BY ORDER OF THE COMMANDER
452D AIR MOBILITY WING

452 AIR MOBILITY WING
INSTRUCTION 16-1404

29 FEBRUARY 2024

Operations Support

INFORMATION SECURITY PROGRAM

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 is no releasability restrictions on this publication.

OPR: 452 AMW/ IP

Certified by: 452 AMW/CC
(Col Daniel J. Ebrecht)

Supersedes: 452AMWI16-1404, 27 September 2018

Pages: 19

This instruction implements Air Force Policy Directive (AFPD) 16-14, Security Enterprise Governance. It standardizes the procedure for handling, controlling, and safeguarding of classified material/information within all organizations of the 452nd Air Mobility Wing (AMW). These procedures do not apply to Special Access Programs that are governed by other instructions. These procedures apply to all personnel within the 452 AMW that handle/control classified information, controlled unclassified information (CUI) or who have a security clearance eligibility. Use these procedures with DOD Manual 5200.01V1/AF Manual 16-1404 V1-3 DOD Information Security Program, DODM 5200.02/DAFMAN16-1405, Personnel Security Program Management; DoDI 5200.28/DAFI16-1403, Controlled Unclassified (CUI); AFI 16-1402, Air Force Counter-Insider Threat Program Management; DODM5220.22/AFMAN16-1406V2, National Industrial Security Program: Industrial Security Procedures for Government Activities. This wing instruction is intended to standardize the 452nd Air Mobility Wing, Information Protection (IP) functions. If an organization has special handling needs or concerns not covered by this AMWI, each commander is encouraged to write additional plans and procedures in conjunction with 452 AMW/IP. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, Management of Records; and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR)listed above using the AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363,

Management of Records, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

1. Responsibilities. The policies and procedures outlined throughout this instruction apply to all personnel assigned, supported, or attached to the 452nd Air Mobility Wing.

1.1. Commanders will:

1.1.1. Developed unit security process, procedures, or plans.

1.1.2. Appoint individuals to perform security duties (i.e. Primary and Alternate Security Assistants, Preliminary Inquiry Officials, etc.), as required. Unit commanders or staff agency chiefs will appoint, in writing, a primary and at least one alternate security assistant. Use the current appointment letter template posted on the Wing IP SharePoint. Provide a copy of the letter to Wing IP.

1.1.3. Ensure security incidents and potential compromises of classified material are properly investigated.

1.1.4. Ensure all assigned unit personnel in/out process through the security assistant. Include the security assistant in the unit in/out processing checklist.

1.1.5. Integrate contractors into the unit's security program.

1.2. Supervisors will:

1.2.1. Ensure personnel complete initial, refresher and specialized Security Education and Training.

1.2.2. Coordinate with the security assistant to ensure civilian employment positions are designated correctly for position sensitivity. Assist the security assistant and enforce the timely submission of periodic reinvestigations or new investigation requirements.

1.2.3. Evaluate cleared personnel to ensure they remain trustworthy for access to classified information. Report knowledge of adverse information to the Commander and assist the Commander in determining appropriate measures when an individual's action reflects non-compliance with adjudication guidelines.

1.2.4. Ensure all newly assigned personnel/employees in-process and out-process through the security assistant.

1.2.5. Verify newly assigned individual's personnel security eligibility and access status with the security assistant and ensure access is granted only at the appropriate level and only when needed to accomplish duties/job assigned.

1.2.6. Ensure subordinates are trained in, understand, and follow work center security procedures and requirements of the information security program.

1.2.7. Report subordinates adverse conduct, or other derogatory information that could have a bearing on their continued eligibility for access to classified information or occupy a position of trust. Any derogatory information will be reported to the respective Unit

Commander, security assistant and to the Personnel Security Office (452 AMW/IP 655-3259/3428).

1.3. Individuals will:

1.3.1. Comply with security requirements and security responsibilities to prevent unauthorized disclosure of classified information.

1.3.2. Not accept custody of classified material or participate in classified discussions for which they are not properly cleared.

1.3.3. Report, without delay, to their Unit Commander or security assistant:

1.3.4. When they become aware of or believe that there may have been a compromise, loss, unauthorized disclosure, or other infraction affecting the safeguarding of classified information.

