BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 10-20

1 OCTOBER 1998

Operations

AIR FORCE DEFENSIVE COUNTERINFORMATION OPERATIONS

OPR: HQ USAF/XOIWD (Lt Col John W. Levy)

Certified by: HQ USAF/XO
(Lt Gen Marvin Esmond)
Pages: 9
Distribution: F

This policy directive provides guidance for planning and conducting defensive counterinformation (DCI) operations, the aerospace function through which the Air Force employs its defensive Information Operations (IO) capabilities. This policy applies to all military and civilian Air Force personnel, members of the Air Force Reserve, Air National Guard, DoD contractors, and individuals or activities under legal agreement or obligation with the Department of the Air Force.

The success of aerospace operations depends on the Air Force's ability to access reliable information, effectively utilize information systems, and perform information functions despite adversarial attempts to exploit or deny those capabilities. The Air Force will employ comprehensive, integrated defensive counterinformation (DCI) operations to protect and defend Air Force information and information systems. DCI is a multi-discipline mission area impacting many functional areas. Air Force DCI capabilities include information assurance, operations security (OPSEC), counterintelligence, counter-deception, counterpsychological operations, and electronic protection. Effective DCI requires the full integration of numerous supporting activities to include intelligence and IO-related law enforcement efforts, as well as physical, personnel, industrial, and information security (e.g., document classification and control) measures. The Air Force will integrate DCI awareness, objectives and capabilities into strategy, plans, operations, acquisition and procurement, exercises, inspections, training, communications and computer architectures, systems development, and professional education. AFPD 10-20 is not intended to duplicate or interfere with the management of those functional aspects of DCI that are already working well; rather, it provides the policy basis for an overarching, integrated DCI program for the Air Force.

1. The identification and protection of sensitive and classified information (see appendix for definitions) is required by public law, Executive Order, and regulation. OPSEC analysis leads to the identification of additional critical information and operational indicators which may be of value to an adversary. Protecting sensitive and classified information, as well as critical information/indicators derived via the OPSEC process is an inherent responsibility of command. Compliance with all DCI policy and directives will be enforced through command channels.

2. DCI planning will be integrated with other aerospace operational planning. Information will be protected and defended at a level commensurate with the threat and the consequences of its compromise, delay, or loss.

2.1. All operational and exercise plans will identify critical and sensitive information and information system dependencies (i.e., centers of gravity). Additional guidance to help determine information criticality/sensitivity is provided in CJCSI 6510.01B, Defensive Information Operations Implementation, and DoDD 5200.xx, Information Assurance (draft). These plans will use and develop IO sections of the Joint Operational Planning and Execution System (JOPES) as applicable.

2.2. Commanders and operational planners will use risk management to apply operational, procedural, physical and technical countermeasures to reduce existing vulnerabilities.

3. Units (i.e., AFIWC, 609IWS), and activities (i.e., Regional/MAJCOM Information Protection Centers and Network Control Centers) that conduct proactive security functions to assist Air Force organizations to deter, detect, defend, report, isolate, contain, and recover from intrusions of information systems will report their resources as part of the Status of Resources and Training System (SORTS) process. Air Staff functional managers, in conjunction with AF/XO, will establish appropriate criteria for this SORTS reporting.

4. Procedures and criteria for reporting DCI events will be adhered to by all Air Force units, to include acquisition and procurement organizations. DCI events include attempted or actual intrusions into Air Force information systems; espionage--to include industrial espionage; spectrum interference incidents; detected adversarial PSYOP or deception efforts; and physical attacks on the Air Force information infrastructure. HQ Air Intelligence Agency (AIA), in coordination with Air Staff, MAJCOMs, HQ AFOSI and HQ AFCA, is the lead agency for developing standardized, comprehensive reporting criteria and reporting procedures for DCI events. HQ AIA, in coordination with the AFOSI, will compile and analyze data on all DCI events and will provide fused reporting to AF command, intelligence, and law enforcement channels and other DCI operational entities (i.e., AFCERT, 609 IWS, AFNCCs, etc.) as appropriate.

5. The Air Intelligence Agency will establish a “Red Team” capability to periodically evaluate the defensive readiness of Air Force units, headquarters, and DRUs. The Red Team will participate as “aggressor units” in operational test, training and exercise events. Air Intelligence Agency will develop policy and procedures for conducting Red Team assessments in concert with appropriate Air Force organizations, such as MAJCOMs who have overall responsibility for the effective implementation of DCI vulnerability assessments within their commands. AFIWC will provide on-demand technical support to all AF organizations to conduct DCI-related vulnerability assessments. AIA will work with the Air Force Inspector General to incorporate assessments into readiness inspections.

