The following are pertinent excerpts from:

AIR FORCE INSTRUCTION 31-401
1 NOVEMBER 2005

INFORMATION SECURITY PROGRAM MANAGEMENT

Supersedes AFI 31-401, 1 November 2001

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-401

1 NOVEMBER 2005

Security

INFORMATION SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ USAF/XOS-FI

Certified by: HQ USAF/XO
(Lt Gen Carrol H. Chandler)

Supersedes AFI 31-401, 1 November 2001

Pages: 87

This publication implements Air Force Policy Directive (AFPD) 31-4, Information Security. It prescribes and explains how to manage and protect unclassified controlled information and classified information. Use this instruction with Executive Order (EO) 12958, as amended, *Classified National Security Information*, 25 March 2003; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, *Classified National Security Information,* Executive Order 12829, National Industrial Security Program (NISP), DOD Manual 5220.22, *National Industrial Security Program Operating Manual,* January 1995; and, Department of Defense (DOD) 5200.1-R, *Information Security Program*, 14 Jan 97, for the management of the Air Force Information Security Program. Additional references include DOD Instruction (DODI) 5240.11, *Damage Assessments*, 23 Dec 91; DOD Directive (DODD) 5210.83, *Unclassified Controlled Nuclear Information (UCNI),* 15 Nov 91; Air Force Policy Directive (AFPD) 31-4, *Information Security*. This instruction is applicable to contractors as prescribed in AFI 31-601, *Industrial Security Program*. All these references are listed at the end of each paragraph where applicable. This instruction is not to be used as a stand-alone document. HQ USAF/XOS-F is delegated approval authority for revisions to this AFI.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. The revision updates the Table of Contents to remove **Attachment 4**, Department of the Air Force Executive Order (EO) 25 Year Automatic Declassification Plan, **Attachment 7**, Air Force Information Security Program Training Standard, and Attachment 10, Air Force Original Classification Authority List, which were moved to web pages; deletes references to Director/Chief of Acquisition Security; defines the term staff agency chief (paragraph **1.3.5.**); refines requirements for security managers (paragraph **1.3.5.1.**); prohibits use of contractors as security managers (paragraph **1.3.5.2.**); establishes the security manager as the organizational Joint Personnel Adjudication System (JPAS) manager (paragraph **1.3.6.10.**); outlines procedures for information security program oversight (paragraph **1.4.**); clarifies waiver process (paragraph **1.6.**); updates reporting requirements (paragraph **1.7.**); updates form requirements (paragraph 1.10.); replaces

level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. The nature of the classified material typically stored within a secure room or vault may preclude the use of cover sheets.

5.19. Use of Key-Operated Locks *[Reference DOD 5200.1-R, C6.4.3.6.1.]*

5.19.1. The authority to determine the appropriateness of using key-operated locks for storage areas containing bulky Secret and Confidential material is delegated to the unit commanders or equivalents, and staff agency chiefs having this storage requirement. When key-operated locks are used, the authorizing official will designate lock and key custodians.

5.19.2. Lock and key custodians use AF Form 2427, (available on the AFEPL) to identify and keep track of keys.

5.20. Procurement of New Storage Equipment *[Reference DOD 5200.1-R, C6.4.5.]*

5.20.1. Requesters of exceptions send their requests through command ISPM channels to HQ USAF/XOS-FI. HQ USAF/XOS-FI will notify USD/I of the exception *[Reference DOD 5200.1-R, C6.4.2.]*

5.20.2. See AFMAN 23-110, Volume II, *Standard Base Supply Customer's Procedures [Reference DOD 5200.1-R, C6.4.2.]*

5.21. Equipment Designations and Combinations.

5.21.1. See AFMAN 14-304 for guidance on marking security containers used to store SCI *[Reference DOD 5200.1-R, C6.4.1.]*

5.21.2. Use SF Form 700, **Security Container Information** (available through the Air Force Publications Distribution system), for each vault or secure room door and security container, to record the location of the door or container, and the names, home addresses, and home telephone numbers of the individuals who are to be contacted if the door or container is found open and unattended. Applying classification marking to SF 700, Part 1, is not required when separated from Part 2 and 2a.

