

**BY ORDER OF THE COMMANDER
EGLIN AIR FORCE BASE**

AIR FORCE INSTRUCTION 31-401



**EGLIN AIR FORCE BASE
Supplement**

24 JUNE 2013

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: 96 TW/IP

Certified by: 96 TW/IP
(Mr. Chris Simpson)

Supersedes: EGLINAFBAFBI31-401,
11 Sep 2009

Pages: 11

This supplement applies to all activities assigned to Eglin AFB, the 96th Test Group (96 TG) at Holloman AFB, NM, and Eglin AFB associate organizations participating in the Information Security Program. This instruction applies to the Air Force Reserve, Air National Guard, and those combatant commands where the Air Force is the executive agent. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). This instruction requires collecting and maintaining information protected by the *Privacy Act of 1974* authorized by Title 10, U.S.C., Section 8013. System of Records notice F033 AF B, Privacy Act Request File, applies. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional chain of command. Waivers for any part of the publication are not granted. See AFI 31-401, Attachment 1, for a glossary of references and supporting information.

SUMMARY OF CHANGES

Revisions include: Changes Information Security Program Review (ISPR) to Local Information Protection Management Evaluation (LIPME); delegates responsibilities of Information Security Program Manager (ISPM) to the Director of Information Protection (96 TW/IP); changes frequency of security manager (SM) meetings from quarterly to semiannually (paragraph

1.3.4.5.); updates information required on SM appointment memos (paragraph 1.3.5.3.); implements electronic handbook option (paragraph 1.3.6.11.); clarifies LIPME requirements for limited LIPME support; removes 18 month extensions based on discrepancy free programs (paragraph 1.4.2.); clarifies contractor self-inspection responsibilities (paragraph 1.4.3.1.); updates Original Classification Authority (OCA) office symbols (paragraph 2.1.1.); identifies granting authority for DoE Form 5631.20, *DoE Request for Visit or Access Approval* (paragraph 1.5.1.1.); removes para 1.5.1.2.1., refer to AFI 31-401 para 1.5.1.2.1.; requires users to mark classified media with unit of origin and contact info when transporting outside the unit (paragraph 4.8.); eliminates EAFB Form 50 and implements secure room certification memos (paragraph 5.18.2); replaces safe, vault, and secure room Preventative Maintenance Inspection (PMI) with Operational Visual Inspection (OVI) (paragraph 5.23.); corrects labeling requirements for data processing equipment (paragraph 5.24.3.4.); removes requirement for 96 TW/IP approval to hand carry classified aboard commercial aircraft overseas (paragraph 6.7.1.1.); adds Escambia County to the local area (paragraph 6.8.1.); implements the EAFB Information Security Training Plan (paragraph 8.3.6.2.); incorporates OCA training for personnel who support an OCA (paragraph 8.6.1.).

1.3.4.1. The Director of Information Protection (96 TW/IP) manages and implements the Eglin AFB Information Security Program for Eglin AFB, 96 TG units at Holloman AFB and other units as identified in support agreements.

1.3.4.5. At Eglin AFB, 96 TW/IP will conduct semiannual security manager meetings. As the information security focal point within each organization, SMs or their designated DoD civilian or military alternates will attend semiannual meetings. DoD contractors may attend, but shall not represent AF organizations. At Holloman AFB, 96 TG/SP will host and document security manager meetings.

1.3.5.3. Send Security Manager (SM) appointment memorandums to 96 TW/IPIP. Include full name, rank/grade, organization, office symbol, phone number, and outgoing security manager if applicable. A sample SM appointment memo is available on the 96 TW/IP SharePoint site.

1.3.5.4. **(Added)** SMs will post flyers identifying both primary and alternate SMs throughout their areas of responsibility. EAFBVA 31-11, *Your Security Manager Is*, may be used, and is available on the 96 TW/IP SharePoint site.

1.3.6.11. **(Added)** SMs must maintain a Security Manager's Handbook, either electronic or hard copy. The table of contents and an electronic Security Manager's Handbook template can be found on the 96 TW/IP SharePoint. The handbook will be organized as follows:

1.3.6.11.1. **(Added)** Tab 1: SM appointment memorandum.

