BY ORDER OF THE COMMANDER
UNITED STATES AIR FORCES IN EUROPE

USAFE INSTRUCTION 33-201

10 JANUARY 2005

Communications and Information

OPERATIONAL DOCTRINE FOR SAFEGUARDING AND CONTROL OF WEAPONS STORAGE AND SECURITY SYSTEM (WS3)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: USAFE CSS/SCMI
(MSgt Dallas L. Webb Jr.)
Supersedes USAFEI33-201, 19 January 2001.

Certified by: HQ USAFE/A6N
(Col John C. Liburdi)
Pages: 31
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection.* This instruction applies to all personnel assigned to USAFE units with a WS3 mission. It does not apply to Air National Guard (ANG) or Air Force Reserve Command (AFRC) units. It outlines the control, accounting, and handling procedures for this material. Refer technical comments or recommended changes and conflicts between this and other publications on an AF Form 847, **Recommendation for Change of Publication,** through channels, to Information Assurance Branch (USAFE CSS/A6NI), Unit 3325 APO AE 09094-3325, with a courtesy copy to Munitions Division (HQ USAFE/A4WN), Unit 3050, Box 105, APO AE 09094-0105. Ensure that any local instructions or supplements are created in accordance with AFI 33-360 Volume1, Air Force Content Management Program-Publications. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at: **https://webrims.amc.af.mil.**

SUMMARY OF REVISIONS

This document has been revised and must be reviewed in its entirety. A thorough review by all personnel responsible for weapon storage and security system (WS3) communications security (COMSEC) material and procedures is required.

Section A—General and System Information

1. Responsibilities.

1.1. Director, National Security Agency (DIRNSA). The overall management of Weapons Storage and Security System (WS3) material, modules, and associated Communications Security (COMSEC) aids is the responsibility of DIRNSA/I551.

1.2. Cryptologic Systems Group (CPSG) has overall responsibility for procuring, manufacturing, and distributing two-person control erasable programmable read-only memory (EPROM) and Message Processor Hard Drives with associated software.

1.3. USAFE Logistics (HQ USAFE/A4WN), USAFE CSS WS3 Program Management (USAFE CSS/SCMM) and USAFE Information Assurance - COMSEC (USAFE CSS/CA635761) are responsible for developing and implementing command WS3 policy and doctrine.

1.3.1. HQ USAFE/A4WN is the controlling authority for WS3 material and maintains responsibility in accordance with AFI 33-215, *Controlling Authorities for COMSEC Keying Material (KEYMAT)*.

1.3.2. USAFE CSS/CA635761, Mission Systems Flight (USAFE CSS/SCMI) is responsible for the overall management of subordinate COMSEC accounts holding WS3 material.

1.3.3. Missions Systems Flight (USAFE CSS/SCMM) is responsible for managing and implementing guidance to Communications and Information Directorate (A6) field maintenance organizations for the WS3 system.

1.4. COMSEC managers (CM) and alternate managers manage all assigned WS3 COMSEC material assigned for use at their base or installation. CMs will conduct semi-annual Information Assurance self-assessments in accordance with AFI 33-230, *Information Assurance Assessment and Assistance Program.*

1.5. WS3 user agencies (UA) receive, store, account for, safeguard, control, and destroy WS3 COMSEC material in accordance with this instruction, AFI 33-211, *Communications Security (COMSEC) User Requirements*, AFI 33-211 USAFE SUP 1, and other applicable national, service, and command directives. UAs will appoint a COMSEC responsible officer (CRO) and alternate(s) according to AFI 33-211.

2. Exceptions. Submit written requests for exceptions to the provisions of this instruction to HQ USAFE/A4WN and USAFE CSS/CA635761. All requests for exceptions must be accompanied, in writing, by complete operational justification and an overall mission impact statement.

3. Terms and Definitions.

3.1. **Caretaker Status.** A term used for a WS3 installation that has been deactivated pending possible future reuse. A WS3 installation placed into caretaker status may be returned to operational use through the procedures contained in technical order (T.O.) 11N-50-1008, *Deactivation and Reactivation Instructions, Weapons Storage and Security System, AN/FSQ-143 (V)*.

3.2. **Coder Transfer Group (CTG).** The CTG is composed of six major components: Code Storage Modules (CSM), Unlock Modules, Recode Modules, Rekey Modules, Universal Release Code (URC) cards and the Code Transfer Unit. Combined they are capable of storing and transferring unlock codes and encoding keys. It also provides a means to enter and update vault identification numbers and time delay. All modules and code cards, except Unlocks, are produced and distributed by DIRNSA and unique to a specific WS3 installation.

3.2.1. **Code Storage Module (CSM).** A pair of “A” and “B” modules used to store maintenance or mass upload codes for subsequent transfer into the unlock modules via the Code Transfer Unit (CTU). As codes are transferred from the CSMs, they are electronically flagged to prevent reuse.

3.2.1.1. **CSM Access Code.** A unique, three-digit, access code entered into the CTU before doing operations involving the CSM. CSMs arrive from DIRNSA with an UNCLASSIFIED shipping access code of “FFF” Installed. The access code is changed prior to becoming the operational set using the CTU. This effective CSM access code is classified SECRET “Not Releasable to Foreign Nationals (NOFORN).

3.2.2. **Code Transfer Unit (CTU).** A transportable unit used to electronically transfer the DIRNSA generated codes from CSMs or manually enter universal release codes (URC) into the Unlock modules for operational use.

3.2.3. **Recode Modules.** A pair of “A” and “B” modules used to install new unlock codes into the Vault Processor (VP).

3.2.4. **Rekey Modules.** A pair of “A” and “B” modules used to install new encryption keys into the Authentication Unit (AU), Data Authenticator (DA), and Sensor Processor (SP).

3.2.5. **Universal Release Code (URC) cards.** A pair of hard copy codes, “A” and “B” pairs, that are manually entered into Unlock modules (via the CTU) and capable of unlocking all Weapons Storage Vault (WSV) on a specific WS3 installation. These codes are produced, placed within protective technologies packaging, and distributed by DIRNSA.

3.2.6. **Unlock Module.** Modules used to store individual maintenance or mass unlock codes transferred from CSMs (via the CTU) for access to WSVs. Unlock modules are also used to electronically store the hard copy codes manually entered (via the CTU) from URCs. Unlock modules have a storage capacity of either six maintenance unlock codes, one mass upload code, or a single URC.

3.3. **COMSEC Terminology.**

3.3.1. **Edition.** A full compliment of COMSEC materials. A WS3 edition consists of two sets, the Primary and Backup. Each of these sets contains both “A” and “B” Rekey, Recode and Code Storage modules and “A” and “B” Universal Release Code (URC) cards. The unique edition number ensures that information in the Recode modules matches that loaded within the Code Storage module and URC.

3.3.2. **Effective Edition.** A complete edition (“A” and “B” pairs) of primary and backup sets of Rekey, Recode and Code Storage Modules and Universal Release Code cards. The effective edition is the material currently installed in and used by the WS3.

3.3.3. **Reserve Edition.** A complete edition (“A” and “B” pairs) of primary and backup sets of Rekey, Recode and Code Storage Modules and Universal Release Code cards. The reserve edition is an on-hand spare edition used to supersede the current effective edition after compromise or during the scheduled rekey/recode operation.

3.4. **Controlled Components.** Major assemblies, or components within these assemblies, that require protection to prevent unauthorized access by a lone individual. These components are afforded protection under the two-person concept in accordance with this instruction and the specific item technical orders, 11N-50-1003 and 11N-50-1004, *Processor, Vault Control Group OL-398/FSQ-143(V) Weapons Storage and Security System AN/FSQ-143(V)*.

3.4.1. **Authentication Unit (AU).** A controlled component when GOLD EPROMs are installed. The AU is located in the WSV and stores keys for the encryption of vault status information being transmitted to the monitoring facilities. Rekey modules are used to transfer new keys to the AU.

3.4.2. **AU to VP Cable.** This cable interconnects the AU to the VP allowing the exchange of information, encryption of messages and transmission from the WSV to monitoring facilities.

3.4.3. **Data Authenticator (DA).** A controlled component when GOLD EPROMs are installed. A DA is located in both the Local Monitoring Facility (LMF) and Remote Monitoring Facility (RMF) and is used to decrypt status information transmitted via the AU or SP.

3.4.4. **Motor Starter.** The motor starter (reversing contactor starter) is located within junction box 2 of the WSV and controls application of AC voltage to the primary drive motor causing the vault structure to open or close as appropriate.

3.4.5. **Motor Starter Relays (K1, K2, K3).** The motor starter relays are located within junction box 1 of the WSV. Application of either the UP or DOWN push buttons cause these relays to close contacts on the motor starter causing upward or downward movement of the WSV.

3.4.6. **Message Processor (MP).** The MP is the computer that interprets all signals received from the WSV and other monitored system components. It translates signals and displays the appropriate message on the operator console along with activating audible alarms. The MP is not a controlled component until the Message Processor Hard Drive is installed.

3.4.6.1. **Message Processor Hard Drive (MPHD).** The Hard Drive is the controlled component which contains the computer operating system, WS3 specific alarm program and base maps. The MPHD is installed within the MP for operational use. This component is afforded special handling from “cradle to grave”.

3.4.7. **Vault Processor (VP).** A controlled component once a GOLD EPROM is installed. The VP is located in the WSV and stores the codes used to access the WS3. The VP also monitors and controls the mechanical operation of the WSV. The VP remains under two-person concept control until integrated circuit (IC) U18 is physically removed per applicable technical order. IC U18 is classified SECRET (NOFORN) until properly destroyed according to T.O. 11N-50-1004, *Processor, Vault Control Group OL-398/FSQ-143(V) Weapons Storage and Security System AN/FSQ-143(V)*. Unlike the DA, AU and SP, the VP retains its codes and controlled component status through power losses. If a vault processor is compromised, the operational codes which reside in IC U18 are also compromised; a system wide rekey/recode must be accomplished using the reserve set.