1.3.5. Any information that could adversely reflect on their or a co-worker's suitability for continued access to classified information or controlled unclassified information.

1.3.6. Individuals notified to complete an SF 86, *Questionnaire For National Security Position,* are responsible for completing and submitting a complete questionnaire to the security assistant for quality review/completeness.

1.3.7. Individuals will complete the SF86 as soon as possible (not to exceed 30 days from notification).

1.4. The Security Assistant will:

1.4.1. Act as the single point of contact for the unit's security program to outside organizations. Advise and assist the Commander and unit personnel on security matters under their purview.

1.4.2. Liaison with Unit Training Manager (UTM) to ensure security training is conducted and completion is tracked. Provide or request assistance from outside agencies in providing specialized security training (i.e. derivative classifiers, courier briefings, foreign travel briefings, preliminary inquiry or investigating officials, etc.). Advise the Commander on the status of the unit's security training program. Along with the UTM, ensure training is documented and records are properly maintained.

1.4.3. Implement the personnel security program and provide support to the servicing security activity (452 AMW/IP). Use the Defense Information Systems for Security (DISS) to review the status of personnel security clearances/eligibility. Notify the Commander of any unfavorable information that could impact an individual's security clearance or access to classified information.

1.4.4. All permanently assigned military and civilians will be in-processed (relationship added) as "owning." All contractors on a classified contract (DD Form 254) that are assigned to the unit will be in-processed as "servicing". Personnel will not be granted access to classified material prior to DISS indoctrination. The unit security assistant will not indoctrinate members into DISS until all required security training has been accomplished. All non-SCI access will match the Security Access Requirement (SAR) code on the unit manning document and not necessarily the eligibility reflected in DISS. All non-SCI access will be removed from DISS prior to out-processing.

1.4.5. Conduct access and termination briefings for government civilians and military personnel. The security assistant will obtain commanders/directors approval prior to granting access in DISS.

1.4.6. Ensure secure areas/rooms have requisite security approvals prior to storing and/or processing classified information.

1.4.7. Act as the conduit between the 452 AMW/IP and unit personnel for clearance and access issues.

1.4.8. Oversee the periodic purge of files in the classified storage containers/areas and, as a minimum, during the designated annual clean-out days. In conjunction with each retention review, ensure appropriate downgrading/declassification actions are taken.

2. Access. Use DISS as the primary source for confirming and recording a commander's approval for an individual to have access to classified information.

2.1. Classified information shall only be released to individuals who meet all of the following requirements:

2.1.1. Possess a valid personnel security eligibility/clearance (equal to or greater than the information being disclosed) that has been verified in DISS.

2.1.2. Possess a valid-need-to-know and granted access (validated in DISS) for the information in order to perform a lawful and authorized government function.

2.1.3. Have a signed SF 312, *Classified Information Nondisclosure Agreement,* verified through DISS or accomplished in person.

2.2. Verify identity by checking a government issued identification card.

2.3. The unit security assistant will verify these elements. Personal assurance shall not be accepted for personnel security eligibility and access verification.

3. Visitors needing access to classified: Official visitors who require access to classified information or facilities that contain classified information must be vetted in DISS or its successor system to ensure proper eligibility and execution of the SF 312. This can be accomplished via a DISS Visit Notification. Need-to-know is established by the organization in possession of the classified information. For contractors, need-to-know is established via DD Form 254. Commanders must establish processes for detailing localized actions specific to the organization. In the few cases where visit requests are not routed through DISS, unit security assistants will ensure personnel are properly cleared prior to classified access; however, this will be limited via the show-up and look-up technique using DISS.

3.1. Receiving Visitor requests:

3.1.1. Incoming visit requests can be sent to the unit hosting the visit via squadrons/units Security Management Office (SMO) in DISS.

3.2. Visit authorization letters will not be used to pass security clearance information unless DISS is not available but must be validated using DISS.

3.2.1. Visit requests for contractors:

3.2.1.1. Classified contractor visit must be transmitted through DISS, accompanied by a Defense Department (DD) Form 254, *Department of Defense Contract Security Classification Specification*, listing March Air Reserve Base as a contract performance location.