6. The Air Force Operations Security (OPSEC) program, managed by AF/XO, and the Air Force Information Assurance program, managed by AF/SC, will be conducted in accordance with existing Air Force policy. MAJCOM commanders are responsible for the effective implementation of these programs. All Air Force members must abide by published security standards and procedures if these programs are to succeed.

7. The Air Intelligence Agency, in coordination with Air Force Special Operations Command and Air Combat Command, will provide a framework for developing and operationalizing the constructs of coun-

terdeception and counter-psychological operations. Various friendly entities (e.g., ISR, military units, and commanders) can identify adversary PSYOP and deception attempts to influence friendly populations and military forces. Air Force counter-PSYOP capabilities will complement existing Joint Psychological Operations Task Force (JPOTF) activities as part of an integrated IO campaign.

8. Air Force commanders must consider how Public Affairs and other military information dissemination can convey truthful, accurate information to mitigate the intended effects of adversary PSYOP. When permitted by National Command Authorities, commanders may use other forces to undertake offensive responses (i.e., physical attack, electronic warfare, etc.) to counter adversarial PSYOP and deception activities.

9. The Air Force will plan and employ Electronic Protection (EP), the defensive component of Electronic Warfare, in accordance with existing doctrine and policy. Air Force EP, while defensive in nature, will be conducted and managed as part of the existing, consolidated EW program which includes electronic attack, electronic protection and electronic support activities. Future EP planning and requirements development must address emerging EW threats (e.g., directed energy weapons, and non-nuclear EMP, other radio frequency weapons, etc.).

10. The Air Force Office of Special Investigations (AFOSI) is the lead agency for the Air Force counter-intelligence program and is responsible for conducting electronic surveillance countermeasures and investigations of unauthorized intrusions into USAF information systems. Close and early coordination between AFOSI and all other DCI team members is critical, as investigations of DCI events frequently cross the functional and legal lines between operations, intelligence, counter-intelligence, and law-enforcement.

11. Effective DCI requires the full integration of several traditional security programs managed by AF/SF:

11.1. The Air Force Physical Security program protects the Air Force critical information infrastructure against conventional or non-conventional attack (e.g., terrorist actions, traditional air base defense threats, etc.) and is an important supporting link in the overall DCI mission area. Air Force operations are vulnerable to unauthorized access and denial-of-service threats. Therefore, commanders must ensure that users and owners of information systems identify both physical and electronic security requirements, and that these requirements be met. Additionally, physical and electronic security requirements must be integrated into operational planning.

11.2. The Air Force Personnel Security program (i.e., security clearances and access controls) is essential to minimize the threat posed by disgruntled employees or hostile internal agents. Internal agents pose a serious threat to Air Force operations due to their unique--often unlimited--access to critical information and information systems. All personnel have a role in maximizing personnel security by being conscious of their working environment, and by noting and reporting suspicious or unusual activities by others.

11.3. The Air Force Information Security program provides policy and procedures for the protection of classified national security information.

11.4. The Air Force Industrial Security program includes policy and procedures for protecting classified information in the hands of US contractors.

12. DCI measures will be embedded into Air Force acquisition programs to ensure security and survivability are integrated throughout the life of a program IAW DoDD 5200.1M, Acquisition System Protection Program and DoDD 5200.39, Security, Intelligence and Counterintelligence Support to Acquisition Program Protection. The Air Force acquisition process will provide Information Assurance for information systems and information-based systems on a "cradle-to-grave" basis, with operational users actively engaged in the definition of operational and training requirements.

13. Air Force DCI operations will respect the rights of US citizens, carefully heeding the rules and procedures in associated laws and directives. DCI activities will be coordinated with cognizant General Counsel and Staff Judge Advocate authorities.

14. The Air Force will work with the other Services and Defense Agencies, the Joint Staff and CINCs, and other government agencies to maximize the security and integrity of USAF information at all times, to include exercises. It will abide by the law and other policies and standards established by appropriate command and control, intelligence, law enforcement, and communications and information authorities.

15. The Air Force will foster strong relationships with commercial industry and other civilian partners to promote the exchange of operational data, tactics, techniques and procedures in order to leverage common capabilities and enhance the overall defensive preparedness of Air Force and critical US information infrastructures. The Air Force will leverage the Reserve Component, with its unique integration into the civilian sector, to achieve this goal.

16. DCI entails a multi-discipline capability that can succeed only as an integrated team effort across nearly all Air Force functional areas. Operations (DO equivalent) is the overall lead for both offensive and defensive counterinformation. Specific DCI disciplines (e.g., OPSEC, counterintelligence, electronic protection, information assurance, etc.) and supporting disciplines (e.g., physical security, personnel security, etc.) will be executed by appropriate functional elements as delineated by existing and emerging Air Force guidance.

17. MAJCOM, NAF, FOA, and DRU Commanders are responsible for implementing and enforcing Air Force DCI policies and directives in their day-to-day operations, as well as for planning, prioritizing, and programming the DCI activities of their commands.