3.4.8. **Alternate Operating System Time Delay Relay**. The time delay relay is located within junction box 3 of the WSV and imposes a specified time delay on the Alternate Operating System before operation is allowed.

3.4.9. **Electronic Programmable Read-Only Memory (EPROM).** EPROMs are a field replaceable component of various electronic equipment sub-systems of the WS3. They are used to both store information and physically control basic equipment functions. They exist in two states of control, GOLD or BRONZE.

3.4.9.1. **GOLD EPROM.** Any EPROM produced and distributed by Cryptological Systems Group/ Force Protection (HQ CPSG/ZIW) for operational use in WS3 components. GOLD EPROMs require continuous protection from access by a lone individual to prevent compromise of system integrity.

3.4.9.2. **BRONZE EPROM.** Any EPROM that has not been controlled in a manner to prevent access by a lone individual. BRONZE EPROMs are installed in components for testing, shipping and storage purposes only. Operational keys or codes will never be loaded into a BRONZE EPROM.

3.4.10. **Selected Code Transfer Group Components.** The Code Storage, Rekey, and Recode Modules along with the Universal Release Code cards are controlled components as identified in TO 11N-50-1005, *Code-Transfer Group OX-69/FSQ-143 (V) Weapons Storage and Security System AN/FSQ-143 (V)*. Collectively these items contain all Unlock codes and encryption key values used by the WS3.

3.4.11. **Sensor Processor (SP).** A controlled component when GOLD EPROMs are installed. The SP is located in the Communication Interface Panel and stores keys for encryption of Interior Intrusion Detection System (IIDS) status information being transmitted to the monitoring facilities. Rekey modules are used to transfer new keys to the SP.

3.5. **Locked Vault.** A WSV is considered locked when the following criteria are met: Upon visual inspection the WSV is down, the Shelter Floor Plate is installed, and the “Locked” indicator illuminated on the Shelter Control Panel (SCP) or a Message Processor indication of code “0” is received at the monitoring facilities indicating a secure condition.

3.6. **Time Delay (TD).** The time delay is a minimum wait period, mandated by Allied Command Operations (ACO) Directive 80-6, Volume II, Part 2/HQ USEUCOM Directive (ED) 60-12, *Nuclear Surety Management for the WS3*, which is set in both the primary and alternate drive system that must be observed before the vault is raised.

3.7. **Two-Person Concept.** A requirement specified in DOD C-5210.41-M/Air Force Supplement, *Nuclear Weapon Security Manual,* and AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs,* to control access to nuclear weapons and related materials. Two-person concept team, two-person rule team, two-person policy rule team, and two-person team are synonymous terms identifying a team consisting of two personnel meeting the two-person concept requirements. This is not Two-Person Control (TPC) and WS3 material must not be associated with CJCSI 3260.01, *Joint Policy Governing Positive Control Material and Devices*. The two-person concept is implemented to protect COMSEC materials and WS3 controlled components against access by a lone individual. An authorized two-person concept team consists of at least two individuals who meet the following criteria:

3.7.1. Certified under the personnel reliability program (PRP) as specified in AFI 36-2104, *Nuclear Weapons Personnel Reliability Program(PRP)* (or NATO equivalent). ***NOTE:*** Host nation personnel can perform duties as one member of a WS3 two-person concept team as long as they are not part of a two-person team performing maintenance on the vault, handling WS3 keyed/ coded material (i.e., modules), or handling two-person concept controlled components. Host nation personnel can never be left alone with an unlocked WSV.

3.7.2. Capable of detecting incorrect or unauthorized procedures with respect to the tasks being performed. Personnel need not be able to identify all controlled components, but rather must know that no maintenance, adjustment or tampering with the WS3, outside the scope of the operation being performed, is allowed.

3.7.3. If performing maintenance on the vault, handling WS3 keyed/coded material (i.e. modules), or handling or performing maintenance on other controlled components, personnel must be trained on handling and control of WS3 keyed/coded material. This training is documented on the AF IMT 4168, **COMSEC Responsible Officer and User Training Checklist**, and the USAFE Form 828, **USAFE Unique Communications Security (COMSEC) Responsible Officer and User Training Checklist**.

3.7.4. Are designated to perform the required task.

3.8. **Two signatures required.** WS3 material entered in Defense Courier Service (DCS) will be referred to as “two signatures required” material while it is in the DCS system. This designation will identify the material as necessitating “special handling” during movement and prevent confusion from other articles in the DCS system. These materials must be signed by two authorized personnel when receiving and turning over material to or from DCS.

3.9. **Unlock Codes.** Unlock codes are electronic values used to gain authorized access to a WSV. Unlock codes are transferred to the VP from Recode modules during Recode operations. These codes are produced in three versions: Maintenance Unlock Code, Mass Upload Unlock Code and the Universal Release Code.

3.9.1. **Maintenance Unlock Code.** Codes used to unlock a particular WSV for normal maintenance or operational requirements with an imposed time delay. These codes are vault specific and contain vault identification (ID) control data matching the VP ID entered during the ID/Time Delay (TD) operation according to T.O. 11N-50-1005, *Code-Transfer Group OX-69/FSQ-143 (V) Weapons Storage and Security System AN/FSQ-143 (V)*. Forty maintenance unlock codes (per WSV) are available after a recode operation. Maintenance codes are stored within CSMs and are transferred into Unlock modules for use. Once used, maintenance unlock codes are electronically flagged to prevent reuse.

3.9.2. **Mass Upload Unlock Code.** Codes used to unlock multiple WSVs on a WS3 installation for readiness exercises or operational requirements. The Mass code is capable of opening each WSV on an installation one time with an imposed time delay. Twenty mass upload codes are available after a recode operation. Mass upload codes are stored within CSMs and are transferred into unlock modules for use. Once used, mass upload codes are electronically flagged to prevent reuse.

3.9.3. **Universal Release Code.** Code designed to be used for operational emergencies only. This code can unlock any vault, any number of times without an imposed time delay. This code requires special handling and authorization prior to use in accordance with ACO Directive 80-6, ED 60-12.

4. Access and Escort Requirements.

4.1. Individuals requiring unescorted access to WS3 keyed/coded material, controlled components, or performing controlled procedures, must be US citizens, possess a final security clearance equal to or higher than the level of the material being accessed, and be certified through the PRP.

4.1.1. Designate those personnel authorized unescorted access to WS3 materials on the Access Approval and Authority Listing (AAAL) in accordance with ACO Directive 80-6, ED 60-12.

4.1.2. Limit to the extent possible, consistent with mission requirements, the number of personnel having access to WS3 equipment and COMSEC material.

4.1.3. Physical control (possession) of keyed/coded material, equipment, or controlled components constitutes access. Viewing of WS3 keyed/coded material (including sealed URC cards and modules), equipment or controlled components does not constitute access. Personnel under escort by an authorized team are not considered as having access.

4.2. Personnel not listed on official unit authorization listings will be escorted into areas containing WS3 keyed/coded material or controlled components. These personnel will remain under the constant supervision of an authorized two-person concept team and are restricted from physically handling or controlling any materials or equipment. Escorted personnel's activities will be limited to viewing materials, administrative documentation and viewing or evaluating operations.

4.2.1. Official inspection teams from Logistics (HQ USAFE/A4), Inspector General (HQ USAFE/IG), Communications (HQ USAFE/A6), HQ USAFE/CSS/CA635761 and the Defense Threat Reduction Agency (DTRA), etc. are authorized escorted entry to areas containing WS3 keyed/coded material or controlled components in the performance of their official duties. Higher headquarters inspectors do not require PRP certification, but must be US citizens and possess a final security clearance commensurate with the material being reviewed. The CM, CRO, or an authorized UA representative, identified on the access list as having escort privileges, will positively identify inspectors by comparing personal identification cards with team composition/site visit messages, properly authenticated entry authorization lists (EAL), or other official notification of visit before allowing viewing of WS3 material.

4.3. Use AF Form 1109, **Visitor Register Log**, to record the arrival and departure of persons granted escorted entry to areas containing WS3 materials or operations in accordance with AFI 33-211.

4.3.1. Personnel (i.e., Monitoring Facility Operator (MFO)) on the facility access list where a safe containing WS3 material is located, and whose duties normally require them to be present in the area, do not need to be entered on an AF Form 1109, but their viewing of WS3 procedures should be limited as much as possible without impacting their duties.

Section B—COMSEC Material

5. Classification and Management of COMSEC Material.

5.1. General COMSEC classification guidance may be found in AFMAN 33-272, (S) *Classifying COMSEC, TEMPEST Information (Secret)*. Additionally, the following guidance applies to the COMSEC components of the WS3:

5.2. Protect and control all COMSEC materials in such a manner as to prevent a lone individual from having access to both the "A" and "B" modules or URC cards. An individual "A" or "B" module/card does not require two-person control. Organizations will institute and enforce the Two-Person Concept in accordance with AFI 91-104 and this instruction to prevent access by a lone individual. Personnel designated as "A" team members will not be issued or otherwise allowed access to "B" modules/cards. Personnel designated as "B" team members will not be issued or otherwise allowed access to "A" modules/cards.

5.3. Rekey, Recode, Code Storage modules, and Universal Release Code cards are classified SECRET - NOFORN. Rekey modules are additionally classified as, and marked with the CRYPTO designator.