3.2.1.2. Commanders must maintain accountability of all contractors requiring access to classified information (collateral, SCI and SAP). This includes maintaining a copies of the associated DD Forms 254, DoD Contract Security Classification Specification, visit notifications for all contractor employees working in the March ARB, key management memorandums, local security policy acknowledgments conveyed to the contractor, and applicable Statements of Work/Performance Work Statements. These documents must be presented for inspection upon request. Upon receipt of visit requests, integrated visitor groups, requiring access to classified, will be "Serviced" in DISS.

3.3. The Chief of Information Protection (452 AMW/IP) is delegated the responsibility to designate contractors as "Visitor Groups" in accordance with DoDM5220.22V2_AFMAN16-1406V2, paragraph 2.8. The Visitor Group designation will be incorporated in the security requirements provided to the contracts Facility Security Officer (FSO).

3.4. The visit sponsors, with the assistance and advice of the security assistant, will arrange for March ARB and facility access.

3.5. Visitors with classified material arriving after hours should be directed to the March Air Reserve Base (MARCH ARB) Command Post in building 470 for temporary overnight storage.

4. Classified Meetings: Prior to conducting a classified meeting, the individual(s) hosting the meeting will contact the security assistant and ensure proper procedures are followed.

4.1. Room/Areas must be checked to determine if sound will travel through the walls/vents/doors. If discernable sound can be heard outside the meeting area, a cleared monitor **must** be posted outside the door/vent/wall to ensure all loitering and/or unauthorized entry is prohibited.

4.2. The security clearance/eligibility and access of all attendees must be verified prior to the meeting. Visit requests are to be on file with the security office for all visiting participants.

4.3. Prior to the start of the meeting, the meeting area will be checked by the host for suspicious objects or obvious recording devices.

4.4. At the beginning and end of the meeting, the facilitator of the meeting must announce classification level of information to be discussed.

4.5. Note taking should be discouraged. If note taking is necessary, all participants must understand that notes become classified working papers and must be marked and protected accordingly.

4.6. All presentation materials must be marked properly in accordance with DODM5200.01V2/AFMAN16-1404V2.

4.7. Completion of the checklist in DODM5200.01V3/AFMAN16-1404V3 Volume 3 is directed.

5. Hand-carrying of Classified Material.

5.1. Hand-carrying classified material from one building to another on March ARB:

5.1.1. Enclose classified material in an inner and outer wrapper/container.

5.1.2. The inner container will be marked with the highest classification of material inside.

5.1.3. The outer container will not contain any external classification markings.

5.1.4. Close or seal the containers to prevent loss or inadvertent access to the classified contents.

5.1.5. All couriers will be briefed by the security manager on courier responsibilities and will not make intermediate or convenience stops with classified material in their possession.

5.2. Hand-carrying of Classified Material off March ARB.

5.2.1. Hand carrying classified material off the March ARB will be done as a last resort, only after considering alternatives such as mailing or electronic transmission. When approved:

5.2.2. A courier must carry a DD Form 2501, *Courier Authorization,* when traveling off the March ARB or aboard commercial passenger aircraft.

5.2.3. Material will be double wrapped and addressed as if it were being mailed.

5.2.4. The DD Form 2501, signed by the 452 AMW/IP will not exceed two years.

5.2.5. Couriers will coordinate security arrangements with the security assistant and destination when leaving the local area, using commercial transportation, or a trip that requires an overnight stay.

5.2.6. Couriers will be briefed and must acknowledge their security responsibilities. The security assistant or supervisor will conduct and record these briefings.

6. Reproduction of Classified Material. Reproduction of classified material should only be done if absolute necessary. Contact your Unit Security Assistant for assistance prior to reproducing any classified information. Reproduction will only be accomplished on equipment specifically designated and approved for classified reproduction. Additional reproduction requirements follow:

6.1. Personnel will maintain constant surveillance and control over reproduction equipment and area where the equipment is located when reproducing classified material.

6.2. Personnel will follow the classified reproduction rules posted on the equipment and ensure the equipment is cleared of any latent images after classified reproduction.