18. Successful DCI begins with each individual accepting and carrying out his/her responsibilities in protecting information and information systems from attack and exploitation by adhering to all applicable policies and procedures.

19. See **Attachment 1** for references and and other supporting information.

F. Whitten Peters
Acting Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD Directive S-3600.1, *Information Operations*, 9 December 1996

DoD Directive 5200.xx, *Information Assurance*, Draft, 19 May 1998

DoD Directive 5200.1M, *Acquisition System Protection Program*, Draft, September 1997

DoD Directive 5200.39, *Security, Intelligence and Counterintelligence Support to Acquisition Program Protection*, 10 September 1997

Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994

CJCSI 3210.01, *Information Warfare Policy*, 2 January 1996

CJCSI 3213.01A, *Joint Operations Security*, 1 December 1997

CJCSI 6510.01B, *Defensive Information Operations Implementation*, 22 August 1997

AFDD 1, *Air Force Basic Doctrine*, September 1997

AFDD 2-5, *Information Operations*, Final Draft, 6 April 1998

NSTISSI No. 4009, *National Information Systems Security Glossary*, August 1997

AFPD 10-7, *Command and Control Warfare*, 12 August 1993

AFPD 10-11, *Operations Security*, 17 May 1993

AFPD 31-1, *Physical Security*, 1 August 1995

AFPD 31-4, *Information Security*, 1 August 1997

AFPD 31-5, *Personnel Security Program Policy*, 1 August 1995

AFPD 31-6, *Industrial Security*, 1 August 1997

AFPD 33-2, *Information Protection*, 1 December 1996

AFPD 71-1, *Criminal Investigations and Counterintelligence*, 3 March 1995

Terms

Classified Information—Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (Joint Pub 1-02)

Counterdeception—Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. (Joint Pub 1-02).

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. (Joint Pub 1-02)

Counterpsychological Operations—Efforts to negate, neutralize, diminish the effects of, or gain advantage from foreign psychological operations.

Defensive Counterinformation—Activities which are conducted to protect and defend friendly information and information systems. Also called DCI. (AFDD 2-5)

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. (DoDD S-3600.1)

Information Operations—Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (Joint Pub 3-13, Preliminary Coordination, 28 Jan 98.) (This term promulgated in DoDD S-3600.1) The Air Force believes that in practice a more useful working definition is: [those a-ctions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare.] {Italicized definition in brackets applies only to the Air Force and is offered for clarity.} (AFDD 2-5)

Information Superiority—The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Also called IS. (Joint Pub 3-13, Preliminary Coordination, 28 Jan 98.) (This term promulgated in DoDD S-3600.1) The Air Force prefers to cast 'superiority' as a state of relative advantage, not a capability, and views Information Superiority as: The Air Force prefers to cast 'superiority' as a state of relative advantage, not a capability, and views IS as: [*That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.]* . {Italicized definition in brackets applies only to the Air Force and is offered for clarity.} (AFDD 2-5)

Critical Information—Information about friendly activities, intentions, capabilities, or limitations that an adversary needs in order to gain a military, political, diplomatic, or technological advantage. (CJCSI 3213.01A)

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. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

Sensitive Information—Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (NSTISSI No. 4009)

Attachment 2

MEASURING AND DISPLAYING COMPLIANCE WITH POLICY

A2.1. Defensive counterinformation (DCI) is a multi-discipline capability impacting many functional areas. Several DCI capabilities (e.g., information assurance, OPSEC, counterintelligence, etc.) have been implemented for years through existing policy and AFIs. AFPD 10-20 is not intended to duplicate or interfere with the management of those elements of the DCI program that are already working well. However, all Air Force policy directives, instructions, and other official guidance pertaining to DCI operations will be reviewed annually by OPRs and, as necessary, updated or reinvigorated to reflect the growing IO threat.

A2.2. The strategy for reporting compliance with this AFPD entails the following: HQ AIA, a field operating agency of HQ USAF/XO, will serve as the OPR for measuring Air Force-wide compliance with DCI policy via a comprehensive annual report to AF/XO. This report will depict the overall health of the Air Force DCI mission area, as measured by the agencies responsible for the various DCI programs and the Inspector General. The report should be developed by assessing existing metrics already in place under current AF policy and by assessing new metrics which will be developed by functional OPRs in support of this AFPD (e.g., SORTS, legal review of defensive IO operational activities, etc.). A comprehensive list of inclusive DCI policy areas, to include those areas for which new metrics are required, as well as specific guidance to functional OPRs for reporting compliance data to HQ AIA, will be provided in a subordinate AFI. As they become available, SORTS reporting and IO-related exercise results and lessons-learned will be compiled by HQ AIA for integration into the annual compliance report to ensure it provides a comprehensive assessment of the DCI program. Examples of metrics from designated functional OPRs to be integrated into the annual report are identified below.