5.3.1. Each person issued a module or URC card, is responsible for its control until returning it to the issuing office or properly transferring it to another authorized person.

5.4. Code and issue all unlock modules under two-person concept. Limit viewing of code transfer operations to the greatest extent possible.

5.4.1. Classify unlock modules SECRET - NOFORN after loading them with any code from the CSMs or URC cards. Unlock modules remain classified SECRET - NOFORN until the issuing agency verifies all loaded codes have been erased. ***NOTE:*** Following issue, the individuals accepting responsibility for the modules and/or URCs are not required to remain together.

5.4.2. Unlock modules should normally contain only those codes necessary to complete maintenance operations scheduled during a 12-hour period. If an unlock module remains loaded with codes and is returned to storage, it must be added to the USAFE Form 868, **Weapons Storage and Security System (WS3) COMSEC Inventory**.

5.4.3. Do not carry modules of any type into public areas including dining facilities, finance centers, base exchanges, military personnel flights, etc.

5.4.4. Unlock modules must be erased when the codes they contain are no longer required.

5.5. Unlock modules that have been erased (do not contain any codes) and the Code transfer Unit (CTU) are not COMSEC materials and are unclassified. Control them in a manner to prevent misuse, theft, sabotage, and/or tampering.

5.6. Backup sets of Rekey, Recode, and CSMs are only issued when a failure or malfunction of the primary set occurs.

5.7. Perform a CSM update monthly. Monthly update is not required if CSMs from primary set were not issued during the month.

5.8. URC cards will only be issued or used when properly authorized in response to actual contingency operations. Do not issue or use URCs for readiness exercises or system rekey/recode operations.

5.9. In the event a URC is compromised or opened during a higher state of alert or readiness, and a subsequent peacetime posture is declared, initiate a system rekey/recode using the reserve edition as soon as possible. Make every effort to complete the rekey/recode operation within 24 hours of the time a peacetime posture was declared.

5.10. Effective Edition COMSEC Materials must be handled according to the following procedures:

5.10.1. Store effective editions of Rekey, Recode, and CSMs in facilities where there is an available General Services Administration (GSA) approved safe. The Primary set ("A" and "B" pairs) and Backup set ("A" and "B" pairs) of Rekey, Recode and CSMs, must be stored in separate facilities.

5.10.2. The Effective Edition, Primary and Backup, "A" URC cards may be stored in the same facility. Similarly, the Effective Edition, Primary and Backup, "B" URC cards may also be stored in the same facility. At no time, however, will both the "A" and "B" URC cards from the Effective

Edition be stored within the same facility. The URCs may be stored in the same container as the Rekey, Recode and Code Storage modules.

5.10.3. Store the Effective Edition URCs in facilities equipped with a duress alarm and manned 24-hours a day. The personnel manning these facilities must be US citizens, possess at least a Secret security clearance and be certified through the PRP. Store “A” or “B” URC code in the US command post and the other code in the Local Monitoring Facitlity (LMF) or Remote Monitoring Facitlity (RMF). The facilities used to store the primary and backup “A” sets and primary and backup “B” sets of effective editions of URCs must be physically separate.

5.10.4. Units may begin treating the Reserve Edition as Effective material, with respects to storage, at any point in the week immediately prior to beginning the Rekey/Recode operation. Once installed in the Data Authenticator, the material formally becomes a second Effective edition. Both the current and new effective editions may be stored together within the same containers until the operation is completed.

5.11. Reserve Edition COMSEC Materials must be handled according to the following procedures:

5.11.1. The complete Reserve Edition may be stored in one container however, never store them in the same safe as effective materials.

5.11.2. Reserve editions of keyed/coded material will be stored within the COMSEC account.

5.12. Store superseded modules in the same manner as reserve material until returned to DIRNSA. Whenever possible, superseded modules will be stored within the COMSEC account. If adequate space and/or security containers are not available, then the superseded modules may be stored with the WS3 UA. An exception to policy is not required for storage of superseded modules outside of the COMSEC account.

5.13. Use the following procedures to record and store CSM access codes on a Standard Form 700, **Security Container Information Form**:

5.13.1. On the detachable portion (Part 2A):

5.13.2. Enter “CSM ACCESS CODE A” or “CSM ACCESS CODE B” (as applicable) in the “CONTAINER NUMBER” Block.

5.13.3. Enter the CSM access code in the “COMBINATION” Block.

5.13.4. On the back of the form, annotate the edition and register number. Do not annotate the short-title.

5.13.5. Mark the classification block SECRET, NOFORN.

5.13.6. Place the form inside of the envelope (Part 2) and seal it.

5.13.7. On the exterior of the envelope (Part 2):

5.13.8. Blocks 1 through 8 are non-applicable and not required to be completed.

5.13.9. Enter the date in Block 9.

5.13.10. Enter “CSM ACCESS CODE A” or “CSM ACCESS CODE B” (as applicable) in Block 10.

5.13.11. Enter the names of personnel making the access code change in Block 11 and any other names deemed necessary. ***NOTE*:** Any personnel listed must be authorized "A" or "B" team members as appropriate.

5.13.12. Annotate "AAAL Access Required" on the front and back of the envelope.

5.13.13. Mark the front and back, top and bottom of the SF 700 with an overall classification of SECRET, NOFORN.

5.13.14. Secure the completed SF 700(s) in a two person safe.

5.13.15. Do not store the completed SF 700(s) in the same container with the modules for which it applies. Completed SF 700(s) must be stored in a manner to allow access by authorized WS3 COMSEC two-person teams only. The SF 700 for the Primary module set must be stored with the Backup module set and vice versa. This ensures only authorized WS3 COMSEC two-person teams can gain access to the recorded codes. Replace the SF 700(s) any time a new CSM access code is assigned (e.g., suspected compromise of old CSM access code, new edition implemented, etc.). Destroy the old SF 700 in the same manner as SECRET collateral information.

6. COMSEC Requisitioning.

6.1. Key Format. Distribute the keys and codes for the WS3 system in module and hard copy form through the COMSEC material control system (CMCS). Control all key or code material as accounting legend code (ALC)-1 COMSEC material within the CMCS.

6.2. DIRNSA/I551/I5171/I513 produces and distributes WS3 material to the appropriate COMSEC account for each WS3 installation. Annual deliveries of material will normally consist of a single edition, the new second reserve edition, for each location.

6.3. Each unit will maintain an effective and two reserve editions of WS3 material. When a unit performs their annual rekey/recode, one reserve edition will be issued to the CRO and the superseded edition will be returned to the CM until disposition instructions are received from the controlling authority. Until the new edition is received the unit will only be required to maintain one reserve edition.

6.4. The controlling authority will send a message to DIRNSA/Y51/Y171 requesting material production and distribution. This request is completed by the Controlling Authority following notification that a Rekey/Recode operation has been completed. This process is outlined in **paragraph 9.3.**.

6.5. Upon receipt, DIRNSA/I551/I5171/I513 will take action to produce and ship the requested materials. Prior to shipment, DIRNSA/Y51 will send a message to the controlling authority identifying the material being shipped and including the appropriate COMSEC account as an information addressee.

7. Receipt of COMSEC Material.

7.1. Upon receipt of WS3 COMSEC material, the CM will process the material under two-person concept. Two individuals will process and issue WS3 COMSEC material in accordance with AFKAG-1, *Air Force Communications Security (COMSEC) Operations* and AFKAG-2, *Air Force COMSEC Accounting Manual*. Office symbol reference Air Force Communications Agency/Information Assurance (AFCA/GCIS). All WS3 COMSEC related correspondence (i.e., SF 153, **COMSEC Material Report**, hand-receipts, destruction vouchers, and inner wrappers of sealed packages, etc.) must contain the following statement:

"TWO-PERSON CONCEPT AS OUTLINED IN DOD C-5210.41-M/Air Force Supplement, IS MANDATORY AT ALL TIMES FOR THIS MATERIAL ANY UNAUTHORIZED ACCESS BY A LONE INDIVIDUAL IS BASIS FOR COMPROMISE AND MUST BE IMMEDIATELY REPORTED TO HQ USAFE/A4WN AND INFO TO DIRNSA/I551/I413, USAFE CSS/CA635761, AND HQ AFCA/GCIS."

7.2. Upon initial receipt, the CM will notify the WS3 UA of initial receipt of reserve WS3 COMSEC material. The CM will temporarily issue WS3 modules to the UA so they may inspect code modules for evidence of tampering and accomplish code module receipt procedures according to T.O. 11N-50-1005. This inspection may also be accomplished by the WS3 UA, in the presence of the CM, at the COMSEC account without requiring the temporary issue procedure.

7.3. Initial inspection of WS3 COMSEC material will be conducted by the UA within 72 hours of arrival on station. The reserve edition is identified by loading the unit ID/TD into the designated set. Refer to T.O. 11N-50-1005 for inspection and ID/TD procedures. Upon completion of these tasks, the UA will return the reserve edition to the CM until needed for operational use (e.g., annual recode/rekey).

7.4. Following COMSEC account addition and T.O. 11N-50-1005 receipt inspection procedures completion, the CM will send a memorandum to the Controlling Authority identifying a new reserve edition is on hand and serviceable.

8. WS3 COMSEC Manager Material Issue Procedures.

8.1. The CM will utilize procedures outlined in AFKAG-1 and AFKAG-2 for the issue of WS3 materials to the UA.

8.2. Issue WS3 COMSEC material under two-person concept procedures. A two-person concept team will be employed by both the COMSEC account and WS3 UA. Two individuals from the WS3 UA must sign the SF 153.

8.3. Receipt of WS3 COMSEC material requires two authorized individuals. Prior to signing for the material, inspect URCs for evidence of tampering or damage. After receipt, immediately transport the WS3 COMSEC material to the authorized storage location.