1.3.6.11.2. **(Added)** Tab 2: Unit security operating instruction and applicable secure room operating instructions. Note: The operating instructions must be reviewed every two years.

1.3.6.11.3. **(Added)** Tab 3: A list of security containers, to include vaults and secure rooms, within the organization showing: container ID number, location,

and primary and alternate safe custodians.

1.3.6.11.4. **(Added)** Tab 4: A list of equipment approved by the commander for classified reproduction.

1.3.6.11.5. **(Added)** Tab 5: Last unit self-inspection report, completed checklists, and corrective actions report, if required. Reports must address all applicable information security disciplines and be signed by the commander, or equivalent. Self-inspections must be conducted and documented IAW the 96 TW/IP Self-Inspection Handbook.

1.3.6.11.6. **(Added)** Tab 6: Last Local Information Protection Management Evaluations (LIPME) report and corrective actions report, if required.

1.3.6.11.7. **(Added)** Tab 7: Information, Personnel and Industrial Security publications and applicable policy memorandums.

1.3.6.11.8. **(Added)** Tab 8: Security Training Documentation, e. g., training statistics, sign-in rosters, e-mail receipts for initial and refresher training, and other forms of training documentation. Training documentation must be maintained for previous and current year.

1.3.6.11.9. **(Added)** Tab 9: Annual Unit Manning Document Review.

1.3.6.11.10. **(Added)** Tab 10: Last Security Manager Meeting Minutes.

1.3.6.11.11. **(Added)** Tab 11: Miscellaneous.

1.3.8. 96 TW/IP manages and implements the Eglin AFB Foreign Disclosure Program. Direct all inquiries involving foreign national visits and disclosures to 96 TW/IPF. At Holloman AFB, 96 TG/SP is the 96 TG focal point.

1.4.3. All units under 96 TW/IP oversight will receive an annual LIPME. Units that do not store classified information will receive a LIPME every 2 years. Units that only require secure room/vault support in accordance with a support agreement will receive a secure room/vault review every 2 years utilizing the 96 TW/IP Secure Room/Vault Checklist.

1.4.4. Units will conduct semi-annual self-assessments 6 months after their LIPME, and follow the guidance in the 96 TW/IP Guide to Conducting Semi-Annual Security Self-Assessments. Use the Information Security, Personnel Security, and Industrial Security self-assessment checklists, as applicable. Organizations that do not store classified information will conduct at a minimum, one unit security self-assessment annually.

1.4.4.1. Integrated Visitor Group Contractors will not conduct annual security self-assessments.

1.5.1.1. The following positions at Eglin AFB may sign DoE Form 5631.20, *DoE Request for Visit or Access Approval*, and appear on the list of certifying officials, at Enclosure 4 to DoDI 5210.02: AFLCMC/EB-OL: AFPEO for Weapons and Director, Armament Directorate, the Deputy Director, Armament Directorate, and 96 TW/IP, Director, Information Protection.

2.1.1. 96 TW/CC, AFLCMC/EB-OL, and AFRL/RW are delegated Secret OCA. Non-AFMC organizations on Eglin AFB with OCA delegation through separate channels will provide delegation documentation to 96 TW/IP.

2.6.2.4. Coordinate Security Classification Guides (SCG) through the following offices: Chain of command as required; 96 TW/IP, Information Protection Office; 96 TW/IPF, Foreign Disclosure Office; and AFLCMC/INMA-OL, Intelligence Directorate.

2.6.3.1.1. Submit guides that exempt classification beyond 25 years through 96 TW/IP to ISCAP for approval.

2.6.3.2. Submit an electronic copy of SCGs and DD Form 2024 for all SCG events to 96 TW/IPIP.

4.11. When transporting classified media outside the unit, in addition to required classification markings, mark media with unit of origin and date.

5.10. Designate, in writing, personnel to conduct end-of-day checks. End-of-day security checks will be conducted anytime an area where classified is stored has been occupied or accessed. If personnel become unable to perform checks, they must coordinate with other office personnel to ensure checks are conducted in their absence.

