BY ORDER OF THE COMMANDER
KADENA AIR BASE (PACAF)

KADENA AIR BASE INSTRUCTION 33-201

10 OCTOBER 2012

Communications and Information

WING COMSEC PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: 18 CS/SCXS

Certified by: 18 CS/CC
(Lt Col Todd R. Stratton)

Supersedes: 18WGI33-201, 3 February 2010

Pages: 42

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* and contains specific procedures, Air Force Instruction (AFI) 33-201, vol. 1, *Communication Security (COMSEC)*, AFI 33-201, vol. 2, *Communications Security User Requirements*, AFI 33-201, vol. 4, *Cryptographic Access Program*, AFI 33-201, vol. 5, *Controlled Cryptographic Items*, AFI 33-201, vol. 7, *Management of Cryptosystems*, AFI 33-201, vol. 9, *Operational Instructions for Secure Voice Devices,* Air Force System Security Instruction (AFSSI) 3014, *Operational Security Instruction for the Motorola Network Encryption System,* and AFSSI 4212 *Reporting COMSEC Deviations,* to effectively establish the local COMSEC Program. This instruction provides direction for the implementation of a base-wide COMSEC program at Kadena Air Base (AB), Okinawa. It applies to all 18th Wing military, civilian, contract personnel and units assigned or attached, or operational control (OPCON) to the 18th Wing and all tenant units and Air National Guard or US Air Force Reserve personnel at Kadena AB.

Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through Major Command (MAJCOM) publications/forms managers. Ensure that 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 Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

SUMMARY OF CHANGES

This publication is updated to reflect changes involving Disposition Record Cards (DRC) and audit trails. Other changes to this publication include additions to the COMSEC accountant and Secure Voice Responsible Officer responsibilities. Additional updates include minor changes to some of the attachments.

1. General.

1.1. Program Objectives.

1.1.1. The *Communication Security* COMSEC program is designed to enable personnel to reach the following base goals:

1.1.1.1. To provide COMSEC Responsible Officers (CROs) and Secure Voice Responsible Officers (SVROs) with detailed procedures for protecting and safeguarding and destroying COMSEC material.

1.1.1.2. To ensure a recognizable, comprehensive base-wide COMSEC program.

1.1.1.3. To develop and implement procedures and policies to prevent COMSEC deviations or incidents.

1.2. Program Administration.

1.2.1. The Kadena COMSEC program will be administered at two levels:

1.2.1.1. Wing Level:

1.2.1.1.1. The COMSEC element of the Wing Information Assurance Office will be responsible for obtaining and issuing COMSEC material to local element accounts (LE), providing guidance and establishing base COMSEC policy and inspecting local elements for compliance with the program outlined within this operating instruction.

1.2.1.2. Organization Level:

1.2.1.2.1. Base organizations will be responsible for compliance with published COMSEC policy and implementation of COMSEC programs.

2. Responsibilities.

2.1. COMSEC element of the Wing Information Assurance Office.

2.1.1. COMSEC Managers.

2.1.1.1. Administer a formal and effective base-wide COMSEC program.

2.1.1.2. Develop, publish, and disseminate COMSEC policies and procedures.

2.1.1.3. Establish a comprehensive user-training program for all CROs/ Secure Voice Responsible Offers (SVRO) and alternates. Document initial and refresher training on the AF Form 4168, COMSEC Responsible Officer and User Training Checklist. Create a separate training checklist for each CRO/SVROs and alternates. Provide annual refresher training to CRO/SVROs and alternates by completing a new AF Form 4168 annually. Maintain only the most current form on file. Ensure CRO/SVROs conduct user training for all personnel having access to COMSEC material according to AFI 33-211.

2.1.1.4. Provide COMSEC guidance to local element CROs/SVROs.

2.1.1.5. Review and endorse all local element Operating Instructions and Emergency Action Plans.

2.1.1.6. Perform a semiannual assessment of both the account and all users according to AFI 33-230 and AFKAG-2. Keep written documentation of the semiannual assessment from one command COMSEC assessment to the next.

2.1.1.7. Conduct the required semiannual inventory according to AFKAG-2.

2.1.1.8. Ensure COMSEC material is issued only to local element personnel with appropriate clearance, training and legitimate need-to-know.

2.1.1.9. Ensure the COMSEC account maintains minimum on-hand requirements and holds only COMSEC material that is mission essential. Request increased aids or disposition instructions for surplus or unneeded material, as required.

2.1.1.10. Ensure COMSEC material is destroyed within prescribed timeframes.

2.1.1.11. Investigate and report all suspected or known COMSEC incidents.

2.1.1.12. Maintain records for CRO/SVRO appointment and training, local element inspections, COMSEC material issue, COMSEC material destruction and COMSEC deviations.