9. Implementing WS3 COMSEC Material.

9.1. The annual rekey of the AU, DA, and SP occurs in the anniversary month of the prior year's rekey. Similarly, the annual recode of the VP occurs in the anniversary month of the prior year's recode. The annual rekey and recode operations will be accomplished together.

9.2. Units are authorized to implement the reserve edition of WS3 material (conduct a Rekey/Recode operation) during the scheduled month without further controlling authority approval. Units must receive authorization from the controlling authority prior to implementing the reserve edition of WS3 material for any other reason, or at any time other than the scheduled anniversary month.

9.2.1. In response to operational emergencies, where prior coordination with the controlling authority is not possible, the wing or Munitions Support Squadron (MUNSS) commander is authorized to direct implementation of the reserve edition of WS3 material. Upon implementation, immediately notify the following addressees via Defense Message System (DMS) message (short title and/or edition is not required) fully detailing the date, time, and reason for implementation of the reserve edition:

ACTION: HQ USAFE/A4WN

INFO: DIRNSA/I551/I5171/I513

HQ CPSG/ZIW

HQ ESC/FDD

USAFE CSS/CA635761

9.3. User Agencies (UA) will submit a memorandum to the base COMSEC Manager (CM), identifying that Rekey/Recode operations have been completed. This memorandum must include the following: edition superseded, edition that became effective, date operation began, date operation was completed, identification of new reserve edition and a statement requesting another reserve edition be provided. This memorandum will be classified Confidential. Completion of this memorandum also fulfills the AFI 33-211 requirement to annually review and validate UA COMSEC requirements. The base COMSEC Manager will forward this information to the Controlling Authority (CONAUTH), (HQ USAFE/A4WN) along with a request for disposition of the superseded edition. The CONAUTH will use this memorandum to provide disposition instructions and also requisition a new reserve edition from DIRNSA.

10. Turn-In of WS3 COMSEC Material.

10.1. For return of superseded WS3 COMSEC materials to DIRNSA/I5171:

10.1.1. The CM will notify HQ USAFE/A4WN by message that superseded WS3 COMSEC material is available for return. This notification is accomplished by completing the memorandum identifying that Rekey/Recode operations have been completed in accordance with **paragraph 9.3.**.

10.1.2. HQ USAFE/A4WN will provide the necessary disposition instructions to the COMSEC account via message with an information copy to DIRNSA/I551/I5171, Information Assurance (HQ USAFE/A6NI) and Cryptological Systems Group/Force Protection (HQ CPSG/ZIW). This message will include the names of the authorized “A” and “B” recipients at DIRNSA/I5171 as well as authority to proceed with shipment.

10.1.3. Package the WS3 material for return shipment DIRNSA/I5171 as follows:

10.1.3.1. Place the “A” and “B” WS3 materials into separate inner packages (e.g., one “A” and one “B”).

10.1.3.2. Document a separate SF 153 (e.g., one “A” and one “B”) identifying the material contained within each package. Annotate “Authority for transfer is HQ USAFE/A4WN message DTG #######” on the SF 153. ***NOTE*****:** Place a copy of each SF 153 in the outer package as well as the inner packages.

10.1.3.3. Enter the following statement on each of the SF 153s:

“TWO-PERSON CONCEPT AS OUTLINED IN DOD C-5210.41-M/Air Force Supplement, IS MANDATORY AT ALL TIMES FOR THIS MATERIAL. ANY UNAUTHORIZED ACCESS BY A LONE INDIVIDUAL IS BASIS FOR COMPROMISE AND MUST BE

IMMEDIATELY REPORTED TO HQ USAFE/A4WN AND INFO TO: DIRNSA/I551/I413, USAFE CSS/CA635761 AND HQ AFCA/GCIS."

10.1.3.4. Place the completed SF 153s into the appropriate inner packages (e.g., "A" SF 153 with "A" material, "B" SF 153 with "B" material). Seal each package using tamper evident tape provided by DIRNSA/Y26.

10.1.3.5. Mark the exterior of each inner package with the appropriate overall classification (e.g., same as the material contained within). Also, mark as "A" or "B" material on the top of the package.

10.1.3.6. Attach a completed DCS Form 29, **DCS Customer Address Label**, (or equivalent) to the exterior of each of the inner packages with the following two-line DCS address annotated:

880231-BA21

DIRNSA/I5171

10.1.3.7. Enter the following statement on each of the DCS Forms 29:

"TWO-PERSON CONCEPT AS OUTLINED IN DOD C-5210.41-M/Air Force Supplement, IS MANDATORY AT ALL TIMES FOR THIS MATERIAL. ANY UNAUTHORIZED ACCESS BY A LONE INDIVIDUAL IS BASIS FOR COMPROMISE AND MUST BE IMMEDIATELY REPORTED TO HQ USAFE/A4WN AND INFO TO: DIRNSA/I551/I413, USAFE CSS/CA635761 AND HQ AFCA/GCIS."

10.1.3.8. Place the sealed inner packages, along with the copies of the completed SF 153s, into the outer package.

10.1.3.9. Seal the outer package using paper tape, with fiber reinforcement.

10.1.3.10. Do not place any classification markings or two-person concept statement on the exterior of the outer package.

10.1.3.11. Attach a DCS Form 29 (or equivalent) to the exterior of the outer package with the following two-line DCS address annotated:

880231-BA21

DIRNSA/I5171

10.1.3.12. Enter the following statement on the DCS Form 29 special handling block in large red letters: "**TWO SIGNATURES REQUIRED**." Enter the following on or next to the DCS Form 29: "Request the delivering station contact a member from both Team A and Team B for delivery."

10.1.3.13. Complete a DCS Form 1, **Receipt to Sender**, annotated with the appropriate DCS two-line addresses (e.g., "FROM" and "TO") and enter "**TWO SIGNATURES REQUIRED**" in block "e" on the line listing the WS3 package. Enter a statement below the listed item "Material must be receipted for at destination address by any one individual from the A personnel group and any one individual from the B personnel group." After this statement enter the names of the A and B personnel groups from the disposition instructions in the message authorizing shipment of the WS3 modules.

10.1.3.14. Transport the package under two-person concept procedures to the DCS station for delivery to DIRNSA/I5171. Ensure two team members sign entering the package into DCS channels and two DCS personnel receipt for the package.

10.1.3.15. One person from each of the designated "A" and "B" personnel groups at DIRNSA/I5171, identified in the controlling authority's transfer approval message, will receipt for the WS3 COMSEC material.

11. Transfer of WS3 COMSEC Material.

11.1. All transfers of WS3 COMSEC material from one COMSEC account to another, except as specifically authorized in this instruction, require prior coordination and approval from the controlling authority. Under no circumstances, will WS3 COMSEC material containing any unit's effective key or code be transferred to another account.

11.2. For those COMSEC accounts holding command-directed reserve WS3 COMSEC editions, transfers of WS3 COMSEC material to other COMSEC accounts will occur only when directed by HQ USAFE/A4WN and under USAFE CSS/CA635761 authorization. The material will be transferred in accordance with AFKAG-1 and AFKAG-2 and packaged in accordance with **paragraph 10.1.3.** substituting the identified account's two-line DCS address on all DCS Forms 1 and 29 where applicable. Under no circumstances, will WS3 COMSEC material containing any unit's effective key or code be transferred to another account.

11.3. Material shipped to USAFE/MUNSS are to be delivered to any two personnel on the DCS Form 10, **DEFENSE COURIER SERVICE AUTHORIZATION RECORD**, for the destination account. Material shipped back to DIRNSA/I5171 must include listing of "A" and "B" team member identification (listed on documentation) and must be delivered to them over the counter at the Baltimore DCS station. Personnel at the Baltimore DCS station will notify DIRNSA/I5171 personnel for pick up of material.

12. Inventory Procedures for COMSEC Material.

12.1. Use USAFE Form 868, **Weapons Storage and Security System (WS3) COMSEC Inventory**, for inventory of all WS3 COMSEC materials. Inventories listing WS3 COMSEC materials are UNCLASSIFIED. Inventory WS3 material as ALC-1 material in accordance with AFI 33-211, USAFE Supplement 1 to AFI 33-211, and this instruction.

12.2. Two properly trained and authorized individuals must conduct and document all inventories. Ensure the short title, edition, quantity, and register number of each item is physically sighted on each item of material and compared against the inventory form by both members performing the inventory. Bring errors and corrections to the immediate attention of the CRO or alternate. If the error can't be resolved, immediately notify your unit CM.

12.3. On days the safe is opened, inventory all material prior to locking the safe for the last time that day. As a minimum, conduct inventories of material issued to the WS3 UA at least once each month.

12.4. Inventories of reserve material stored within the COMSEC account need only be conducted semiannually or as required on days the safe is opened. Also accomplish inventories prior to change of CRO, CM, or when directed by higher authority.

12.5. If the number of documented inventories conducted during a single calendar day exceeds the number of blocks available for documentation of such inventories, place a brief, dated memorandum for record on the reverse of the USAFE Form 868. Each member of the two-person concept team will initial (INITS) the memorandum for record (e.g., DD MMM YY - SECOND INVENTORY REQUIRED ALL ITEMS LISTED ARE PRESENT AND ACCOUNTED FOR INITS/INITS).

12.6. When adding new WS3 COMSEC material (i.e., Temporary storage of Unlock modules), one individual will annotate the USAFE Form 868 with the short title, edition, quantity, and register number of the material. A second individual will verify the information annotated on the inventory is accurate. In the event a correction is necessary, place a single line through the erroneous entry, both individuals initial, and annotate a brief, dated memorandum for record on the reverse of the form (e.g., DD MMM YY - SHORT-TITLE INCORRECTLY ENTERED CAUGHT AND CORRECTED ON THE SPOT INITS/INITS). Once material has been added and all entries checked, secure the inventory form and the WS3 COMSEC material in the safe.