5.12.1. For all levels of collateral classified material: Eglin Command Post (96 TW/CP), Bldg 1, Rm 23, DSN 875-4020. For bulk classified material up to and including Secret: 96th Logistics Readiness Squadron (96 LRS), Receiving Area, Building 600, Room 300, contact LGRM Admin during duty hours at DSN 872-4676; contact 96 TW/CP for after-hours access. For Special Compartmented Information (SCI): AFLCMC/INMS-OL Special Security Office (SSO), Bldg 1, Rm 26.

5.13.2.2. Personal electronic devices such as cell phones and other communication devices, laptop computers, etc. are not allowed in areas used for classified events and meetings unless the sponsoring OPR states otherwise and specifically outlines security measures in the classified event plan.

5.13.2.4. At Eglin AFB, contact 96 TW/IP for approved classified event and meeting locations. Units must submit a classified event plan to 96 TW/IP to approve an alternate facility. A sample classified event/meeting plan is available on the 96 TW/IPI SharePoint in the Program Procedures folder. 96 TG personnel at Holloman AFB will submit classified event plans to 96 TG/SP for approval.

5.13.3. Eglin units coordinate foreign participation in classified meetings with 96 TW/IPF, 96 TG personnel at Holloman AFB coordinate with 96 TG/SP.

5.18.2. Commanders must justify secure room establishment during planning stages before construction begins. SMs will submit justification to 96 TW/IP for approval. When approved, 96 TW/IP will conduct an initial physical security assessment and provide a detailed report outlining construction and certification requirements, coordinate construction requirements with 96 CEG/CEP, conduct a final assessment upon completion of construction, and provide a certification memo. At Holloman AFB, 96 TG/SP will review and approve secure room certification and construction, coordinate

with local CE personnel when necessary, provide a certification memo and forward a copy to 96 TW/IP.

5.18.2.4. SMs will notify 96 TW/IP of changes in secure room and vault status, modifications, and deactivation. SMs will coordinate alarm account deactivation with 96 SFS/S5E, Electronic Security Systems. At Holloman AFB, 96 TG SMs will coordinate with 96 TG/SP.

5.21.2. At a minimum, two names will be listed on Standard Form 700, *Security Container Information*. List the primary and alternate "Safe Custodians" who are responsible for the container's serviceability, preventive maintenance, and contents. The SF 700 is an acceptable safe custodian appointment document. Integrated Visitor Group contractors will not be appointed safe custodians and cannot be listed on the Standard Form 700.

5.23. SMs who have completed 96 TW/IP SM training are authorized to perform, and may train safe, vault, and secure room custodians to perform Preventative Maintenance Inspections (PMI). Safe, vault, and secure room custodians may also perform PMI upon completing the 96 TW/IP Safe Custodian Course. SMs will ensure primary and alternate safe, vault, and secure room custodians are appointed in writing and trained. The SF 700 is a sufficient appointment document. Secure room PMI will be conducted every 2 years. All PMI will be completed IAW AF T.O. 00-20F-2.

5.23.1. **(Added)** SMs will affix a unique permanent marking such as office symbol and a locally developed serial number to the front of containers in the upper left or right corner. Example: 96 TW/IP #1.

5.23.2. **(Added)** The tops of security containers shall be kept completely clear of items so that visual inspection will easily confirm classified information or equipment was not inadvertently left on top.

5.24.3.4. **(Added)** Affix EAFBVA 31-9, *Classified Reproduction Rules*, and EAFBVA 31-10a, *GO Authorized For Classified Processing GO*, on copiers and FAX machines that have been approved by the commander for classified processing. Affix EAFBVA 31-10a to other equipment that is approved for classified processing such as scanners and printers. Affix EAFBVA 31-10, *STOP Not Authorized For Classified Processing STOP*, on all copiers and FAX machines that are not authorized for classified reproduction. In areas where SIPRNet is accessible, affix EAFBVA 31-10 on all computer equipment that is not authorized for classified processing, and EAFBVA 31-10a on all computer equipment that is authorized for classified processing.

5.27.2. During the annual "Clean-out Day", identify all documents 25-years old or older to determine the review requirements of AFI 31-401 paragraphs 3.4. and 3.6.. Review all documents and electronic media to ensure they have the appropriate classification markings.