6.3. Account for all originals, copies, and waste before departing the copy area.

7. Destruction. Classified material will be destroyed when no longer required for operational requirements or by law. The security assistant will obtain necessary approvals and ensures devices have been approved for the destruction of classified material by referencing the National Security Agency/Evaluated Products List (NSA/EPL). Contact 452 AMW/IP at 655-3428 for assistance. Other destruction requirements are as follows:

7.1. The 452 Air Mobility Wing annual clean-out day will be 15 August of each year. The focus of this event will be a retention review and the disposal of all classified material that is obsolete or unnecessary. This does not preclude the units from establishing their own additional clean out days. Document when clean out is conducted. The clean out event will be recorded in a memorandum for record by each squadron.

7.2. Excess material no longer required by law or mission accomplishment will be identified and subsequently destroyed.

7.3. During the retention review, complete any downgrading/declassification actions noted on the material.

8. Security Incidents. All personnel are personally responsible for the protection of classified information. Reporting procedures for security:

8.1. Any person who has knowledge of the loss or possible compromise of classified information will immediately report such facts to the security assistant, immediate supervisor, or the Commander.

8.2. A person finding classified material unattended or improperly stored is responsible for protecting it until the responsible custodian or other such official regains proper custody.

8.3. The security assistant will advise the Commander on inquiry/investigative requirements. The security assistant is responsible for reporting the incident to the 452 AMW/IP Office no later than the first duty day following the reporting of the incident.

8.4. The Commander or appointing authority will appoint the preliminary inquiry official IAW DODM 5200.01V3/AFMAN16-1404V3 for all security incidents.

8.5. The inquiry official appointment letter will be accomplished and signed by the appointing authority. Upon notification of appointment, the inquiry official will make an appointment with the 452 AMW/IP office for a briefing on the incident and their responsibilities. The inquiry official will provide a copy of their appointment letter to the 452 AMW/IP.

8.6. The inquiry official will prepare a written report. The report will be routed through the 452 AMW/IP to the appointing official. The Chief, Information Protection will provide technical reviews of the report.

8.7. The appointing official will close incident in IAW DODM 5200.01V3/AFMAN16-1404V3 and will be forwarded the report closure 452 AMW/IP.

9. Security Education and Training. Commander or equivalents must ensure that each individual receives security education and training throughout their duty assignment.

9.1. Security assistants or Unit Training Managers will utilize a system of record that identifies the names of personnel trained, subjects presented, and date(s) training was completed.

9.2. Newly appointed Security Assistants will complete training within 60 of their appointment. At a minimum, the following training is required.

9.2.1. Local Security Assistant Training (Contact 452 AWM/IP to schedule a session) Introduction to Information Security IFO11.13 **https://www.cdse.edu/catalog/elearning/IF011.html**)

9.2.2. Classified Storage Requirements (Squadrons with classified storage only) (**https://securityawareness.usalearning.gov/cdse/multimedia/shorts/csr/story_html5.html**)

9.2.3. Introduction to Personnel Security PS113.16 (**https://www.cdse.edu/catalog/elearning/PS113.html**)

9.2.4. Adverse Action Reporting (**https://securityawareness.usalearning.gov/cdse/multimedia/shorts/adverse/story_html5.html**)

9.2.5. Insider Threat Awareness (**www.securityawareness/usalearning.gov/itawareness/story.html**)

9.2.6. Identifying and Safeguarding Personally Identifiable Information (PII) DS-IF101.06 (**http://www.cdse.edu/catalog/elearning**)

9.2.7. DoD Mandatory Controlled Unclassified Information (CUI) Training (**https://securityhub.usalearning.gov/index.html**)

9.2.8. Introduction to Industrial Security IS011.16 (Squadrons with contractors only) (**https://www.cdse.edu/Training/eLearning/IS011/**)

10. Safeguarding North Atlantic Treaty Organization (NATO) Classified. No NATO classified information is currently being stored within any organization. Contact your Unit security manager should a requirement arise to store, discuss, or process NATO classified material. All personnel that require "Access" will receive the NATO Security Briefing and document the training utilizing the NATO Brief-Rebrief-Debrief form, which will be maintained by the Security Manager. Training will be documented on the annual training log.

11. Review of Personnel Security Clearance Status. The security assistants will conduct a monthly review of the unit's DISS reports to monitor the Continuous Enrollment/Vetting status of assigned personnel. The security assistant will be responsible for requesting initiation of an SF86, *Questionnaire For National Security Position,* on behalf of the commander.