12.7. Use of multiple inventory forms based on local requirements is authorized. Maintain inventory forms for 6 months plus the current inventory in accordance with Air Force Records Disposition Schedule (RDS) located at: **https://webrims.amc.af.mil** and AFI 33-211.

12.8. The CM will conduct and document a semiannual inventory of all WS3 COMSEC material in accordance with AFKAG-1 and AFKAG-2 every 6 months. This includes a physical inventory of all effective and reserve WS3 COMSEC material.

12.8.1. The CM and an authorized two-person concept team for the WS3 UA will perform a complete physical inventory of all WS3 COMSEC material (primary and backup) held within the WS3 UA (including LMF and RMF facilities).

12.9. Erased (empty)unlock modules are not COMSEC materials and may be accounted for using local inventory forms or by documenting inventories on the AF Form 2432**, Key Issue Log**.

13. Issue Procedures for COMSEC modules and URC cards.

13.1. The WS3 UA commander will designate in writing by name, rank, social security number, and security clearance, the personnel authorized to issue and receive modules and URCs. Designate personnel as being assigned to either the “A” or “B” team. Once assigned to the A or B team, personnel are not allowed to change teams while assigned to the same duty station. If reassigned to another base where duties require WS3 COMSEC access, personnel may be assigned to either the A or B team regardless of their designation at a previous unit. They must meet **paragraph 4.** access requirements. Personnel may be authorized to issue, receive or issue and receive modules and/or URCs. If authorized to receive coded unlock modules, personnel must be job qualification standard qualified in vault access procedures and properly trained in WS3 COMSEC procedures. The commander must also specifically designate those individuals authorized to escort visitors viewing WS3 materials. The number of individuals authorized escorted privileges must be kept to the absolute minimum. The requirements of this letter may be combined with the ACO 80-6, ED 60-12, Access Approval and Access Authority Listing (AAAL) listing to create one comprehensive listing of personnel authorized access to WS3 materials.

13.2. Use the AF Form 2432, **Key Issue Log**, to record the issue and subsequent turn-in of modules/code cards. (Inventories are recorded on the USAFE Form 868).

13.2.1. For coded unlock modules, annotate the "Structure" block of the form with the unlock module serial number (including "A" or "B" designation), type of unlock code loaded, and WSV ID loaded.

13.2.2. For Rekey, Recode, and CSMs, annotate the "Structure" block with the module type, "A" or "B" designation, and serial number.

13.2.3. For URC cards, annotate the "Structure" block with "URC Card", register number and indicate "A" or "B" designation.

13.2.4. Additionally, this form will reflect the name, rank, and signature of the individual receiving or turning in the module with the time and date of the transaction in the appropriate blocks.

13.3. Local transfer of modules or URC cards between assigned personnel is authorized provided the transfer is coordinated with and approved by an individual authorized to issue modules on behalf of the WS3 UA. For local transfer of modules and/or URCs, annotate the AF Form 2432 as follows:

13.3.1. On a new line, enter the word "TRANSFER" and serial number of module being transferred in the "Structure" block. Enter the date and time the transfer was authorized in the "Time" and "Date" blocks of the "In" block on the original line entry, and "Out" block of the new line entry. Print the names of the personnel receiving the modules and/or URC cards to be transferred in the "Signature" block of the "Out" block of the new line entry.

13.3.2. When the personnel who transferred the modules and/or URC cards return, they will sign the "Signature" block on the "In" block of the original line entry. When the personnel receiving the modules and/or URC cards return, they will sign the "Out" and "In" "Signature" blocks on the new line entry.

13.4. The use of multiple key issue logs is authorized. Key issue logs are UNCLASSIFIED. Maintain disposition of completed AF Forms 2432 for 30 days plus the current record according to Air Force Records Disposition Schedule (RDS) located at: **https://webrims.amc.af.mil**.

13.5. URCs may only be issued for use in accordance with ACO Directive 80-6, ED 60-12. Specify these procedures and authority for use in local Emergency Action Plans (EAP) and checklists.

14. Caretaker Status and Training Code Transfer Group Requirements.

14.1. Once placed into "caretaker" status according to T.O. 11N-50-1008, the following CTG requirements will be accomplished:

14.2. Immediately return the effective edition Rekey modules and the entire reserve edition (e.g., primary and backup Rekey, Recode, Code Storage modules, and URC cards) to the COMSEC account responsible for the WS3 installation placed into caretaker status. The COMSEC account will inform the CONAUTH that these materials are available for return to DIRNSA/I5171.

14.3. Declassify the effective edition Code Storage and Recode modules. Remove classification labels from these modules, their associated storage containers and the Vault Processors.

14.4. Record the short title and serial number of the declassified Code Storage and Recode modules on an AF IMT 3126, **General Purpose**. Annotate the name of the WS3 installation across the top of the form (e.g., RAMSTEIN AB). Retain this form with the declassified CSMs and recode modules. Notify the CM of the declassification of the CSMs and recode modules and request they remove these items from accountability. A Standard Form (SF) 153, **COMSEC Material Report**, must be generated to officially document this declassification and notify the CM. This action will ensure removal from accountability and prevent declassified material from reentering operational channels.

14.5. Obtain the effective edition URC values and record them on the AF Form 3126. Destroy the opened/exposed URCs according to **paragraph 15.**. Provide a copy of the SF 153 to the CM notifying them of URC destruction.

14.6. Document the CTU(s) by nomenclature, serial number, and part number on the AF Form 3126.

14.7. Initiate transfer of the declassified Code Storages, Recode modules, and CTU(s), along with the original AF Form 3126, to the UA of the parent wing or Unit identified with support responsibility for the location placed into caretaker status. These items must be hand-carried, transferred via Department of Defense supply or transportation channels, or forwarded via US registered mail. Specific instruction will be provided by the Controlling Authority, at the time of placing a base in caretaker status.

14.8. Once removed according to T.O. 11N-50-1008, document the nomenclature, serial number and part number of each Message Processor Hard Drive (MPHD) on the AF Form 3126.

14.9. Send a priority message to DIRNSA/I551/I5171, HQ CPSG/ZII/ZIW, HQ USAFE/A4WN, and USAFE CSS/CA635761 indicating the date the material was declassified, the date the material was transferred, via what method, and the intended recipient.

14.10. DIRNSA/I551/I5171 will forward unclassified rekey modules as replacements for the classified Rekey modules. These unclassified Rekey modules will be maintained at the caretaker installation's support location along with the declassified CSMs and recode modules, and CTU(s) for possible future reactivation and any necessary periodic maintenance.

14.11. Store the caretaker installation's CTG in a manner to prevent misuse, theft, sabotage, or tampering. Inventory the CTG on a monthly basis. Use serial number of components for accountability purposes. If inventory discrepancies cannot be resolved, immediately notify the controlling authority.

14.12. Originally produced Training Code Transfer Group materials were unclassified and utilize non-COMSEC materials. These will be stored and inventoried in the same manner identified for caretaker materials. All other training materials will be protected according to their assigned classification and COMSEC status, normally UNCLASSIFIED, ALC-4.

15. Destruction.

15.1. The only WS3 COMSEC materials authorized for local destruction are superseded URCs. Destruction of URCs is only authorized on DIRNSA approved destruction devices listed on the DIRNSA approved destruction device list (contact the CM for assistance). Accomplish destruction within 12 hours of supersession. Document destruction on the SF 153. This form is Unclassified. Keep SF 153 for 3 years after destruction. Reports are UNCLASSIFIED.

Section C—Controlled Components

16. Classification and Management of Other Controlled Components.

16.1. Protect and control all identified WS3 controlled components in such a manner as to prevent access by a lone individual in accordance with this instruction and the item technical orders 11N-50-1003, 11N-50-1004, 11N-50-1005, 11N-50-1006 and 11N-50-1008. Air Force personnel will institute and enforce the Two-Person Concept in accordance with AFI 91-104 and this instruction to prevent access by a lone individual.

16.2. To ensure system integrity, GOLD EPROMs require constant protection from access by a lone individual. Surplus GOLD EPROMs require the same level of protection as those operationally configured within WSVs. EPROMs are not Mission Support Kit items; base supply will not procure, issue, or stock. GOLD EPROMs are requisitioned and receipted according to this instruction.

16.3. Only install GOLD EPROMs into components of an operational system. Components in the Mission Support Kit (MSK) (i.e., AU, VP, DA, MP, SP) have non-controlled “BRONZE” EPROMs installed. These must be replaced with controlled EPROMs prior to installing the component into an operational system. Never install any component, equipped with BRONZE EPROMs, into an operational system.

16.4. The AU, DA, and SP are unclassified, however, they become controlled components once GOLD EPROMs are installed. They are classified SECRET CRYPTO (NOFORN) when loaded with operational keys from the Rekey modules. The AU, DA, and SP become unclassified in the event of a power loss, however, they still require control under two-person concept to prevent unauthorized tampering when the GOLD EPROM is installed.

16.5. The VP is an unclassified however, it becomes a controlled component once GOLD EPROMs are installed. The VP is classified SECRET (NOFORN) when loaded with operational codes from the Recode modules**.** The VP becomes unclassified after performance of procedures in technical order 11N-50-1004 to remove IC U18 and, or when the data contained has been declared unclassified and the operational codes superseded.