5.21.2.1. Affix the form to the vault or secure door or to the inside of the locking drawer of the security container. Post SF Form 700 to each individual locking drawer of security container with more than one locking drawer, if they have different access requirements.

5.21.2.2. The SF 700 contains Privacy Act information and must be safeguarded from casual view, but must be readily identifiable by anyone that finds the facility unsecured.

5.21.3. When SF Form 700, Part II, is used to record a safe combination, it must be:

5.21.3.1. Marked with the highest classification level of material stored in the security container; and,

5.21.3.2. Stored in a security container other than the one for which it is being used.

5.22. Repair of Damaged Security Containers *[Reference DOD 5200.1-R, C6.4.7.]*

5.22.1. Locksmiths or technicians must be GSA certified and either have a favorable NAC or must be continuously escorted while they are repairing security containers. See guidance for unescorted entry to restricted areas in AFI 31-501.

5.22.2. The Naval Facilities Engineering Service Center (NFESC) Technical Data Sheet (TDS) 2000-SHR, *Neutralizing Locked Out Security Containers*, can be obtained from the NFESC, 1100 23rd Avenue, Code ESC66, Port Hueneme, California 93043-4370 or at: **http://locks.nfesc.navy.mil/pdf_files/TDS-2000-SHR.pdf** *[Reference DOD 5200.1-R, C6.4.7.2.]*

5.22.3. Federal Standard 809, Neutralization and Repair Of GSA-approved Containers can be obtained from the NFESC, 1100 23rd Avenue, Code ESC66, Port Hueneme, California 93043-4370 or at: **http://locks.nfesc.navy.mil/pdf_files/fs809.pdf**.

5.22.4. Personnel who have had their GSA-approved security containers repaired, must have the locksmith or technician confirm that the container still meets GSA standards. If there is doubt, personnel may contact the DOD Lock Hotline managed by NFESC (800-290-7607) or GSA through supply channels for assistance. Findings and the source of confirmation must be recorded on an AFTO Form 36 retained in the container.

5.23. Maintenance and Operating Inspections. Personnel will follow maintenance procedures for security containers provided in AFTO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Security Type Equipment*. Commanders or equivalents and staff agency chiefs may authorize trained security managers and security container custodians to perform inspections and preventive maintenance on safes and vaults. Note: Training is conducted by locksmiths or other personnel who are qualified as to technical construction, operation, maintenance, and purpose of such security type equipment *[Reference DOD 5200.1-R, C6.4.7.]*

5.24. Reproduction of Classified Material.

5.24.1. Unit commanders or equivalents, and staff agency chiefs designate equipment for reproducing classified material.

5.24.2. The DAA approves networked equipment used to reproduce classified information. Information managers (3A0X1) issue procedures for clearing copier equipment of latent images.

5.24.3. Security managers:

5.24.3.1. Should display procedures for clearing latent images of equipment used to copy classified material in a location clearly visible to anyone using the equipment;

5.24.3.2. Develop security procedures that ensure control of reproduction of classified material; and,

5.24.3.3. Ensure personnel understand their security responsibilities and follow procedures.

5.25. Control Procedures. Unit commanders or equivalents and staff agency chiefs designate people/positions to exercise reproduction authority for classified material in their activities *[Reference DOD 5200.1-R, C6.5.1.]*

5.26. Emergency Authority. *(*See *EO 12958, as amended, Section 4.2(b) and ISOO Directive No. 1, Section 2001.51.)*

5.26.1. In emergency situations, in which there is an imminent threat to life or in defense of the homeland; Military Department or other DOD Component Agency, MAJCOM/FOA/