11.1. SF86 initiation request will be submitted to 452 AMW/IP over SharePoint. The security assistant will maintain tracking of the request until a CE/V Enrollment is updated in the DISS Person Summary or change the investigation has been opened.

11.2. Individuals notified to complete an SF 86 are responsible for completing and submitting a complete questionnaire to the security assistant for quality review/completeness. The security assistant will review the SF86 and provide guidance/assistance in the completion of the SF86. The security assistant will direct individuals to sign and release the SF86 if no issues are discovered.

11.3. The individual will complete the SF86 as soon as possible (not to exceed 30 days from notification).

12. Open Storage/Secure Room Request: Commanders and equivalents must justify, in writing, the need for secure room open storage of classified materials that will not fit inside a GSA approved security container. Secure room/open storage will not be approved for the storage of products such as paper documents, optical media, and other devices or products that will fit inside a GSA approved security container. Commanders and equivalents are responsible for vault and

secure room funding and work order submission through appropriate channels. Security Assistants will coordinate open storage justification, approval, and certification with 452 AMW/IP**.**

12.1. Request for establishment of Secure Rooms will be made through the Chief of Information protection (452 AWM/IP). IAW DoDM 5200.1/AFMAN 16-1404, Volume 1, Enclosure 2, paragraph 7n(5)(h), the authority to certify/approve open storage areas/secure rooms is delegated to the Chief, Information Protection.

12.2. 452 AMW/IP or the requesting squadron will obtain support from 452 Civil Engineer (452 CE) to certify construction standards of the rooms/facilities.

12.3. 452 AMW/IP or the requesting squadron will obtain support from 452 Security Forces Squadron (SFS) for access control and intrusion detection systems March ARB or validation. Reference guidance in accordance with DoDM5200.01V3/AFMAN 16-1404V3, *DoD Information Security Program: Protection of Classified Information*, Appendix to Enclosure 3.

12.4. 452 AMW/IP will develop and coordinate certification packages. Once approved, rooms will undergo yearly review during the scheduled 452 AMW/IP squadron assessments.

12.5. Squadrons/units operating approved secure rooms are responsible for ensuring that their local security instructions, plans and/or processes include the guidance required by DODM5200.01V1/AFMAN16-1404V1, Enc 2, **para 7**n(7)(b). See enclosure 3.

12.6. Recertification. Recertification will occur every 5 years. 452 AMW/IP will obtain 452 CE and 452 SFS validation on the requirements that correspond to their area of responsibility.

12.7. Commanders will notify the Information Protection Office when approved open storage areas/secure rooms which are no longer required, the mission changes, and/or when modifications are planned for the approved space.

12.8. Security Containers:

12.8.1. IAW DoDM 5200.1/AFMAN 16-1404, Volume 1, Enclosure 2, paragraph 7n(6)(b)3h and Volume 3, Enclosure 3, **paragraphs 10**. & 11, commanders must create processes to ensure personnel with knowledge of combinations to security containers, secure rooms and vaults are maintained and combinations are changed.

12.8.2. Commanders will ensure security containers no longer needed are inspected to ensure they do not contain classified and controlled unclassified information, the combination is reset to the factory setting of 50-25-50, and turned into the Defense Reutilization Marketing Office.

12.8.3. Safe lock-outs and lock replacements are managed at the expense of the organization.

13. Counter Insider Threat. AFI 16-1402, Counter-Insider Threat Program Management, establishes a framework to integrate policies and procedures to detect, deter, and mitigate insider threats to national security and Air Force assets and establishes implementing guidance. The AF C-InT helps protect our most critical assets – personnel, information, and resources from a broad spectrum of insider threats (workplace violence, espionage, fraud, unauthorized disclosure, and more). 452 AMW/IP is Wing Point of Contact for C-InT.

13.1. Commanders and Directors shall report, within five (5) days of any incident meeting one or more of the Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) threshold-level events to 452 AMW/IP for submission to the AFRC Point of Contact (AFRC/IP). The thirteen DITMAC reporting thresholds are: serious threat, allegiance to the United States, espionage/foreign considerations, personal conduct, behavioral considerations, criminal conduct, unauthorized disclosure, unexplained personnel disappearance, handling protected information, misuse of information technology, terrorism, criminal affiliations, and adverse clearance actions.