5.28.1. SMs will initially inspect shredders and other destruction equipment to ensure they appear on the appropriate NSA evaluated products list. SMs will then complete and post EAFB Form 53, *Destruction Equipment Certification*, inside each machine's access door or panel, and conspicuously post EAFB VA 31-10a on the exterior so it is easily

seen by users. Recertification is required upon major damage, repair or replacement of blades or cutting devices, to verify NSA standards are still met. Conspicuously post EAFB VA 31-10 on the exterior of other shredders and equipment used to destroy unclassified media and documents.

6.7.1.1. When approval is granted to hand carry classified on board commercial flights, security managers will ensure couriers are briefed IAW DoDM 5200.01-V3, ENCL 4, Section 12. When applicable, coordinate the release of classified information to a foreign government or foreign representative with the unit Foreign Disclosure Officer.

6.7.2. SMs will utilize the courier briefing posted in Attachment 1 of the 96 TW Classified Courier/Hand carrying Handbook, located on the 96 TW/IP SharePoint in the Publications / Eglin Handbooks folder, to brief authorized personnel on courier responsibilities. Have personnel acknowledge the briefing and keep a copy on file until courier duties are no longer necessary.

6.7.2.1. **(Added)** When hand carrying classified, couriers will ensure material is transported in two vessels. A briefcase, courier bag or similar vessel can be used as the outer wrapping.

6.8.1. **(Added)** For hand carrying purposes, the local area at Eglin AFB is defined as Okaloosa, Walton, Escambia, and Santa Rosa counties. The local area for 96 TG units is defined by 96 TG/SP.

8.3.6.2. The Eglin AFB security training plan is included in Attachment 2 of this supplement. Unit SMs will use this training plan as a guideline and supplement as needed to meet organizational needs. (i.e., Processing and handling of special types of information such as FGI, NATO, CNWDI, etc.)

8.4.1.1. Accomplish and document initial security training as soon as possible when new personnel report for duty but before granting access to classified information. Initial training documentation at a minimum shall include the date of training, individual's name and duty status (i.e. Military, Civilian, or Contractor).

8.6.1. 96 TW/IP will provide original and derivative classification, marking, and SCG preparation training to unit SMs that support an OCA, who will in-turn train program managers and subject matter experts who prepare SCGs for OCA approval.

8.9.1.2. The quarterly refresher training standard goal is 100% completion by all assigned personnel. The minimum training standard is 90% completion. Eglin AFB SMs and associate unit SMs, participating through support agreements (SA), will provide training documentation and training percentage statistics during annual LIPMEs. Units reporting less than 90% must include a short explanation as to why the training standard was not achieved and when it will be.

8.9.2. 96 TW/IP provides OCA refresher training during the first quarter of each year and will coordinate training through appropriate unit SMs to ensure accurate OCA appointment and training. The unit SM will coordinate training for newly assigned OCAs through 96 TW/IP.

- 8.11.1.2. SMs will retain Air Force Form 2587, *Security Termination Statement*, for 2 years.
- 9.8.1. Report security incidents involving computer systems to the unit Information Assurance Officer or unit Information Assurance Manager. Report incidents involving COMSEC material or cryptographic information to the unit COMSEC Responsible Officer. At Eglin AFB, report security incidents involving Sensitive Compartmented Information (SCI) to AFLCMC/INMS-OL at Commercial (850) 882-3908 or DSN 872-3908. At Holloman AFB, 96 TG/SP will coordinate and track security incidents involving 96 TG units. They will provide unit commanders with technical guidance regarding inquiry official appointment, preliminary inquiries, technical reviews, damage assessments. 96 TG/SP will forward a copy of completed preliminary inquiry reports with associated documentation to 96 TW/IP, and report compromises to 96 TW/IP immediately upon discovery.
- 9.9.1.2. Seek assistance to administer oaths, take verbal testimony or sworn statements, and other legal matters as necessary. The inquiry official will submit reports for legal review when recommending administrative or disciplinary action. Use the "96 TW/JA Work Flow" email address to coordinate legal reviews. Inquiry officials may staff JA and 96 TW/IP reviews simultaneously. 96 TG/SP will coordinate with Holloman AFB JA when necessary.
- 9.9.3. Inquiry officials must complete inquiries within 10 duty days after appointment. Appointing authorities may extend inquiries when necessary to properly categorize an incident or make a compromise determination. The appointing authority will submit a justification memo to the DIP or the inquiry official may include a statement in the report detailing appointing authority granted extensions.
- 9.11.2.1. Submit a copy of the appointment memo to 96 TW/IP.
- 9.12.1. Inquiry Official will route completed inquiry reports through unit SMs who will review for completeness, request additional information as necessary, and submit completed reports to 96 TW/IP. Refer to Eglin AFB Security Incident Handout for security incident procedures.
- 9.12.3.1. At Holloman AFB, 96 TG/SP will provide management oversight and technical assistance for 96 TG security incidents.
- 9.13. When an individual having access to classified information is absent without authorization, agency heads shall determine if there are indications that classified information may be at risk, and report status to the 96 TW/IP [*Reference DODM 5200.01-V3, ENCL 6, para 5.n.*].