16.6. The Message Processor Hard Drive (MPHD) is unclassified however, it requires constant protection from access by a lone individual. MPHDs are not Mission Support Kit items; base supply will not procure, issue, or stock. MPHDs are requisitioned and receipted according to this instruction.

16.7. The vault motor starter, motor starter relays, AU to VP cable and alternate operating system time delay relay are unclassified. They are only controlled components following two-person inspection and installation in an operational WSV.

16.8. An authorized team must safeguard controlled components under two-person concept requirements at all times when the WSV is not down, locked, and alarms secured.

16.8.1. If a WS3 cannot be closed, locked and have the alarms returned to secure , refer to ACO Directive 80-6, ED 60-12 for appropriate actions.

16.9. Store unassociated controlled components according to **paragraph 19.**. Units should procure enough safes so that drawers are available to store all WS3 related materials.

16.10. While not controlled components, compact flash cards used to transfer data from the Message Processor will be identified for, and used only for this purpose. Units are authorized to commercially procure as many cards as necessary to meet local requirements. Store these cards in a manner to prevent theft and misuse. Events Files, Site Unique Configuration or any other information downloaded from the Message Processor will be controlled as For Official Use Only (FOUO) information.

17. HQ USAFE/A4WN Controlling Authority Procedures.

17.1. The controlling authority will initiate a request for new EPROMs and MPHDs to HQ CPSG/ZIW by message with an informational copy to USAFE CSS/CA635761, USAFE CSS/SCMM, the COMSEC accounts, and maintenance shops at least 120 days prior to re-supply.

17.2. Resolve emergency requests from the unit by transferring stocks within theater and/or controlling authority request for emergency restock from HQ CPSG/ZIW.

17.3. Upon receipt of the re-supply request, HQ CPSG/ZIW will take action to produce and ship all required material. HQ CPSG/ZIW will notify the controlling authority, USAFE CSS/CA635761, COMSEC accounts, and the maintenance shops by message of the quantities of material being shipped to each unit and the date material will be transferred to DCS.

17.4. HQ CPSG/ZIW will ship EPROMs and MPHDs via DCS to the applicable COMSEC accounts and enter (in large letters) "**TWO SIGNATURES REQUIRED**" in the Special Handling block of the DCS Form 1 and DCS Form 29.

17.5. The "**TWO SIGNATURES REQUIRED**" special handling identifies to the DCS couriers that two personnel listed on the DCS Form 10 must sign for the package. The package will include an AF Form 310, **Document Receipt and Destruction Certificate**, listing the EPROMs and MPHDs by serial number. Two personnel will sign the DCS Form 1 to enter each package into DCS channels.

18. Unit Procedures.

18.1. The COMSEC accounts will receive the EPROMs and MPHDs from the DCS. Two personnel from the COMSEC account must receive the shipment due to the special handling of "**TWO SIGNATURES REQUIRED**" for these items. The COMSEC account will transport and store EPROMs and MPHDs under two-person concept.

18.1.1. EPROMs and MPHDs are not COMSEC material. Do not enter into CMCS or the computerized management of COMSEC material (CM2) program. Do not voucher documentation received with the EPROMs and MPHDs or send to the central office of record (COR). The COMSEC account must create a separate folder to file EPROM and MPHD-related receipt and transfer documentation (i.e., DCS Forms, AF Forms 310 for receipt or transfer).

18.1.2. COMSEC accounts will acknowledge receipt of the EPROMs and MPHDs as listed on the AF Form 310 included in the package received from DCS. Two COMSEC account personnel must verify the material received by serial number, sign the receipt, and mail it back to HQ CPSG/ZIW, 230 Hall Blvd Suite 224, San Antonio TX 78243-7056.

18.1.3. Transfer EPROMs and MPHDs from COMSEC accounts to the communications or vault maintenance shop within 72 hours of receipt. Use an AF Form 310 to document transfer (not issue) of the EPROMs and MPHDs to the communications or vault maintenance two-person concept team. Identify the EPROMs and MPHDs (individual or kit) by serial number on the AF Form 310.

18.2. When receipted by the communications or vault maintenance shop, the packaged EPROM kit or MPHD will be opened and removed from any packaging. Conduct an inspection of each individual EPROM or the MPHD for evidence of tampering or damage. Once inspected, return any components to their packaging to prevent damage while in storage.

18.3. Keep an inventory of controlled components on an AF Form 3126 in the following manner:

18.3.1. Fill in the Heading Blocks as shown on the example AF Form 3126 contained in **Attachment 2**.

18.3.2. Enter the controlled component nomenclature, type, part number, and serial number in the large block to the left. ***NOTE***: If the components are contained within a kit, the kit nomenclature, part number and serial number may be entered on the line above the individual component information. This kit information is not necessary, nor can it be used for accountability, but may be useful in identifying current stocks.

18.3.3. In the next smaller block enter the date received.

18.3.4. The second smaller block to the right is the "Date Removed" block. This block is filled only when the item is permanently removed from the inventory listing. Temporary removal is accounted for on the AF Form 2432 as outlined in **paragraph 18.6.**.

18.3.5. If the component is permanently installed, enter the installation location (i.e. Vault 120, LMF DA, etc.) in the third small block to the right.

18.3.6. If the component is transferred to another unit or destroyed, enter this information in the fourth small block.

18.3.7. Once a component is permanently installed and the nomenclature and serial numbers are entered on an AFTO Form 95, **Significant Historical Data**, or other electronic historical document, it can be lined out on the existing AF Form 3126 and omitted when a new inventory sheet is created. Items removed for destruction or transfer can also be removed from the inventory sheet in the same manner once the transaction is complete. Keep obsolete or transcribed AF Forms 3126 for 6 months plus the current record.

18.4. An inventory of controlled components is required at the end of day any time the container is opened or at a minimum monthly if the container is not opened. Two persons authorized access to controlled components will perform and sign the inventory.

18.5. Two properly trained and authorized individuals must conduct and document all inventories. Ensure the part number and serial number of each item is physically sighted on each item of material and compared against the AF Form 3126, inventory form by both members conducting the inventory. Bring errors and corrections to the immediate attention of the CRO or alternate. If the error can't be resolved, immediately notify HQ USAFE/A4WN.

18.6. Use an AF Form 2432 to sign controlled components in and out of the container for use, transfer or destruction, and to annotate inventories. The AF Form 2432 will be filled out according to the following instructions:

18.6.1. Enter the nomenclature, part number, serial number, and destination (i.e., Vault 120 or LMF DA) in the "Structure" block.

18.6.2. Enter the time and date in the "Out" section.

18.6.3. Two authorized individuals sign the "SIGNATURE" blocks.

18.6.4. If the component is returned to the safe, enter time, date and signatures in the "IN" section.

18.6.5. If the component is permanently installed or not returned to the safe for any other authorized reason, leave time and date of "IN" section blank. Two personnel will sign on first signature line and enter “installed,” “transferred,” or “destroyed”, or other appropriate comment on second signature line.

18.6.6. Keep completed AF Forms 2432 for 30 days plus the current record in accordance with Air Force Records Disposition Schedule (RDS) located at: **https://webrims.amc.af.mil.**

18.7. Destroy compromised or defective EPROMs in accordance with the procedures in the specific item technical order, 11N-50-1004. If the EPROMs are unassociated from the WS3 then destroy by clipping all pins and crushing with a hammer.

18.8. When MPHDs are deemed defective or compromised, send a request for disposition to HQ CPSG/ZIW with an informational copy the Controlling Authority, HQ USAFE/A4WN. All MPHDs must be controlled according to this instruction until returned to CPSG/ZIW for destruction. Never install a defective or compromised MPHD into a Message Processor.

18.9. EPROM and/or MPHD re-supply shipments to the theater will be scheduled for April and October of each year. Units must submit a consolidated message to HQ USAFE/A4WN in May and November for quantities of EPROMs required in the next shipment. Submit emergency requests when any spare EPROM quantity is one (1) or zero (0). Each unit will have one spare MPHD on-hand. If the MPHD is used, submit an emergency request for replacement immediately.

Section D—General Procedures

19. Physical Security of COMSEC and Controlled Components.

19.1. Store WS3 COMSEC and controlled components in a GSA approved security container configured in one of the following methods:

19.1.1. A safe with two three-position dial combination locks installed.

19.1.2. A safe with one electromechanical combination lock that is capable of holding two independent combinations (e.g., MAS-Hamilton X-07/X-08).

19.1.3. A safe within a safe; or by using two safes, one positioned within the other so that each must be opened in turn to gain access to the WS3 material stored within. Securely fasten the inner safe inside the outer safe with internal bolts, permanent welds, etc. Ensure the outer safe is of sufficient size and weight that one person cannot remove it.

19.2. Consider individual drawers, of a multiple-drawer safe, separate security containers only if each drawer is equipped with a separate lock.

19.3. All drawers must be installed and locked to ensure that safe is secured.

19.4. Controlled components may be stored in the same safe drawer as WS3 COMSEC materials as long as a physical divider is used to keep them separated from modules and code cards.

19.5. Authorized individuals must change combinations when the lock is initially placed into use, at least once every 12 months, when a person knowing the combination is no longer authorized access, or when the possibility exists that the combination has been compromised.

19.5.1. It is not necessary to change combinations if an individual is temporarily PRP decertified or suspended, providing the commander determines WS3 material is not in jeopardy. The decision not to change combinations must be documented in writing and maintained by the CRO for the entire period of the suspension or decertification.

19.5.2. Do not use the same combinations for two separate security containers in the same facility. At no time will one person know or have access to both combinations.

