BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-2005

14 AUGUST 2002

Operations

DEFENSIVE COUNTERINFORMATION SECURITY CLASSIFICATION GUIDE

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: HQ USAF/XOIW (Sharon McMahon)

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

Pages: 11
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 10-20, *Air Force Defensive Counterinformation Operations*. This guide establishes security procedures, guidelines and administrative controls to protect information related to defensive counterinformation (DCI) policies, programs, capabilities, assessments and activities and serves as classification guidance for exercises and operations relating to DCI. It will be used as a classification/declassification guide to Air Force programs related to DCI. Information noted as classified by this guide could be expected to cause damage or serious damage to national security if disclosed without authorization. The Original Classification Authority (OCA) shall identify or describe the nature of such damage.

1. POLICY.

1.1. This guide establishes security classification of information involved in Air Force DCI activities. While many of the general concepts involved in DCI may be unclassified, the compilation of information may result in products that should be classified (see EO 12958). Information on specific capabilities of the six DCI programs (information assurance, operations security (OPSEC), counterintelligence, counterdeception, counterpropaganda operations and electronic protection) may need to be classified, and separately published classification guidance may be developed to cover these. When conflicts between this guidance and any future guidance associated with specific programs occur, the OCA shall promptly be notified to adjudicate any differences. Until resolved, the more restrictive guidance shall be followed.

1.2. If implementing any of the requirements contained in this guide creates practical problems, requests for exception or recommendations for changes to this security classification guidance may be made through appropriate channels to the office of primary responsibility (OPR). Any such requests must be accompanied by a rationale delineating the reason an exception or change is necessary.

1.3. The classification authority for DCI will be retained by the Director of Intelligence, Surveillance and Reconnaissance. Users shall adhere to the guidance provided in this guide and shall cite authority derived from this guide when classifications and markings are applied. This guide should be listed on your office file plan and maintained IAW AFMAN 37-139, Table 31-4, R24 (original at issuing activity) and Table 31-4, R25 (copy at using activity).

2. RESPONSIBILITIES.

2.1. The Director of Intelligence, Surveillance and Reconnaissance (HQ USAF/XOI) will:

2.1.1. Provide DCI security guidance and oversee and monitor compliance with this guide.

2.1.2. Function as the OCA for Air Force DCI as identified in this security classification guide.

2.1.3. Function as the OPR for the maintenance and modification of this guide. All inquiries concerning content and interpretation of this guide shall be made to the Deputy for Information Warfare (HQ USAF/XOIW) within the Directorate of Intelligence, Surveillance and Reconnaissance.

2.2. The Heads of the other Air Force organizations shall ensure compliance with this guide when involved in Air Force DCI.

3. PROCEDURES.

3.1. DCI impacts many functional areas within its multi-discipline mission area. DCI capabilities include those actions that protect information, information systems, and information operations from any potential adversary. In addition to the six programs, DCI includes supporting activities such as acquisition, procurement, force protection, and security programs as outlined in AFPD 10-20.

3.2. The determination to classify DCI information is based on the potential damage to national security in the areas of military plans, weapon systems, operations and intelligence. The existence of AF DCI, the broad concepts and general discussions associated with information operations, and the fact that the Air Force is involved in DCI are unclassified. The fact that conducting DCI in the Air Force requires the leveraging of functions, processes and systems, such as the effective design, integration, and interaction among the Information Assurance, Intelligence, and Counterintelligence communities is unclassified.

3.3. The fact that the Air Force is developing policies, capabilities, and programs to cover the use of DCI, the six programs and associated activities is unclassified. Classification of specific capabilities or targets, if not covered in this document, is addressed under the individual component program, system, or operations planning security classification guides.

3.4. In certain circumstances, the compilation of unclassified or open source information may result in a sensitive or classified product. This can happen when the compilation reveals specific Air Force's interest, employment of DCI tools, techniques, methodologies, or vulnerabilities. Compilations should be reviewed for marking or classification under the guidance in this document and related documents. Any questions concerning the final classification of compiled information shall be referred to the OCA for final determination.

3.5. Event reports and assessments covering a single DCI discipline or supporting activity will be classified by the OCA if the subject matter is not covered in this document.

3.6. Release of Information: Release or disclosure of information classified per this guide to U.S. government agencies and contractors, foreign governments or the public follow para 6.6. of DoD Instruction S-3600.2, *Information Operations (IO) Security Classification Guidance*. For public release, further review and processing is required IAW DoD Regulation 5400.7/AF Supplement, *DoD Freedom of Information Act Program*. Contact your Freedom of Information Act Office at the MAJCOM/FOA/Base.