2.1.1.13. Ensure all COMSEC local elements are complying with Cryptographic Access Program (CAP) procedures.

2.1.1.14. Destroy COMSEC aids according the AFKAG-1 and ensure users destroy COMSEC aids according to AFI 33-201 volume 1.

2.1.1.15. Oversee daily operations within the COMSEC main-account.

2.1.1.16. Correct any deficiencies involving procedures at the account.

2.1.2. Main Account COMSEC Accountants.

2.1.2.1. Issue COMSEC material to local element personnel with appropriate clearance, training and legitimate need.

2.1.2.2. Provide local element personnel information regarding effective dates, supersession dates and physical security requirements.

2.1.2.3. Review local element Simple Key Loader (SKL) audit trails. Ensure 100% audit trail review is conducted quarterly.

2.1.2.4. Register at the (**https://www.iad.gov/SecurePhone/index.cfm**) website and conduct all STE software upgrades for the SVROs assigned to the account.

2.1.2.5. Obtain minimum COMSEC aides needed to meet the operational requirements of local elements.

2.1.2.6. Interact with Controlling Authorities on behalf of the local elements.

2.1.2.7. Disseminate official message traffic pertaining to COMSEC material to appropriate local elements.

2.1.2.8. Maintain a six-part folder for each local element.

2.1.2.9. Conduct initial and refresher training for all appointed CRO/SVROs assigned to the account.

2.2. Unit Commanders: The Commander of each unit that requires COMSEC material:

2.2.1. Appoints a Primary and at least one Alternate CRO/SVRO in writing. CROs/SVROs will be active duty military or US Department of Defense civilian employees. Primary CROs/SVROs will have a minimum grade requirement of E-5 or GS-5 equivalent. Alternate CROs/SVROs will have a minimum grade requirement of E-4 or GS-4 equivalent.

2.2.2. Commanders approve waivers for personnel with lower grades. Process all waivers through the COMSEC manger.

2.2.3. Change CROs if the CRO will be deployed or on Temporary Duty (TDY) for more than 90 days, or is pending a transfer.

2.3. COMSEC Responsible Officers:

2.3.1. Provide a copy of the appointment letter to the COMSEC office and maintain the original in the continuity binder (see **Attachment 2**).

2.3.2. Upon appointment by unit commander, attend initial training. Attend refresher training annually. Obtain a copy of your AF Form 4168, *COMSEC Responsible Officer and User Training Checklist*, from the COMSEC office and maintain in your Continuity Binder. A new AF Form 4168 will be accomplished each year during refresher training.

2.3.3. Notify the COMSEC office in writing, of any new requirements, changes (increase or decrease), or pending requirements to existing requirements.

2.3.4. Review annually the requirement for COMSEC material according to AFI 33-201 volume 2.

2.3.5. Upon appointment of a new primary CRO/SVRO, request a COMSEC material report of the local elements COMSEC holdings from the COMSEC office, and perform a physical inventory, accounting for all holdings. The incoming and outgoing CROs/SVROs must both participate in this inventory. After all holdings have been reconciled, request a consolidated inventory from the COMSEC office. Sign and file this document in your continuity binder and dispose of all previously held hand receipts. Additionally, upon appointment of a new Primary CRO/SVRO, a self-inspection will be performed, a new COMSEC requirement letter will be drafted with the new CRO/SVRO signature, and all COMSEC documents will be page checked. Both the outgoing and incoming CRO/SVROs participate in accomplishing these tasks.

2.3.6. Devise and implement a unit COMSEC program that complies with this instruction, AFI 33-201, vol. 1, AFI 33-201, vol. 2, AFI 33-201, vol. 4, AFI 33-201, vol. 5, AFI 33-201, vol. 7, AFI 33-201, vol. 9, AFSSI 4212, AFSSI 3014 (if applicable), and AFSSI 3035, *Operational Systems Security Instruction for TACLANE (KG-175)* - if applicable.

2.3.7. Part of the COMSEC program implementation will consist of the development of an account operating instruction. Account operating instruction will establish local procedures on storing, handling, controlling, accessing, and inventorying of COMSEC material, protective technology inspection, keying and rekeying procedures for Controlled Cryptographic Items (CCI), Two Person Integrity (TPI – if applicable), Cryptographic Access Program (CAP), destruction, Emergency Action Plan (EAP)

implementation, incident reporting and a requirement for the CRO to obtain COMSEC manager clearance from responsibility prior to a permanent change of station (PCS), permanent change of assignment (PCA), or a deployment or TDY of over 90 days. Coordinate account operating instruction through the COMSEC office and maintain it and the coordination sheet in a continuity binder.