DAVID A. HARRIS, Brigadier General, USAF
Commander

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

EAFBVA 31-9, *Classified Reproduction Rules*, 28 Oct 09

EAFB VA 31-10, *STOP Not Authorized for Classified Processing STO*, 23 Sept 09

EAFBVA 31-10a, *GO Authorized For Classified Processing GO*, 23 Sept 09

EAFBVA 31-11, *Your Security Manager Is*, 5 May 09

Prescribed Forms

EAFB Form 53, *Destruction Equipment Certification*,

Adopted Forms

AF IMT 847, *Recommendation for Change of Publication*,

All Purpose Checklist, *Information Security Self-Inspection Checklist*,

All Purpose Checklist, *Personnel Security Self-Inspection Checklist*,

All Purpose Checklist, *Industrial Security Self-Inspection Checklist*,

SF 700, *Security Container Information*,

AF Form 2587, *Security Termination Statement*,

DoE Form 5631.20, *U.S. DOE Request for Visit or Access Approval*,

Attachment 2

EGLIN INITIAL AND ANNUAL INFORMATION SECURITY TRAINING STANDARDS

A2.1. This training plan is the blueprint to follow when planning initial and annual refresher training for cleared and uncleared personnel. 96 TW/IP derived this plan from AF Information Protection training standards developed by the Secretary of the Air Force. These standards were used to prepare quarterly Information Security training presentations 96 TW/IP provides to Security Managers at the beginning of each quarter. Security Managers are responsible for administering training to unit personnel and are encouraged to tailor the presentations and incorporate unit specific information when necessary. When used, ensure locally developed training meets these standards. Initial training presentations are often specific to each unit, and therefore units are expected to develop their own presentations. However, sample presentations are available upon request.

A2.1. During Local Information Protection Management Evaluations (LIPME), 96 TW/IP will compare your annual program with this training plan to validate information protection training standards are being followed.

Table A2.1. Information Protection training standards. The far right columns indicate the training standard applies to “C” for cleared personnel and “U” for uncleared personnel.

1. POLICY AND PROGRAM MANAGEMENT	REFERENCE		
a. Policy	AFI 31-401, Chapter 1		
(1) Policy	AFI 31-401, para 1.1	C	U
(2) Philosophy	AFI 31-401, para 1.2	C	
b. Program Management	AFI 31-401, para 1.3	C	U
(1) Terms and Definitions	AFI 31-401, Attach 1	C	
(a) Personnel Security	AFI 31-501	C	U
(b) Industrial Security	AFI 31-601	C	
(c) Operations Security (OPSEC)	Training provided by Eglin OPSEC PM	C	U
(d) Emission Security (EMSEC)	AFI 33-203	C	
(e) Computer Security (COMPUSEC)	AFI 33-202	C	U
(f) Physical Security	AFI 31-101	C	U
(g) Freedom of Information Act (FOIA)	DOD 5400-7/AF Supplement	C	U
(h) Privacy Act	AFI 33-360, Air Force Privacy Act Program	C	U
(i) Security and Policy Review	AFI 35-102	C	
(j) Foreign Disclosure	AFI 16-201	C	
(k) Remanence Security	AFMAN 33-282	C	
c. Special Types of Information	AFI 31-401, Chapter		