14. Emergency Protection, Removal and Destruction of Classified Material. The following procedures/guidance are provided to be used during emergency situations in regard to the protection of collateral classified information. When time is of the essence, material may be secured in any available security container, evacuated with the holder, or as a last resort, left behind.

14.1. At a minimum:

14.1.1. In case of fire, natural disaster, civil disturbance, or overt attack (e.g., active shooter or terrorist attack), and time permitting, secure classified information in a GSA-approved security container within the immediate work area. Do not risk injury or loss of life to secure classified information.

14.1.2. If the emergency is such that classified material cannot be secured, the holder of all such material will secure it on their person and evacuate the area immediately. The holder will secure the classified material until the emergency is terminated or take action to have it temporarily secured in an approved GSA-approved security container. Immediately following the emergency, personnel will return to their work areas and check for unsecured classified information.

14.1.3. Under no circumstances will the classified material be transported off base or to private living quarters.

14.1.4. Planners must ensure deployment/redeployment plans address how to properly safeguard classified information during military operations. This includes planning for the emergency destruction of classified information at deployed locations and the funding/acquisition of applicable destruction equipment and devices for applicable unit type code LOGDETs.

14.1.5. Conspicuously post a copy of specific organizational emergency protection procedures or task cards in the immediate vicinity of any GSA-approved security containers containing classified information or in a conspicuously location within vaults or approved open storage areas.

14.2. Each activity that processes or stores classified information must develop an emergency action plan (EAP) for protection of classified material and recovery post incident. Units with Secure rooms/open storage will incorporate EAPs into their Emergency Response Notebook (ERN) as part of the March ARB Emergency Management Plan (IEMP). In addition, these procedures should be part of the annual exercise of emergency plans in accordance with DoDM5200.01V3_AFMAN16-1404V3, enclosure 2, para 10.

14.3. Emergency Action Plans for the protection of collateral classified. Templates are located in Attachment **2** and **3** to assist in the preparation of EAPs. Units can tailor the templates as needed.

14.3.1. Emergency Action/Protection Plan for Classified Material (Secure Room/Open Storage), **Attachment 2**: This templated can be tailored for the use with approved secure rooms. It's essential that pre-planning take place in order for the actions listed to be effective. The location of March ARB, emergency actions procedures should be tailored to provide steps for earthquake preparedness and recovery.

14.3.2. Emergency Action Plan for the protection of collateral classified (Areas with Security Containers), **Attachment 3**. This template can be tailored and must be within all areas that container a security container (GSA approved safe) that are used for the protection of classified.

DANIEL J. EBRECHT, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 16-1402, Air Force Counter-Insider Threat Program Manager

AFMAN33-363, *Management of Record*

DoDM 5200.02/AFMAN 16-1405, Personnel Security Program Management

DoDM5200.1 V1/AFMAN 16-1404V1, *DoD Information Security Program: Overview, Classification and Declassification*

DoDM5200.1 V2/AFMAN 16-1404V2, *DoD Information Security Program: Marking of Classified Information*

DoDM5200.1, V3/AFMAN 16-1404V3, *DoD Information Security Program: Protection of Classified Information*

DODM5220.22/AFMAN16-1406V2, National Industrial Security Program: Industrial Security Procedures for Government Activities

DoD15200.48/DAFI16-1403, *Controlled Unclassified Information (CUI)*

Adopted Forms

AF Form 847, *Recommendation to change for Publication*

DD Form 254, *Department of defense Contract security Classification Specification*

DD Form 2501, *Courier Authorization*

SF 86, *Questionnaire For National Security Position*

SF 312, Classified Information Nondisclosure Agreement

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRCVA—Air Force Reserve Command Visual Aid

AFRIMS—Air Force Records Information Management System

ARB—Air Reserve Base

AMW—Air Mobility Wing

AMWI—Air Mobility Wing Instruction

CAC—Common Access Card

CC—Commander

CDSE—Center for Development of Security Excellence

CE—Civil Engineer

CIP—Chief, Information Protection

COMSEC—Communication Security

COR—Contracting Office Representative

CP—Command Post

CS—Communication Squadron

CUI—Controlled Unclassified Information

DD—Defense Department

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDM—Department of Defense Manual