2.3.8. Accomplish a COMSEC requirements letter (see **Attachment 3**). This letter justifies the need for requested COMSEC keys within a local element. Maintain this letter in your continuity binder and provide a copy to the wing COMSEC office along with proof of cryptographic equipment registration into the Standard Base Supply System (SBSS) via a CA/CRL (R-14). Re-accomplish the requirements letter annually, when requirements change, or when CRO/SVRO changeover occurs.

2.3.9. Ensure only authorized and trained users have access to COMSEC material by accomplishing a COMSEC access list (see **Attachment 4**), ensuring individual clearances are verified in the process. Re-verify or re-accomplish this list monthly by listing each month at the bottom of the access list and initialing for each month after verification is complete. Do not retain old access lists to show documentation of monthly reviews. The access list must be re-accomplished annually or when an addition to the access list is required.

2.3.10. Train all personnel on the COMSEC access list annually. Annotate this training on AF Form 4168 and maintain these forms in your continuity binder.

2.3.11. Ensure all personnel on the COMSEC access list perform semi-annual required reading. This reading will consist of Emergency Action Plan (EAP) dry-runs (i.e. a walk through), reviewing AFI 33-201, vol. 1, and AFI 33-201 vol. 2, AFI 33-201 vol. 4, AFI 33-201 vol. 5, and AFI 33-201 vol. 9 (volume 9 is only required for CROs performing SVRO functions). Have the individuals sign a document stating they have performed these actions (see **Attachment 5**) and maintain in the continuity binder.

2.3.12. Limit COMSEC material access to those personnel listed on the COMSEC access list. The only individuals not on the COMSEC access list who can access your holdings are the COMSEC Manager, the Alternate COMSEC Manager, wing COMSEC accountants and IG inspectors who are trained and enrolled in CAP. Track access by these individuals via AF Form 1109, *Visitor Register Log*. Maintain this log in your continuity binder from inspection to inspection.

2.3.13. Develop EAPs to ensure the safeguarding of all COMSEC material and keyed CCI items during fire, bomb threat or emergency evacuation scenarios. Additionally, develop EAPs for priority and emergency destruction of COMSEC. Coordinate the EAPs through the COMSEC office and conduct dry runs at least semi-annually. Post the EAPs and coordination sheet in a conspicuous location where they can be easily located when needed.

2.3.14. Pick-up COMSEC from the main-account at the designated time. Be advised that the main-account will not issue COMSEC material to any CRO overdue for training, not on an updated appointment letter and any local element that has not provided wing COMSEC with their SKL audit trails (see **Attachment 20**). CROs late for or missing their designated pick-up time will be rescheduled by the COMSEC office after all other

accounts receiving issues have been processed. When picking-up COMSEC, always bring your continuity binder, Data Management Device (DMD) laptop and SKL audit trails with you. Maintain Standard Form (SF) 153, *COMSEC Material Report;* used for hand receipt issued during pick-up in your continuity binder until it becomes inactive (i.e. all items listed are destroyed).

2.3.15. Maintain constant accountability for all COMSEC material and aides within your account. Document the inventory of COMSEC material on AFCOMSEC Form 16, *COMSEC Account Daily Shift Inventory,* once per shift when a safe is opened (see **Attachment 6**). Be advised that inventories must also be maintained for deployed COMSEC material. All AFCOMSEC Form 16s must be stamped for official use only (FOUO). Maintain the current AFCOMSEC Form 16 in your safe. Maintain inventories for the prior 6 months in your continuity binder.

2.3.16. Ensure correct procedures are followed by personnel within your unit deploying with COMSEC as defined in **Attachment 7**.

2.3.17. Ensure all opening and closing of safes is documented on SF 702, *Security Container Checksheet.*

2.3.18. Change safe combinations at least annually. Document the changes on SF 700, *Security Container Information*, and post inside the locking drawer of the applicable safe. Conduct a visual inspection after the combo change and document the inspection on an AFTO Form 36, *Maintenance Record for Security Type Equipment*.

2.3.19. Ensure a preventive maintenance inspection (PMI) is conducted by the Civil Engineering Squadron (CES) every five years for safe drawers and every two years for vault doors. Document the preventive maintenance on an AFTO Form 36.

2.3.20. Be familiar with your short-title holdings and their effective and supersession dates.

2.3.21. Maintain three years worth of Disposition Record Certificates (DRC). As of Apr 2012 DRCs are no longer required due to the implementation of 100% audit trail reviews. However, three years worth of DRCs are still to be maintained and are inspectable. Example: If a DRC was accomplished in March 2012 that DRC must remain in your continuity binder until March of 2015, at which time the DRC may be destroyed.