3.7. Reproduction, Extraction and Dissemination: Authorized recipients of this guide may reproduce, extract and disseminate the contents of this guide, as necessary, for application by specified groups involved in DCI, including industrial activities. Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR.

CHARLES F. WALD, 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

AFMAN 37-139, Records Disposition Schedule

DoD Directive S-3600.2, Information Operations (IO) Security Classification Guidance

DoD 5200.1-H, Department of Defense Handbook for Writing Security Classification Guidance

DoD 5400.7-R/AF Supplement, DoD Freedom of Information Act Program

Executive Order 12958, Classification of National Security Information

Abbreviations and Acronyms

DCI—Defensive Counterinformation

DoD—Department of Defense

EO—Executive Order

FOA—Field Operating Agency

IAW—In Accordance With

IO—Information Operations

MAJCOM—Major Command

OCA—Original Classification Authority

OPR—Office of Primary Responsibility

OPSEC—Operations Security

Terms

Computer Network Defense—Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Also called CND. See also computer network attack. (JP 1-02)

Counterdeception—Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. See also deception. (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. Also called

CI. See also counterespionage; countersabotage; countersubversion; security; security intelligence. (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)

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

Electronic Protection—See Electronic Warfare.

Electronic Warfare—Any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving passive and active means 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. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. See also directed energy; electromagnetic spectrum. (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. Also called IA. See also information; information operations; information system. (JP 1-02)

Information Operations—Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. See also defensive

information operations; information; information system; offensive information operations; operation. (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.
(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 informaiton environment by denying, degrading, disrupting, destroying, and deceiving the adversary'' information and information systems. (AFDD 2-5)

Operations Security (OPSEC)—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. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (AFDD 2-5)

Attachment 2

CLASSIFICATION SPECIFICATIONS

A2.1. The classifications listed in **Figure A2.1.** through **Figure A2.5.** are the security classification levels deemed appropriate by the OCA. Column 2 provides the marking or classification specification for those items listed in column 1. Columns 3 and 4 provide the reason for classification and the declassification specification in accordance with EO 12958. When a product results from the compilation of information which when reviewing the individual information items may be unclassified based on criteria in a particular specification paragraph below, a review shall be conducted on the compiled product to determine if it meets the criteria for marking or classification in subsequent specification paragraphs.

Figure A2.1. Organization and Administration.

TOPIC	CLASS	REASON	DECL
1. That the Air Force or subordinate organizations have a DCI mission if no details are given.	U		
2. Identification of DCI support units or unit support to DCI, provided the information does not reveal mission details.	U		
3. Operational structure of a DCI organization or unit.	U		
4. If operational structure reveals mission details.	C	1.5.(a), (c)	X1, X4
5. Identity of DCI analysts.	U		
6. Funding for program, total financial plan, or program cost.	U		
7. Peacetime location of units.	U		
8. Wartime or deployed location of units.	C	1.5.(a), (c)	X1, X4
9. Acknowledgment that new capabilities are continually being developed.	U		
10. Generic nonspecific analysis techniques such as multi-source intelligence, search of open source databases, etc.	U		
11. Actual analysis techniques whose effectiveness is not influenced by adversary knowledge of them.	C	1.5.(c)	X1
12. Actual tactics, techniques and procedures which, if known, would aid an adversary in the detection of DCI efforts or facilitate development of countermeasures.	S/NF	1.5.(a), (c)	X1, X4
13. Actual tactics, techniques and procedures whose disclosure might reveal intelligence sources or collection capabilities.	S/NF or higher	1.5.(c) Derivatively classify according to sources and capabilities	X1

Figure A2.2. Operational and Employment Concepts.