19.6. Each safe combination must have a separate SF 700, **Security Container Information Form** and SF 702, **Security Container Check Sheet**. Do not store the completed SF 700(s) in the same container for which it applies. Completed SF 700(s) must be stored in a manner to allow access by authorized WS3 COMSEC two-person teams only. The SF 700 for the, Primary module set container must be stored with the Backup module set container and vice versa. This ensures only authorized WS3 COMSEC two-person teams can gain access to the recorded combinations.

20. Safe Lockout Procedures.

20.1. In the event you are unable to open a safe used to store WS3 COMSEC materials:

20.2. Notify the CRO and CM immediately and recall all other two-person concept team members in the local area to ensure the proper combination is being performed. Allow each WS3 team member an opportunity to open the safe.

20.3. If the safe will not open, follow local procedures to contact a locksmith. A two-person concept team will remain in the area of the safe at all times while forcible entry is being attempted. Do not allow the locksmith access to safe contents. Remove them from the area once it is possible to open the safe.

20.4. Due to possible damage to the material stored within, torching will be used only as a last resort.

20.5. After the team accesses the safe, assesses the damage, and properly safeguards/ stores the material in accordance with this paragraph, the CM will immediately notify by message (if short title and/ or edition is included mark the message as CONFIDENTIAL) the addressees listed in **paragraph 14.8.** of all actions taken and the current status of WS3 material.

21. Inspection and Reporting Damage or Tampering.

21.1. Inspect modules and code cards upon initial receipt and prior to each use according to T.O. 11N-50-1005. Also inspect for signs of possible tampering and/or sabotage prior to each use, after each use, and as part of the monthly inventory.

21.1.1. If evidence of tampering is detected, report in accordance with **paragraph 25.**. Maintain the material under two-person concept control and/or storage until further instructions are received from the controlling authority and/or DIRNSA/I551.

21.1.2. Modules may be damaged if dropped or otherwise mishandled. Repairs should only be attempted after controlling authority approval and under depot authorization unless procedures are specified in the item technical order. WS3 UA CROs will develop procedures and methods to ensure adequate protection for modules.

21.1.2.1. Immediately remove damaged modules from use.

21.1.2.2. Modules deemed defective or damaged retain their original classification and control requirements.

21.1.2.3. Damage discovered on the connector or connector pins of a module will require inspections of all system components the damaged module came in contact with since documentation of the last satisfactory inspection.

21.2. Periodically conduct random visual inspections to detect signs of possible damage and/or tampering. Although manning factors and operational requirements may hinder the frequency of these inspections, regular inspections, especially at unmanned sites, increase the odds for early detection of damage or tampering, and follow-on reporting, thereby limiting adverse effects on overall system security.

21.3. Any damage to or malfunctions, outside of the normal failure mode, of modules, SCPs, Vault Processors, Authentication Units or Data Authenticators will be reported according to AFI 91-221 Weapons *Safety Investigations and Reports*, Chapter 1. Include the following as action and information addressees on all such reports:

ACTION: HQ USAFE/A4WN

HQ CPSG/ZII/ZIW

INFO: DIRNSA/I551/I5171

HQ ESC/FDD

USAFE CSS/CA635761

Section E—Training

22. WS3 COMSEC Training.

22.1. The CM will train individuals appointed as a CRO or alternate. These individuals act on behalf of the CM and the WS3 UA Commander and must become thoroughly familiar with all required COMSEC procedures.

22.2. The CRO will ensure each individual authorized access to WS3 COMSEC material completes initial and annual refresher training according to this publication, AFI 33-211, and USAFE Supplement 1.

22.3. The CRO will ensure each individual authorized access to WS3 COMSEC material is trained prior to access being granted.

22.4. The CRO will maintain training documentation for the entire period the individual is authorized access to WS3 COMSEC material.

22.5. Personnel authorized access to WS3 COMSEC material will be familiar with AFI 33-211, USAFE Supplement 1 to AFI 33-211, this publication, associated manuals and reference material, and applicable local procedures (e.g., operating instructions and checklists).

23. Additional Training for WS3 Maintainers and Users. Users of WS3 are responsible for ensuring all personnel tasked with any level of maintenance to COMSEC equipment, systems employing COMSEC functions, or equipment with embedded COMSEC components are trained to a level commensurate with their involvement with these systems and/or equipment. For specific requirements, refer to AFI 21-109, *COMSEC Equipment Maintenance and Maintenance Training*. Additionally, training should address the following:

23.1. Security and technical threat awareness.

23.2. Awareness of protective technologies, where appropriate.

23.3. Any unique security requirements pertaining to operational or caretaker systems, components, or equipment.

23.4. Unique reporting requirements for WS3 related materials.

Section F—Emergency Action Plans (EAP)

24. Emergency Evacuation and Disablement Procedures.

24.1. Activities with a WS3 mission must develop, maintain, and conduct dry runs of EAPs for emergency evacuation and emergency disablement as identified in ACO 80-6, ED 60-12, of all WS3 equipment and associated classified COMSEC items in addition to those EAPs required by AFI 33-211. Maintain EAPs in accordance with AFI 33-211 and USAFE Supplement 1 to AFI 33-211. EAPs and local plans should detail procedures with consideration for hostile and peacetime activities.

24.2. Unless otherwise warranted by a local threat assessment, accomplish and document dry runs of WS3 COMSEC EAPs semi-annually (e.g. once every 6 months) for all personnel having access to WS3 COMSEC material. Maintain documentation of these dry runs from command Information Assurance Assessment and Assistance Program (IAAP) to command IAAP.

24.3. Employ simple "stow and go" procedures to lock all WS3 COMSEC material and records in the appropriate container, rather than remove them from the facility, in response to fire, bomb threat, and natural disasters.

24.4. With proper notification, authority, or if a situation arises requiring emergency evacuation or emergency disablement procedures, "lock down" all WS3 equipment and associated classified COMSEC items within an empty WSV.

24.4.1. Upon completion of the emergency evacuation and/or disablement of all assigned priority assets, a two-person concept team from the WS3 UA will evacuate the remaining WS3 COMSEC materials (effective edition, primary and backup) from the local and remote monitoring facilities. Transport these materials under two-person concept requirements to a predetermined, empty WSV for storage and "lock down."

24.4.2. The next available two-person concept team from the WS3 UA will evacuate the WS3 COMSEC material (reserve edition(s)) from the COMSEC account for transport to a predetermined, empty WSV for storage and "lock down."

24.4.3. As dictated by operational necessity and limited manpower, combine the evacuation and transport of the effective and reserve materials when deemed necessary. In this instance, the two-person concept team will evacuate material from the LMF/RMF (e.g., effective edition) first and then proceed with the evacuation of material from the COMSEC account (e.g., reserve edition) before proceeding to a predetermined, empty WSV for storage and "lock down."

24.4.4. All COMSEC materials and equipment may be stored within one WSV during these contingencies if room permits.

Section G—Compromise and Reporting

25. Compromise. A general listing of reportable COMSEC incidents and the standards for reporting are contained in AFI 33-212, *Reporting COMSEC Deviations* any suspicious or unusual occurrences immediately. While these occurrences may or may not result in subsequent determination of a compromise, you must report them for full and proper investigation and subsequent evaluation.

25.1. Report suspected COMSEC incidents to the CM who will in turn notify the following offices:

ACTION: HQ USAFE/A4WN

DIRNSA/I551/I5171

INFO: HQ CPSG/ZII/ZIW

HQ ESC/FDD

USAFE CSS/ CA635761

25.2. Additional reportable incidents specifically related to WS3 COMSEC material, systems, and components include:

25.2.1. Any unauthorized loss of required two-person concept handling.

25.2.2. Any loss, unauthorized access, or unauthorized destruction, of WS3 keyed/coded material, equipment, or controlled components.

25.2.3. Installation of any component containing BRONZE EPROMs into an operational WS3 system.

25.2.4. If one of the effective URCs is inadvertently opened and/or compromised, a base wide rekey/recode will be initiated immediately using the reserve edition.

25.2.5. Compromised modules will be handled as follows:

25.2.5.1. Users and COMSEC accounts will retain all compromised modules under Two-Person Concept control unless explicit instructions are provided by the CONAUTH.

25.2.5.2. After receiving CONAUTH authorization, package according to **paragraph 10.**, except ship to the following address:

616600-KE10

CPSG/CA616600

25.2.5.3. HQ CPSG/ZIW will perform required inspections and forward the shipment under TPC to DIRNSA.

25.2.5.4. DIRNSA will perform additional inspections to determine if compromised modules may be returned to operational use.

25.2.5.5. Forms Prescribed: USAFE Form 868, ***Weapons Storage and Security System (WS3) COMSEC Inventory***.

25.2.5.6. Forms Adopted: AF 310, **Document Receipt and Destruction Certificate**; AF 847, **Recommendation for Change of Publication**; AF Form 3126, ***General Purpose (8 ½ x 11")***; AF 1109***,*** **Visitor Register Log**; AF Form 2432, ***Key Control Log***; AF 3126, **General Pur-**

pose; AF 4168, **COMSEC Responsible Officer and User Training Checklist**; AFTO 95, **Significant Historical Data**; SF Form 153, **COMSEC Material Report**; SF Form 700, **Security Container Information Form**; SF Form 702, **Security Container Check Sheet**; DCS Form 1, **Receipt to Sender**; DCS Form 10, **DEFENSE COURIER SERVICE AUTHORIZATION RECORD**; DCS Form 29, **DCS Customer Address Label**; USAFE Form 828, **USAFE Unique Communications Security (COMSEC) Responsible Officer and User Training Checklist**.