2.3.22. Store all pulled key tape segments in a sealed opaque envelope until the pulled segments are destroyed. These envelopes will be sealed and their outside labeled with the appropriate short title, edition and segment number. During COMSEC semi-annual inspections, all sealed opaque envelopes will be opened for inventory purposes.

2.3.23. Destroy COMSEC within a 12-hour window after its supersession (see **Attachment 10**). Document this destruction, to include electronic key, on SF 153 as a destruction report. Provide the COMSEC Office a copy of the Destruction Report within 48 hours. Be advised that late destruction will at minimum be considered a Practice Dangerous to Security (PDS).

NOTE: Offices using COMSEC material that do not normally operate during weekends (normal or extended) must destroy superseded material on the first duty day after the weekend.

2.3.23.1. The requirement for opening a safe to specifically perform destruction of daily electronic key segments on an SKL is waived. However, the electronic key edition must be destroyed within 12 hours of supersession. Accounts with daily electronic key segments loaded on an SKL will be required to perform at least weekly destruction of the daily key segment. If the safe is entered more than once a week, all required destruction must be performed upon opening the safe.

2.3.24. Perform page checks of COMSEC documents as required by AFI 33-201, vol. 2, paragraph 22, and during changeover of primary CROs.

2.3.25. Perform self-inspections every 90 days. Utilize the Self-Inspection Checklist and maintain this form in your continuity binder from inspection to inspection.

2.3.26. Maintain SF 701, *Activity Security Checklist*, in all areas where COMSEC is utilized or stored to include areas with safes and NES/TACLANE devices. Ensure there are appropriate entries (examples: Safe CS04 has been secured and checked; NES key removed from device and properly secured) and that this form is completed at the end of each work day, or for 24/7 operations, the beginning of each shift.

2.3.27. Provide written response to COMSEC inspection reports within 10 duty days. Continue to provide written responses every 30 days until all findings have been resolved.

2.3.28. Report all known or suspected COMSEC incidents and PDS to the COMSEC manager. Maintain all generated paperwork for 1 year after Air Force Network Information Center (AFNIC) (incident) or local (PDS) closeout date.

2.3.29. Perform the duties of CAP Administrator as outlined in AFI 33-201, vol. 4, if applicable. Approval authority for CAP Administrator appointment is unit commander. Provide the wing COMSEC office with a copy of the appointment letter and file copy in continuity binders. Enroll all personnel on COMSEC Access Lists in CAP by completing an AFCOMSEC Form 9, *Cryptographic Access Certificate (PA)*, and remove them from the program when removed from COMSEC Access List. Forward all original enrollment/removal AFCOMSEC Forms 9, to the COMSEC office and maintain a copy in your Continuity Binder for 90 days after the individual has been removed from the program.

2.3.30. Request annually COMSEC Material Report from the wing COMSEC office and account for all holdings. After all holdings have been 100% reconciled, sign a consolidated hand receipt via SF Form 153 and file a copy in the continuity binder and provide the COMSEC office with the original. Dispose of all previously held hand receipts.

2.3.31. Maintain a continuity binder. Its contents will include: CRO Appointment Letter; COMSEC requirements letter; COMSEC access list; AF Form 4168s; CAP manager appointment letter; User CAP Paperwork; Two Person Integrity (TPI) Team Paperwork (if applicable); signed Consolidated Hand Receipt dated within the last year; signed Hand Receipts for material received since posting Consolidated Hand Receipt; signed Destruction Reports; AFCOMSEC Form 16, which is rendered (inactive) and kept for 6 months; Semi-Annual KSV-21 Inventory; COMSEC Incident and PDS documentation; COMSEC Inspection and Self-Inspection documentation. Additionally, a

second binder (or set of binders) should be maintained (if needed for additional space) containing the following: Quarterly EAP dry-run and required reading documentation; this instruction; your account operating instruction; AFI 33-201, vol. 1, AFI 33-201, vol. 2, AFI 33-201, vol. 4, AFI 33-201, vol. 5, AFI 33-201, vol. 7, AFI 33-201, vol. 9, AFSSI 4212, AFSSI 3014 (if applicable), AFSSI 3035 (if applicable), and Secure Telephone Equipment (STE) Users Guide.

2.3.32. Ensure TPI procedures are followed – where applicable (see AFI 33-201, vol. 2).

2.3.33. Secure Voice Responsible Offers:

2.4. Secure Voice Responsible Offers: SVROs are required in units that have no other COMSEC devices other than secure telephone equipment (STE). In units with other devices, CROs will perform the duties of an SVRO. In units with STEs only, the unit commander will appoint a primary and at least one alternate SVRO in writing. SVROs will be active duty military or US Department of Defense (DoD) civilian employees. Primary SVROs will have a minimum grade requirement of E-5 or GS-5. Alternate SVROs will have a minimum grade requirement of E-4 or GS-4.