	1		
(1) NATO (Awareness)	AFI 31-406	C	U
(2) Controlled Unclassified Information	AFI 31-401, Attach 3	C	U
(3) STINFO	AFI 61-204	C	
d. Security Incidents	AFI 31-401, Chapter 9		
(1) General Policy	AFI 31-401, para 9.1.1.	C	
(2) Corrective Actions and Sanctions	AFI 31-401, para 1.8	C	
(3) Reporting of Incidents	AFI 31-401, para 9.8	C	
(4) Reporting Requirements	AFI 31-401, para 9.8	C	
2. ORIGINAL/DERIVATIVE CLASSIFICATION	AFI 31-401, Chapter 2		
a. Policy	AFI 31-401, para 2.1	C	
b. Definition	AFI 31-401, para 2.2.1	C	
3. DECLASSIFICATION AND DOWNGRADING	AFI 31-041, Chapter 3		
a. Policy	AFI 31-401, para 3.2	C	
b. Declassification Authority	AFI 31-401, para 3.1	C	
c. Declassification Systems	AFI 31-401, para 3.2	C	
d. Automatic Declassification	AFI 31-401, para 3.4	C	
e. Public Release	AFI 31-401, para 3.8	C	
f. Downgrading	AFI 31-401, para 3.9	C	
4. FOREIGN GOVERNMENT INFORMATION	AFI 31-401, Chapter 4		
a. Policy and Procedures	AFI 31-401, para 4.5.	C	
b. Communication with Foreign Governments	AFI 16-201	C	
5. MARKING	AFI 31-401, Chapter 4		
a. General Provisions	AFI 31-401, para 4.1	C	
b. Required Markings on Documents	AFI 31-401, para 4.2	C	
c. Marking Special Types of Documents and Materials	AFI 31-401, para 4.3	C	
d. Marking Special Types of Materials	DoDM 5200.01 V3 Encl 3	C	
e. Declassification and Downgrading Markings	AFI 31-401, para 4.2.8	C	
f. Foreign Government Information	AFI 31-401, para 4.5	C	
6. SAFEGUARDING	AFI 31-401, Chapter 5		
a. Control Measures	AFI 31-401, Chapter 5	C	
b. Access	AFI 31-401, para 5.2	C	U

c. Safeguarding	AFI 31-401, Section 5C	C	U
d. Administrative Controls	AFI 31-401, para 5.8	C	
e. Storage	AFI 31-401, para 5.17, 5.18	C	U
f. Reproducing Classified Material	AFI 31-401, para 5.15.1, 5.24	C	
h. Disposition and Destruction	AFI 31-401, para 5.27.2.5	C	
7. TRANSMISSION AND TRANSPORTATION	AFI 31-401, Chapter 6		
a. Methods	AFI 31-401, Chapter 6	C	
b. Preparation of Material for Transmission	AFI 31-401, Chapter 6	C	
c. Escort or Hand-Carry of Classified Material	AFI 31-401, Chapter 6,	C	
8. SPECIAL ACCESS PROGRAMS (SAP)	AFI 31-401, Chapter 7		
a. Policy	AFI 31-401, para 7.1	C	
9. SECURITY EDUCATION AND TRAINING	AFI 31-401, Chapter 8		
a. Policy	AFI 31-401. Para 8.1	C	U
b. Initial Orientation	DoD 5200.01-M, Vol 3	C	U
c. Special Requirements	DoD 5200.01-M, Vol 3	C	
d. Continuing Training	AFI 31-401, Section 8D	C	
e. Access Briefings	AFI 31-401, para 8.11	C	
f. Termination Briefings	AFI 31-401, para 8.12	C	
g. Program Oversight	AFI 31-401, Section 8F	C	
10. ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION	AFI 31-401, Chapter 9		
a. Policy	AFI 31-401, para 9.1	C	U
b. Reporting	AFI 31-401, para 9.7	C	U
c. Inquiry/Investigation	AFI 31-401, para 9.8, 9.10	C	
d. Verification, Reevaluation, Damage Assessment	AFI 31-401, para 9.9	C	
e. Management and Oversight	AFI 31-401, para 9.11	C	U