMENT REPORT**

**Section I.** Mission Integration Efforts

**Section II.** Specific areas

**Section III.** Information Assurance

**Subsection A.** Organization

**Subsection B.** Training

**Subsection C.** Equipment

**Subsection D.** Planning/Execution

**Section IV.** Operations Security

**Subsection A.** Organization

**Subsection B.** Training

**Subsection C.** Equipment

**Subsection D.** Planning/Execution

**Section V.** Counterintelligence

**Subsection A.** Organization

**Subsection B.** Training

**Subsection C.** Equipment

**Subsection D.** Planning/Execution

**Section VI.** Electronic Protection

**Subsection A.** Organization

**Subsection B.** Training

**Subsection C.** Equipment

**Subsection D.** Planning/Execution

**Section VII. Counterpropaganda**

**Subsection A. Organization**

**Subsection B. Training**

**Subsection C. Equipment**

**Subsection D. Planning/Execution**

**Section VII. Counterdeception**

**Subsection A. Organization**

**Subsection B. Training**

**Subsection C. Equipment**

**Subsection D. Planning/Execution**

**Section VIII. Overall DCI Assessment**