2.4.1. Provide a copy of the appointment letter to the COMSEC office and maintain the original in the continuity binder (see **Attachment 2**).

2.4.2. Upon appointment by unit commander, attend initial training. Attend refresher training annually. Obtain a copy of your AF Form 4168, *COMSEC Responsible Officer and User Training Checklist*, from the COMSEC office and maintain in the continuity binder. A new AF Form 4168 will be accomplished each year during refresher training.

2.4.3. Upon appointment of a new primary SVRO, request an Inventory Worksheet from the COMSEC office and perform a physical inventory to account for all holdings. The incoming and outgoing SVROs must both participate in this inventory. After all holdings have been 100% reconciled, request a Consolidated Inventory from the COMSEC office. Sign and file this document in your continuity binder and dispose of all previously held hand receipts. Additionally, upon appointment of a new Primary SVRO, a self-inspection will be performed. Both the outgoing and incoming SVRO will participate in this task.

2.4.3.1. Devise and implement a unit STE program that complies with this wing instruction, AFI 33-201, vol. 9, AFSSI 4212, and AFI 33-201, vol. 5.

2.4.3.1.1. Part of the COMSEC program implementation will consist of the development of an account operating instruction. Account operating instruction will establish local procedures on storing, handling, controlling, accessing, and inventorying of COMSEC material, protective technology inspection, keying and rekeying procedures for Controlled Cryptographic Items (CCI), Two Person Integrity (TPI – if applicable), CAP, destruction, EAP implementation, incident reporting and a requirement for the SVRO to obtain COMSEC manager clearance from responsibility prior to a PCS, PCA, or a deployment or TDY of over 90 days. Coordinate account operating instruction through the COMSEC office and maintain it and the coordination sheet in a continuity binder.

2.4.4. Request COMSEC material as required (see **Attachment 12** - **be advised that first-time STE key requirements are accomplished via a Military Interdepartmental Purchase Request [MIPR] to Headquarters Electronic Device Center [HQ ESC]**). Provide the wing COMSEC office a copy of this letter and maintain the original in the account continuity binder.

2.4.5. Accomplish a COMSEC access list (see **Attachment 13**); ensuring individual clearances are verified in the process. Re-verify or re-accomplish this list monthly by listing each month at the bottom of the access list and initialing each month after verification is complete. Maintain this letter in the account continuity binder.

2.4.6. Train all personnel on the COMSEC access list annually. Annotate this training on AF Form 4168, and maintain these forms in the account continuity binder.

2.4.7. Limit COMSEC material access to those personnel listed on the COMSEC access list. The only individuals not on the COMSEC access list who can access your holdings are the COMSEC manager, the alternate COMSEC manager, wing COMSEC accountants and Inspector General (IG) inspectors who are trained and enrolled in CAP. Track access by these individuals via AF Form 1109. Maintain the AF Form 1109 for one year.

2.4.8. Develop EAPs to ensure the safeguarding of all COMSEC material and keyed CCI items during fire, bomb threat or emergency evacuation scenarios. Additionally, develop EAPs for priority and emergency destruction of COMSEC. Coordinate the EAPs through the COMSEC office and post the EAPs along with the coordination sheet in a conspicuous location where they can be easily located when implemented.

2.4.9. Ensure all personnel on the COMSEC access list perform semi-annual required reading. This reading will consist of EAP dry-runs (i.e. a walk through), reviewing AFI 33-201, vol. 2, AFI 33-201, vol. 9, AFSSI 4212, and your account operating instruction. Have the individuals sign a document stating they have performed these actions (see **Attachment 5**) and maintain in the accounts continuity binder from inspection to inspection.

2.4.10. Accomplish a secure voice device access list at least annually, listing all individuals who utilize or work around STEs, Iridium phones, OMNI terminals and SECTERA wireline terminals (SWT) and Global System for Mobiles (GSMs) within your unit (see **Attachment 13**). Ensure all individuals listed on this letter complete the appropriate certification annually (see **Attachment 14**). Re-verify or re-accomplish this list monthly by listing each month at the bottom of the access list and initialing each month after verification is complete Maintain the Access List and certifications in the account continuity binder.

2.4.11. Ensure TPI procedures are followed – if applicable (see AFI 33-201, vol. 2).

2.4.12. Ensure correct KSV-21 management and re-key procedures are followed within your account (see **Attachments 15 and 16**). KSV-21 cards require a re-key annually to ensure secure voice capabilities. However, a re-key of the KSV-21 card may be conducted at any point throughout the year (doing so will extend the key for one year from re-key date).