STEVEN J. SPANO, Colonel, USAF
Director of Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DOD Directive C-5210.41-M/Air Force Supplement, *Nuclear Weapon Security Manual*

CJCSI 3260.01, *Joint Policy Governing Positive Control Material and Devices*

SHAPE ACO Directive 80-6, Volume II, Part 2/HQ USEUCOM Directive (ED) 60-12, *Nuclear Surety Management for the WS3*

AFI 21-109, *COMSEC Equipment Maintenance and Maintenance Training*

AFI 21-116, *Maintenance Management of Communications- Electronics*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-211_USAFESUP1, *Communications Security (COMSEC) User Requirements*

AFI 33-212, *Reporting COMSEC Incidents*

AFI 33-215, *Controlling Authorities for COMSEC Keying Material (Keymat)*

AFI 33-230, *Information Protection Assessment and Assistance Program*

AFI 36-2104, *Nuclear Weapons Personnel Reliability Program*

AFI 91-101, *Air Force Nuclear Weapons Surety Program*

AFI 91-101_USAFESUP1, *Air Force Nuclear Weapons Surety Program*

AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs*

AFI 91-204, *Safety Investigations and Reports*

AFI 91-221, *Weapons Safety Investigations and Reports*

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

AFKAG-2, *Air Force COMSEC Accounting Manual*

AFMAN 33-272, (S) *Classifying COMSEC, TEMPEST, & C4 Systems Security (U)*

AFMAN 37-123, *Management of Records*

T.O. 11N-50-1003, *Console Group OJ-619/FSQ-143(V) and Monitor-Indicator Group OD-203/ FSQ-143(V) Weapons Storage and Security System AN/FSQ-143(V)*

T.O. 11N-50-1003-1, *Console Group OJ-619/FSQ-143(V) and Monitor-Indicator Group OD-203/ FSQ-143(V) Weapons Storage and Security System AN/FSQ-143(V)*

T.O. 11N-50-1004, *Processor, Vault Control Group OL-398/FSQ-143(V) Weapons Storage and Security System AN/FSQ-143(V)*

T.O. 11N-50-1005, *Coder-Transfer Group OX-69/FSQ-143(V) Weapons Storage and Security System AN/ FSQ-143(V)*

T.O. 11N-50-1006, *Depot Overhaul Instructions With Illustrated Parts Breakdown, Vault Cover Plate Assembly and Vault Screw Assembly; Processor, Vault Control Group OL-398/FSQ-143(V); Weapons Storage and Security System AN/FSQ-143(V)*

T.O. 11N-50-1008, *Deactivation and Reactivation Instructions, Weapons Storage and Security System AN/FSQ-143(V)*

Records Disposition Schedule (RDS) located at: **https://webrims.amc.af.mil**

Abbreviations and Acronyms

AAAL—Access Authority Authentication List

ACO—Allied Command Operations

ALC—Accounting Legend Code

AU—Authentication Unit

CM—COMSEC Manager

CMCS—COMSEC Material Control System

COMSEC—Communications Security

CONAUTH—Controlling Authority

COR—Central Office of Record

CPSG—Cryptologic Systems Group

CRO—COMSEC Responsible Officer

CSM—Code Storage Module

CTG—Code Transfer Group

CTU—Code Transfer Unit

DA—Data Authenticator

DCS—Defense Courier Service

DIRNSA—Director, National Security Agency

DMS—Defense Message System

DTRA—Defense Threat Reduction Agency

EAL—Entry Authorization List

EAP—Emergency Action Plan

EPROM—Erasable Programmable Read-Only Memory

GSA—General Services Administration

IAAP—Information Assurance Assessment and Assistance Program

IC—Integrated Circuit

ID—Identification

IDS—Intrusion Detection System

INITS—Initials

LMF—Local Monitoring Facility

MFO—Monitoring Facility Operator

MP—Message Processor

MPHD—Message Processor Hard Drive

MSK—Mission Support Kit

MUNSS—Munitions Support Squadron

NOFORN—Not Releasable to Foreign Nationals

PAS—Protected Aircraft Shelter

PRP—Personnel Reliability Program

RMF—Remote Monitoring Facility

SCP—Shelter Control Panel

SP—Sensor Processor

TD—Time Delay

T.O.—Technical Order

TPC—Two Person Control

UA—User Agency

UPS—Uninterrupted Power Supply

URC—Universal Release Code

USAFE—United States Air Forces in Europe

VP—Vault Processor

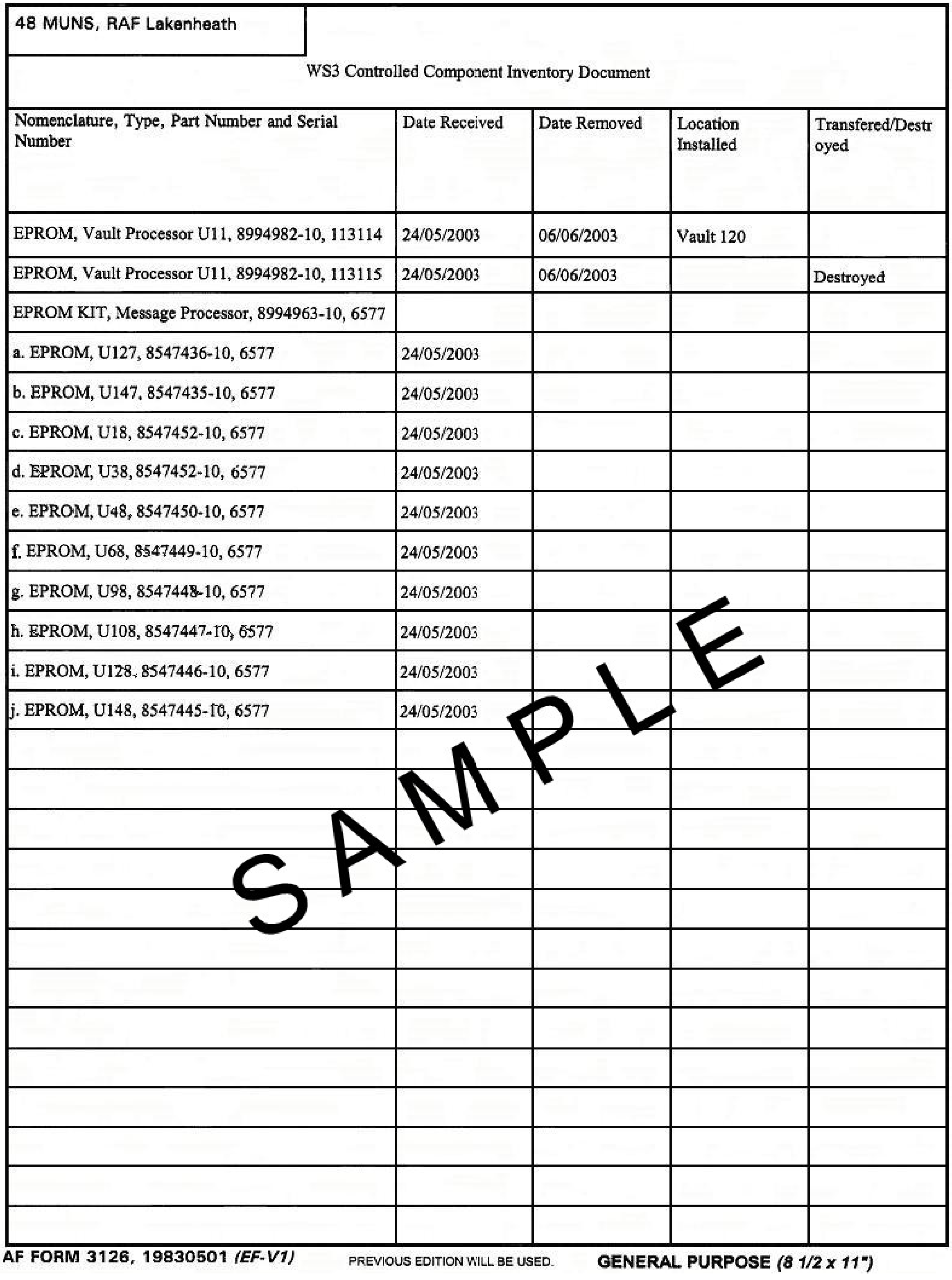
WS3—Weapon Storage and Security System

WSV—Weapons Storage Vault

Attachment 2

WS3 CONTROLLED COMPONENT INVENTORY DOCUMENT

Figure A2.1. Example of AF Form 3126, WS3 Controlled Component Inventory Document



48 MUNS, RAF Lakenheath

WS3 Controlled Component Inventory Document

Nomenclature, Type, Part Number and Serial Number	Date Received	Date Removed	Location Installed	Transfered/Destroyed
EPROM, Vault Processor U11, 8994982-10, 113114	24/05/2003	06/06/2003	Vault 120	
EPROM, Vault Processor U11, 8994982-10, 113115	24/05/2003	06/06/2003		Destroyed
EPROM KIT, Message Processor, 8994963-10, 6577				
a. EPROM, U127, 8547436-10, 6577	24/05/2003			
b. EPROM, U147, 8547435-10, 6577	24/05/2003			
c. EPROM, U18, 8547452-10, 6577	24/05/2003			
d. EPROM, U38, 8547452-10, 6577	24/05/2003			
e. EPROM, U48, 8547450-10, 6577	24/05/2003			
f. EPROM, U68, 8547449-10, 6577	24/05/2003			
g. EPROM, U98, 8547448-10, 6577	24/05/2003			
h. EPROM, U108, 8547447-10, 6577	24/05/2003			
i. EPROM, U128, 8547446-10, 6577	24/05/2003			
j. EPROM, U148, 8547445-10, 6577	24/05/2003			

SAMPLE

AF FORM 3126, 19830501 *(EF-V1)* PREVIOUS EDITION WILL BE USED. **GENERAL PURPOSE *(8 1/2 x 11")***