EPL—Evaluated Products List

FSO—Facility Security Officer

GSA—General Services Administration

IAW—In Accordance With

IP—Information Protection

DISS—Joint Personnel Adjudication System

LAN—Local Area Network

LES—Law Enforcement Sensitive

MARCH ARB—March Air Reserve Base

NATO—North Atlantic Treaty Organization

NSA—National Security Agency

OCA—Original Classification Authority

OF—Optional Form

OPM—Office of Personnel Management

OPR—Office of Primary Responsibility

OVI—Operation Visual Inspection

PED—Portable Electronic Devices

PM—Project Manager

POC—Point of Contact

PR—Periodic Reinvestigation

PWFD—Personal Wearable Fitness Device

RDS—Records Disposition Schedule

SAP—Special Access Program

SEAD—Security Executive Agent Directive

SF—Standard Form

SFS—Security Forces Squadron

SIPRNet—Secret Internet Protocol Router Network

SJA—Staff Judge Advocate

SM—Security Manager

SMO—Security Management Office

STE—Secure Telephone Equipment

SVRO—Secure Voice Responsible Officer

UCNI—Unclassified Controlled Nuclear Information

USB—Universal Serial Bus

V—Volume

Attachment 2

EMERGENCY ACTION/PROTECTION PLAN FOR CLASSIFIED MATERIAL (Secure Room/Open Storage)

1. PURPOSE. To establish procedures for the protection, removal and/or destruction of classified material located in building _____, room _____, on March ARB—. These procedures will be executed in case of emergency, such as fire, natural disaster, civil disturbance, or terrorist activities.

2. BACKGROUND—. A fire, a major accident response, natural disasters, civil disturbances, or terrorist activities may require relocation of classified material. Locally, earthquakes are the concern from a natural disaster standpoint. The responsibility for protection, removal or destruction of classified material under emergency conditions rests with the owner/user's organization.

Although the importance of protecting collateral material cannot be discounted, it must be accomplished in such a way as to minimize the risk of loss of life or injury to employees.

This plan is in accordance with DoDM 5200.1V3/AFMAN16-1404V3, Enclosure 2, para 10, enclosure 3 para 9b.

3. PRE—PLANNING

Verified on	*ROLES/ACTIONS*
	The units response team: Security Assistant (SA)/Facility Manager (FM)
	Primary/alternate staging locations: Bldg XXX evacuation rally point
	Facility points of contact: Security Assistant/Facility Manager
	Supplies/equipment needed: Emergency Response Notebook (ERN), (suggested: burn bags, NSA approved shredders/degausser) XXX, XXX, XXX
	March ARB/facility maps: Located in Emergency Response Notebook
	Unit response team communications needs: (Suggested LMR), XXX, XXX
	Container/classified material inventory: Unit specific list placed in ERN
	Transportation requirements: TBD by unit
	Verify pre-planned actions are viable, valid and completed

4. ACTIONS: Classified information will only be relocated at the direction of the commander or senior office official—normally, only as a last resort. Do not risk loss of life to complete a relocation action!

A. If An Evacuation Is Ordered (Leaving Classified In—Place): If there is no imminent danger to employees.

INITIALS	*ACTIONS*	*OPR*
	Thoroughly check workspaces for unsecured collateral material prior to departure.	SA/FM
	Secure collateral material in authorized containers before evacuation.	Custodian SA/FM
	Evacuate the area	All

	If authorized storage is not immediately available, attempt to carry collateral material from the area, seeking assistance from other cleared personnel, as needed.	SA/FM
	Should circumstances require that some collateral material be left unattended, immediately report this fact to the local security office.	SA/FM
	The custodian/holder will notify the senior government official, or incident commander and the Recovery Team at the central evacuation point that classified materials has been left unsecured in the work area. The holder will provide the location, type of classified (i.e., media, documents, etc.) and the approximate amount.	Custodian, SA/FM
	Upon cancellation of the emergency situation and when given the authorization to do so, employees will return to the work area and inventory any unsecured collateral material, reporting the results of this action to the security office. As appropriate, custodian, SA/FM will also check security containers, secure rooms, and vaults for evidence of forced entry.	Custodian, SA/FM
	If There Is Imminent Danger To Employees:	
	Evacuate immediately, leaving collateral material in place. Under no circumstances should employees endanger themselves attempting to secure or remove classified information from workspaces.	Custodian, SA/FM
	When possible, report the existence of unattended collateral material to the unit Recovery Team, supervisor, who will then, as conditions allow, arrange for monitoring of the area perimeter.	Custodian, SA/FM