2.4.13. Ensure SECTERA and OMNI procedures are followed within your account (see **Attachment 17**).

2.4.14. Pick-up COMSEC from the main-account when required. Be advised that the main-account will not issue COMSEC material to any SVRO overdue for training and/or not on a current appointment letter. When picking-up, always bring your continuity binder with you. Maintain the SF 153 issued during pick-up in the account continuity binder until it becomes inactive (i.e. all items listed are destroyed).

2.4.15. Maintain constant accountability for all COMSEC material and aides within your account. Document the inventory of COMSEC material on AFCOMSEC Form 16, *COMSEC Account Daily Shift Inventory,* once per shift when a safe is opened (see **Attachment 6**). Be advised that inventories must also be maintained for deployed COMSEC material. All AFCOMSEC Form 16s must be stamped for official use only (FOUO). Maintain the current AFCOMSEC Form 16 in your safe. Maintain inventories for the prior 6 months in your continuity binder.

2.4.16. Ensure all opening and closing of safes is documented on SF 702.

2.4.17. Change safe combinations at least annually. Document the changes on SF 700 and post in the locking drawer of applicable safe.

2.4.18. Destroy COMSEC within a 12-hour window after its supersession (see **Attachment 10**). Document this destruction on SF 153 as destruction report and provide a copy to the COMSEC office and maintain a copy in the account continuity binder for 3 years. Late destruction will at minimum be considered a practice dangerous to security.

2.4.19. Ensure only individuals on the COMSEC access list perform keying operations on STEs. Rekeys can be performed by anyone on the Secure Voice Device Access List and should be accomplished semi-annually on all STEs, Iridiums, OMNIs, SECTERAs and GSMs devices.

2.4.20. Ensure that STEs are installed in locations that adhere to a common-sense approach to acoustic security concerns as well as ensuring Emission Security (EMSEC) requirements are met. All personnel assigned to the area where the STE is located should have the same security clearance as the STE key. Where this is not possible or practical, develop and implement local procedures to prevent unauthorized personnel from accessing the device or overhearing classified telephonic conversations.

2.4.21. Maintain SF 701 in all areas where COMSEC is utilized or stored – to include areas with safes, STEs. Ensure there are appropriate entries (examples: Safe CS04 has been secured and checked; KSV-21 removed from phone and properly secured) and that this form is completed at the end of each work day, or for 24/7 operations, the beginning of each shift.

2.4.22. Ensure Controlled Cryptographic Item equipment is zeroized before any personnel not on your COMSEC Access List perform maintenance on the device (see **Attachment 16**).

2.4.23. Accomplish a STE Private Residence Letter for all STEs installed in private quarters (see **Attachment 18**). Provide a copy to the COMSEC office and maintain a copy in the account continuity binder.

2.4.24. Accomplish and document a KSV-21 inventory, accounting for all KSV-21s keyed into STEs (see **Attachment 19**). This letter should be drafted whenever a new KSV-21 is initialized or at least semi-annually. Provide a copy of this letter to the wing COMSEC office and maintain a copy in the account continuity binder.

2.4.25. Provide written response to COMSEC inspection reports within 10 duty days. Continue to provide written responses every 30 days until all findings have been resolved.

2.4.26. Report all known or suspected COMSEC incidents and Practice Dangerous to Security (PDS) to the COMSEC manager. Maintain all generated paperwork for 1 year after AFNIC (incident) or local PDS closeout date.

2.4.27. Perform the duties of CAP administrator as outlined in AFI 33-201, vol. 4, if applicable. Approval authority for CAP Administrator appointment is unit commander. Provide the wing COMSEC office with a copy of the appointment letter and file copy in continuity binders. Enroll all personnel on COMSEC Access Lists in CAP by completing an AFCOMSEC Form 9, *Cryptographic Access Certificate (PA)*, and remove them from the program when removed from COMSEC Access List. Forward all original enrollment/removal AFCOMSEC Forms 9, to the COMSEC office and maintain a copy in your Continuity Binder for 90 days after the individual has been removed from the program.

2.4.28. Request annually COMSEC Material Report from the wing COMSEC office and account for all holdings. After all holdings have been 100% reconciled, sign a consolidated hand receipt via SF Form 153 and file a copy in the continuity binder and provide the COMSEC office with the original. Dispose of all previously held hand receipts.