TOPIC	CLASS	REASON	DECL
1. Information revealing the existence of general DCI policy, doctrine, tactics, material, techniques, and training program.	U		
2. Specific DCI capabilities.	C	1.5.(a), (c), (g)	X1, X4
3. Specific DCI capabilities that reveal shortfalls and vulnerabilities.	S/NF or higher	1.5.(a), (c), (g) Derivatively classify according to source and sensitivity of information	X1, X4
4. Information revealing there is a policy of employing DCI to support operational planning and combat operations.	C	1.5.(a), (c)	X1, X4
5. General information concerning the planning and conduct of DCI operations and exercises.	C	1.5.(a), (c)	X1, X4
6. Actions indicating planning of DCI are in progress to support a specific OPLAN/CONPLAN	C	1.5.(a), (c)	X1, X4
7. Information that matches specific DCI analysis efforts to specific geographical areas.	S	1.5.(c)	X1, X4
8. The association of specific personnel and organizations with developing DCI for a particular OPLAN.	C	1.5.(a), (c)	X1, X4
9. General DCI options available to a combat commander during hostilities.	U		
10. Specific DCI information identified with the specific OPLAN.	S or higher	1.5.(a), (c) Derivatively classify according to specific OPLANs	X1, X4
11. Objectives, concepts, plans for specific or actual use of DCI to support defense of forces or planning of combat forces.	S	1.5.(a), (c)	X1, X4
12. Specific DCI options available to a combat commander during hostilities or information revealing specific types of DCI skills and practices.	S	1.5.(a), (c)	X1, X4
13. After-action reports on DCI operations.	U to S/NF	1.5.(a), (c) Derivatively classify according to detail/ actual content	X1, X4

Figure A2.3. System Capabilities and Vulnerabilities.

TOPIC	CLASS	REASON	DECL
1. General categories of equipment used in database activities (e.g., servers and workstations).	U		
2. Inventory listing of one or more systems with details, such as model numbers, locations, serial numbers, etc.	U	1.5.(c), (g) Derivatively classify if it shows specific connectivity or capability	X1
3. Specific functions of particular DCI system or equipment other than standard commercial capabilities.	C	1.5.(e), (g)	X1, X3
4. Capability assessment of DCI systems which use the database (or portions) to detect, identify, locate or counter specific targets.	S	1.5.(c), (g)	X1
5. Capabilities, or limitations of the database to provide DCI options to battlefield commanders against specific threat systems.	S	1.5.(c), (g)	X1
6. Actual tactics or techniques which, if known, would aid an adversary in the detection of DCI efforts or facilitate development of countermeasures.	S	1.5.(c), (g)	X1
7. Capabilities which reveal limitations of the program.	S	1.5.(c), (g)	X1
8. Specific program performance information which individually or collectively would indicate capabilities or limitations.	S	1.5.(c), (g)	X1
9. Information revealing specific Air Force DCI vulnerabilities and the compiled results of vulnerability analyses for classified systems.	S or higher	1.5.(c), (g) Derivatively classify according to individual components of analyses	X1
10. Information, correspondence, and documents that reveal the operational effectiveness of a database or other information sources.	S	1.5.(c), (e)	X1, X3
11. Estimates of adversary capability to conduct denial and deception of US intelligence systems.	C or higher	1.5.(c) Derivatively classify this information using intelligence sources and specific blue force vulnerability being evaluated.	X1

TOPIC	CLASS	REASON	DECL
12. Estimates of target intelligence capability.	C or higher	1.5.(c) Derivatively classify this information using intelligence sources and specific blue force vulnerability being evaluated.	X1

Figure A2.4. Exercise Objectives and Results.

TOPIC	CLASS	REASON	DECL
1. The fact that DCI testing and training are conducted.	U		
2. Details on exercise planning for DCI.	S or higher	1.5.(a) Derivatively classify this information according to content and details	X4
3. Training deployment plans for DCI units, personnel, or supplies that may indicate real world planning.	S	1.5.(a)	X4
4. Any results of the operational effectiveness of a database or other information sources exercise.	S or higher	1.5.(a), (e) Derivatively classify this information when operational deficiencies are identified	X1, X3
5. After-action reports on DCI exercises.	U to S/NF	1.5.(a), (c) Derivatively classify according to level of detail/actual content	X1, X4

Figure A2.5. Data and Production.

TOPIC	CLASS	REASON	DECL
1. Individual data elements when standing alone.	U to S/NF	1.5.(b), (c) Derivatively classify according to source material	X1, X5
2. Fused data elements.	U to S/NF	1.5.(b), (c) Derivatively classify by evaluating overall combined content against criteria in this guide	X1, X5
3. Data depicting vulnerabilities of foreign systems or identification of any specific enemy DCI vulnerability which would provide benefit if jammed, exploited, or attacked.	S/NF or higher	1.5. (b), (c) Derivatively classify according to NSA/ CSSM 123-3.	X1, X3, X4, X6
4. MAJCOM annual DCI assessment reports.	U to S/NF	1.5.(a), (c) Derivatively classify based upon the security classification level of the source material	X1, X4
5. AIA annual DCI assessment reports.	U to S/NF	1.5.(a), (c) Derivatively classify this information based upon the security classification level of the source material	X1, X4