

1 APRIL 2000



Security

INDUSTRIAL SECURITY

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

OPR: HQ USAF/XOFI (Mr Dan Green)

Certified by: HQ USAF/XOF (Brig Gen Richard A. Coleman)

Supersedes AFD 31-6, 1 July 1995

Pages: 5
Distribution: F

This directive provides Air Force policy for protecting classified national security and sensitive unclassified information (regardless of its classification, sensitivity, physical form, media or characteristics) and sensitive government resources entrusted to industry. It assigns responsibility for implementing and managing the Industrial Security Program. It establishes a system of review that identifies outdated, inappropriate or unnecessary contractual security requirements. This directive implements Executive Order 12829, *National Industrial Security Program (NISP)*, DoD 5220.22-R, *Industrial Security Regulation*, DoD 5220-22-M, *National Industrial Security Program Operating Manual (NISPOM)*. It interfaces with other security program publications to protect the United States national security interests.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. This revision requires Air Force activities to identify government information and resources that must be protected against compromise and to include appropriate security guidance and/or requirement into their solicitation. It allows on-base contractors to operate under Air Force Policy Directive (AFPD) 31-4, *Information Security* and Air Force Instruction (AFI) 31-401, *Information Security Program Management*, via the execution of a Visitor Group Security Agreement (VGSA). See Glossary of References and Supporting Information at Attachment 1.

- 1.** The Air Force will implement security policies and procedures consistent with the standards of the National Industrial Security Program Operating Manual (NISPOM), Information Security Program and Federal Acquisition Regulations (FAR). Commanders at all levels will ensure protection of national security classified and sensitive unclassified information released to contractors.
- 2.** The Administrative Assistant to the Secretary of the Air Force (SAF/AA) is designated the Air Force Senior Security Official responsible for ensuring implementation of the Industrial Security Program.

3. The Headquarters United States Air Force, Directorate of Security Forces, Information Security Division (AF/XOFI) is responsible for policy development, interpretation, administration, and program oversight.
4. Headquarters US Air Force, Director of Intelligence, Surveillance, and Reconnaissance (AF/XOI) is responsible for Sensitive Compartmented Information (SCI) policy.
5. The Administrative Assistant to the Secretary of the Air Force, Director of Security and Investigative Programs (SAF/AAZ) is responsible for Special Access Program (SAP) policy.
6. Each major command (MAJCOM) will establish an industrial security program and provide oversight for its subordinate activities. Installation commanders will ensure program implementation and provide program oversight as necessary.
7. Air Force on-base contractor visitor groups will be integrated into the host installation's Information Security Program unless the mission, operational requirements, autonomous nature or other factors require them to establish and maintain their own security program under the NISPOM.
8. Air Force activities will identify government information and sensitive resources unique to their programs or projects that must be protected. These activities will incorporate appropriate security classification guidance, if applicable and handling, processing, marking, and safeguarding requirements into all their solicitations.
9. Contracting officers will ensure that contractual security specifications, safeguards and/or protection requirements are coordinated with and thoroughly reviewed by the appropriate security activity and functional area or office of primary responsibility (OPR) prior to issuing the solicitation.
10. See **Attachment 2** for the way to measure and display policy results.

F. WHITTEN PETERS
Secretary of the Air Force

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

Executive Order 12829, *National Industrial Security Program*, 7 Jan 1993

Executive Order 12958, *Classified National Security Information*, 20 Apr 1995

Office of Management Budget (OMB) Circular A-130, *Management of Federal Information Resources*, 8 Feb 1996

Federal Acquisition Regulation (FAR), Jun 1997

DoD Regulation 5200.1-R, *Information Security Program*, Jan 1997

DoD Manual 5220.22-M, *National Industrial Security Program Operating Manual*, Jan 95

DoD Regulation 5400.7/AF Supplement, *Freedom of Information Act Program*

Defense Federal Acquisition Regulation Supplement (DFARS), 17 Aug 1998

Air Force Federal Acquisition Regulation Supplement (AFFARS), 1 May 1996

AFPD 16-7, *Special Access Programs*, 10 Mar 1993

AFPD 31-4, *Information Security*, 1 Sep 1998

AFPD 37-1, *Air Force Information Management*, 19 Nov 1993

AFPD 64-1, *Contracting System*, 29 Mar 1993

AFI 31-401, *Information Security Program Management*, 1 Jan 1999

AFI 33-332, *Air Force Privacy Act Program*, 12 Oct 99

Abbreviations and Acronyms

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

DoD—Department of Defense

DRU—Direct Reporting Unit

FAR—Federal Acquisition Regulation

FOA—Field Operating Agency

ISPM—Information Security Program Manager

MAJCOM—Major Command

OPR—Office of Primary Responsibility

SAP—Special Access Program

SCI—Sensitive Compartmented Information

VGSA—Visitor Group Security Agreement*Terms*

Classified National Security Information—(or “classified information”). Information that has been determined pursuant to Executive Order 12958, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status.

Contract—A mutually binding legal relationship obligating the seller to furnish the suppliers or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, in writing.

Sensitive Information—(or “sensitive unclassified information” or “controlled unclassified information”). Consistent with the Computer Security Act of 1987, “sensitive” information is defined as any 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 Title 5, United States Code, Section 552a (The Privacy Act), but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (**NOTE:** Privacy information also qualifies for protection under Title 5, United States Code, Section 552 (Freedom of Information Act of 1974).

Attachment 2

MEASURING AND DISPLAYING POLICY

A2.1. Information security program managers (ISPMs) will review AF contractual documents to determine if appropriate security guidance or protection requirements have been incorporated which requires contractors to protect classified and sensitive unclassified information. New and revised contracts must specifically address protection requirements for classified national security and sensitive unclassified information.

A2.2. The ISPM will review applicable sections or parts of draft solicitation documents (invitation for bid (IFB), request for proposal (RFP), request for quote (RFQ), statement of work (SOW) statement of objective (SOO), DD Form 254, etc.) submitted to the servicing contracting activity during the third quarter of each fiscal year (FY) to assess the originating AF activity’s understanding of and compliance with this AFPD. The ISPM will compile statistical data related the total number of draft solicitation documents reviewed, in relation to the number of documents returned to the originating activity for cause (outdated, excessive, insufficient or inappropriate security guidance or protection requirements). MAJCOMs will consolidate the data collected by their respective ISPMs and forward the previous fiscal year data report to HQ USAF/XOFI, via RCS: HAF-XOFI(A)9224, Industrial Security Measurement Report by 1 Nov. Discontinue reporting during MINIMIZE.

A2.3. Data will be collected effective 1 Apr through 30 Jun each fiscal year. ISPMs reporting will be via MAJCOM channels and, FOAs and DRUs will report direct HQ USAF/XOFI.

Figure A2.1. Sample Metric of Industrial Security Program.