2.4.29. Maintain a continuity binder. Its contents will include: SVRO appointment letter; Secure Voice Device Key requirements letter; COMSEC access list; Secure Voice Device access list; AF Form 4168s; Secure Voice Device User Certification Paperwork; CAP Manager appointment letter; user CAP Paperwork; AFCOMSEC Form 9, TPI Team Paperwork (if applicable); signed Consolidated Hand Receipt dated within the last year; signed hand receipts for material received since posting Consolidated Hand Receipt; signed destruction reports; AFCOMSEC Form 16, which is rendered (inactive) and kept for 6 months; STE Private Residence Letter; Semi-Annual KSV-21 Inventory; copies of converted STEs; COMSEC Incident and PDS documentation; COMSEC Inspection and Self-Inspection documentation; semi-annual (quarterly for 353 SOG associated units) EAP dry-run and required reading documentation; this wing instruction; Your account operating instruction; copies of AFI 33-201, vol. 9, AFI 33-201, vol. 4 (if applicable), and AFI 33-201, vol. 5.

MATTHEW H. MOLLOY, Brigadier General, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 33-2, *Information Protection,* 3 August 2011

AFI 33-201, vol. 1, *Communication Security (COMSEC,* 1 May 2005

AFI 33-201, vol. 2, *Communications Security User Requirement,* 26 April 2005

AFI 33-201, vol. 4, *Cryptographic Access Program,* 15 April 2005

AFI 33-201, vol. 5, *Controlled Cryptographic Items,* 13 May 2005 incorporating through change 1, 8 June 2009

AFI 33-201, vol. 7, *Management of Cryptosystems,* 11 May 2005

AFI 33-201, vol. 9, *Operational Instructions for Secure Voice Devices*, 13 April 2005

AFSSI 3014, *Operational Security Instruction for the Motorola Network Encryption System,* 23 July 2003

AFSSI 3021, *Operational Instruction for the AN/CYZ-10/10-A Data Transfer Device*, 23 July 2003

AFSSI 3035, *Operational Systems Security Instruction for TACLANE (KG-175),* 16 May 2001

AFSSI 4212, *Reporting COMSEC Deviations,* 25 Jul 2007

AFI 33-230, *Information Assurance Assessment and Assistance Program,* 4 August 2004

AFKAG-1N, *Air Force COMSEC Operations*, 27 January 2003

Amend 1 to AFKAG 1N, *Air Force COMSEC Operations,* 27 February 2003

Amend 2 to AFKAG 1N, *Air Force COMSEC Operations,* 18 July 2003

Amend 3 to AFKAG 1N, *Air Force COMSEC Operations,* 19 September 2003

Amend 4 to AFKAG 1N, *Air Force COMSEC Operations,* 24 March 2004

AFKAG-2, *Air Force COMSEC Accounting Manual,* 15 May 2007

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 1109, *Visitor Register Log*

AF Form 4167, *Two-Person COMSEC Material Inventory*

AF Form 4168, *COMSEC Responsible Officer and User Training Checklist*

AFCOMSEC Form 9, *Cryptographic Access Certificate (PA)*

AFCOMSEC Form 16, *COMSEC Account Daily Shift Inventory*

AFCOMSEC Form 16s, *COMSEC Physical Inventory*

AFTO Form 36, *Maintenance Record for Security Type Equipment*

SF 153, *COMSEC Material Report*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Checksheet*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFSSI—Air Force Systems Security Instruction

CAP—Cryptographic Access Program

CIK—Crypto Ignition Key

COMSEC—Communications Security

CRO—COMSEC Responsible Officer

DRC—Disposition Record Card

EAP—Emergency Action Plan

EMSEC—Emission Security

NES—Network Encryption Server

OI—Operating Instruction

PCA—Permanent Change of Assignment

PCS—Permanent Change of Station

PDS—Practice Dangerous to Security

SKL—Simple Key Loader

STE—Secure Telephone Equipment

SVRO—Secure Voice Responsible Officer

TDY—Temporary Duty

TPI—Two Person Integrity

Attachment 2

SAMPLE CRO/SVRO APPOINTMENT LETTER

Figure A2.1. Sample CRO/SVRO Appointment Letter

MEMORANDUM FOR 18 CS/SCXS DATE

FROM: (*Unit/Office Symbol*)

SUBJECT: Appointment of COMSEC Responsible Officer & Alternate, Secure Telephone Responsible Officer and Alternates, and Cryptographic Access Program Administrator & Alternate

1. The individuals listed below have been appointed the COMSEC and/or Secure Telephone Responsible Officer's for my unit. Appointees are responsible for maintaining the *(identify your unit and office symbol*) COMSEC program IAW AFI 33-201 v1, v2, v9 and AFSSI 4212. Appointees can receive and carry all COMSEC materials issued, up to and including *(the classifications indicated below)* directly between 18 CS/CA632312 building 400 and _____ (*users unit and building number*). They will make sure that all applicable materials they receive are entered on their daily inventory and are responsible for other actions required of users of COMSEC materials by AFI 33-201 volume 2, and AFI 33-201 volume 9. These individuals have been granted access to classified COMSEC information and appropriate documentation is on file.