Figure A2.1. Sample Metric of Systems Accreditation Status.

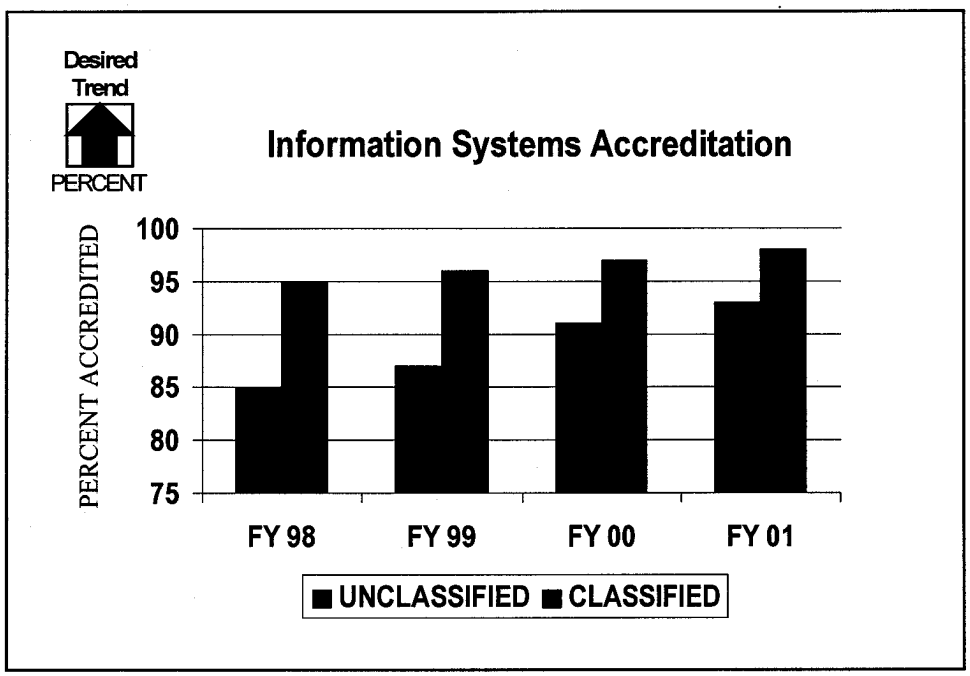

Figure A2.2. Sample Metric of AFOSI Case Resolution Rates for Counterintelligence and Computer Crime.

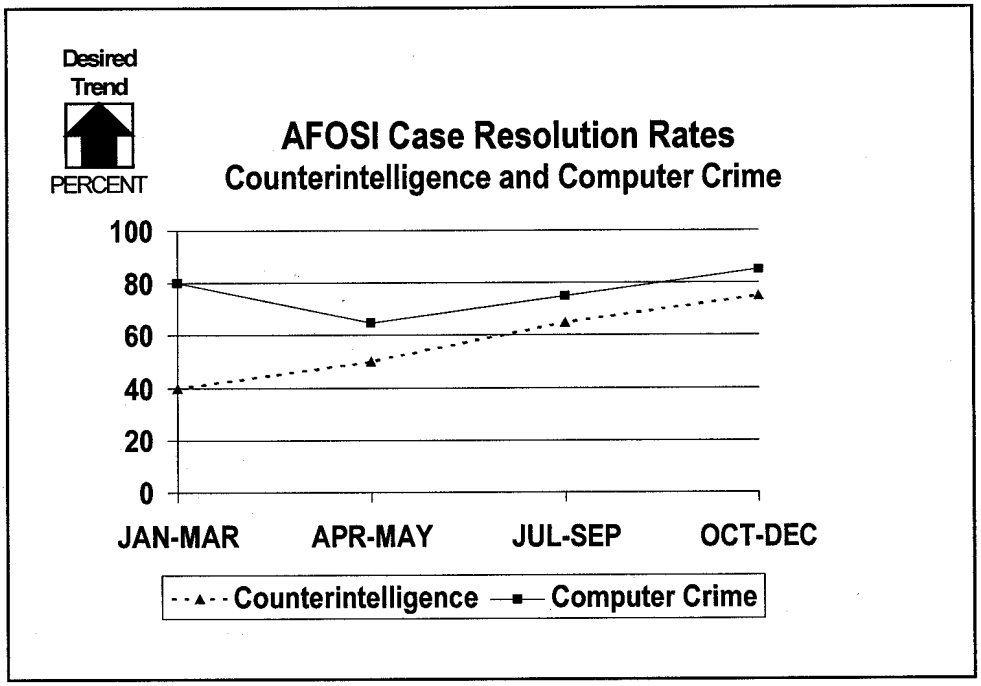

Figure A2.3. Sample Metric of IG Inspection Results for OPSEC Programs.