B—.Should Destruction Of Collateral Material Be Warranted (E.G., Enemy/Terrorist Attack):

INITIALS	ACTIONS	OPR
	When possible, collateral material should be destroyed using equipment previously authorized for classified destruction (e.g., burn bags, approved shredders and degaussers).	Custodian SA/FM
	As possible, document the destruction of all accountable collateral material by noting, at a minimum, the accountability number (e.g., barcode or serial number).	Custodian SA/FM
	Report the overall destruction totals to 452 AMW/IP.	Custodian

C—.IF THE RELOCATION OF CLASSIFIED MATERIAL IS ORDERED:

INITIALS	ACTION	OPR
	Place documents to be transported to relocation site in cardboard boxes or other suitable containers.	Custodian
	Seal and/or lock the boxes or other suitable containers.	Custodian
	Take boxes or other suitable containers containing classified material to relocation site. Use private vehicles or government transportation, as necessary.	Custodian, SA/FM

	Ensure all classified material reached the intended destination, it is properly accounted for, and it is secured or released to an authorized individual.	Custodian, SA/FM
	The custodian/holder will notify the senior government official, or incident commander and Recovery Team at the central evacuation point that they are holding classified material. Protect the classified material until the emergency is terminated or take action to secure it in an approved security container. Individual is responsible for returning the classified information to the proper security container unless otherwise directed	Custodian SA/FM

D. POST—INCIDENT RECOVERY TEAM ACTIONS:

INITIALS	ACTION	OPR
	Receipt/account for all classified materials.	Custodian SA/FM
	If the materials were relocated, return all classified materials to their authorized storage container or facility.	
	If unauthorized access is apparent and/or there is missing or compromised classified material, report the loss or compromise to 452 AMW/IP.	Custodian SA/FM
	Notify the commander or senior official of all actions.	SA/FM

PLACE THIS PLAN IN AREAS AUTHORIZED TO PROCESS OR STORE CLASSIFIED INFORMATION AND IN THE ERN

DO NOT REMOVE

Attachment 3

EMERGENCY PROTECTION PLAN FOR CLASSIFIED MATERIAL

(Areas with Security Containers)

Classified information will only be relocated at the direction of the commander or senior office official—normally, only as a last resort. Do not risk loss of life to complete a relocation action!

A fire, a major accident response, natural disasters, civil disturbances, terrorist activities or enemy action may require relocation of classified material. The responsibility for protection, removal or destruction of classified material under emergency conditions rests with the owner/user's organization.

Ref: DoDM 5200.1V3/AFMAN16-1404V3, Enclosure 2, para 10, enclosure 3 para 9b.:

1. THE SAFE CUSTODIAN OR RESPONSIBLE OFFICIAL WILL:

INITIALS	***ACTIONS***
	Increase vigilance during heightened threat conditions.
	Return any classified materials to their security container(s).
	Verify pre-planned relocation point(s) are still viable and haven't been compromised.

2. IF AN EVACTUATION IS ORDERED (LEAVING CLASSIFIED IN-PLACE):

INITIALS	***ACTIONS***
	Properly secure all classified material (without risk of injury or loss of life) before leaving the area.
	Evacuate the area.

3. IF THE RELOCATION OF CLASSIFIED MATERIAL IS ORDERED:

INITIALS	***ACTIONS***
	Place documents to be transported to relocation site in cardboard boxes or other suitable containers.
	Seal and/or lock the boxes or other suitable containers.
	Take boxes or other suitable containers containing classified material to relocation site. Use private vehicles or government transportation, as necessary.
	Ensure all classified material reached the intended destination, it is properly accounted for, and it is secured or released to an authorized individual.

4. POST INCIDENT/RECOVERY ACTIONS:

INITIALS	***ACTIONS***
	Receipt/account for all classified materials.

	If the materials were relocated, return all classified materials to their authorized storage container or facility.
	If unauthorized access is apparent and/or there is missing or compromised classified material, report the loss or compromise to the servicing Information Protection Office.
	Notify the commander or senior office official of all actions.

DO NOT REMOVE