2. The individuals listed below are authorized to grant access and withdraw access in the commander's name to all personnel who require, or have authorized access to classified cryptographic information IAW AFI 33-201 v4.

Name/Rank	SSN	Clearance	Duty Phone	Home Phone	DEROS

Use a "*" to designate Primary CRO Status.
Use a "**" to designate Primary SVRO if not the Primary CRO.
Use a "# to designate Primary CAP Administrator Status
Use a "##" to designate Alternate CAP Administrator Status.

PRIVACY ACT INFORMATION
This information is subject to the Privacy Act of 1974 and is **FOR OFFICIAL USE ONLY**

3. CRO/SVROs are responsible to ensure all COMSEC users on the account are trained via an AF Form 4168, have a signed AFCOMSEC Form 9 on file and are enrolled in the Cryptographic Access Program (CAP) IAW AFI 33-201 (18 WG), AFI 33-201 v2, & 9, AFSSI 4212, and Local Emergency Action Plans.

4. A replacement CRO/SVRO will be appointed in writing 90 days prior to a primary or alternate CRO/SVRO deployment or TDY that will be longer than 90 days or any PCS or PCA. It is the CRO/SVROs responsibility to route a new appointment letter to the unit commander.

5. This letter supersedes all previous letters from this office of the same subject.

Commander's Signature Block

DATE

1st Ind, (***Squadron/Security Managers Office Symbol***)

MEMORANDUM FOR 18CS/CA632312

I have verified the names, clearances, and U.S. citizenship of all individuals listed above using the unit Clearance and Access Verification System (CAVS).

Security Manager's Signature Block

PRIVACY ACT INFORMATION
This information is subject to the Privacy Act of 1974 and is **FOR OFFICIAL USE ONLY**

Attachment 3

SAMPLE COMSEC REQUIREMENT LETTER

***NOTE*: The information you put on this form may be classified. Think before you decide to process the request on an unclassified computer, you may need to use a classified system. Be advised that TACLANE, secure voice devices (STE, Iridium, GSM, SECTERA and OMNI) keys are not listed on this letter (see Attachment 13).**

Figure A3.1. Sample COMSEC Requirement Letter

MEMORANDUM FOR 18 CS/SCXS DATE

FROM: ***Unit and CRO Account Number and DAO Code***

SUBJECT: COMSEC Requirements Letter

1. COMSEC requirements for ***CRO Account Number*** are:

Short Title	On Hand	Change	Electronic or Physical	Authorization Justification Code

Authorization/Justification Code Legend

2. This letter supersedes all previous letters with the same subject. POC is ***Name and Rank*** at ***Duty Phone***.

3. Attached is proof that the equipment has been entered into the Standard Bases Supply System according to AFMAN 23-110.

CRO Signature Block

Attachment 4

SAMPLE COMSEC ACCESS LIST

Figure A4.1. Sample COMSEC Access List

MEMORANDUM FOR COMSEC ACCOUNT 632312 DATE

FROM: ***Unit and CRO Account Number***

SUBJECT: Communications Security (COMSEC) Access List

1. The following individuals are granted access to the COMSEC material associated with this account. Their clearances have been verified through the Unit Security Manager, they have a valid need to know and their COMSEC training has been documented and is on file.

Name/Rank **SSN** **Clearance**

2. All personnel with an asterisk (*) next to their name have authority to grant access to others not listed who have a valid need to know. They will sign these individuals in on AF Form 1109, *Visitor Register Log*, before giving them access to COMSEC information.

3. This letter supersedes all previous letters with the same subject. POC is ***Your Name and Rank*** at ***Duty Phone***.

CRO Signature Block

1st Ind, (***Squadron/Security Managers Office Symbol***)

MEMORANDUM FOR 18CS/CA632312

I have verified the names, clearances, and U.S. citizenship of all individuals listed above using the unit Clearance and Access Verification System (CAVS).

Security Manager's Signature Block

VERIFY ALL INDIVIDUALS SECURITY CLEARANCES MONTHLY; ANNOTATE VERIFICATION BY INITIALING THE BOTTOM OF THE ACCESS LIST.

PRIVACY ACT INFORMATION

This information is subject to the Privacy Act of 1974 and is **FOR OFFICIAL USE ONLY**

Attachment 5

SAMPLE SEMI-ANNUAL REQUIRED READING/TRAINING LETTER

Figure A5.1. Sample Semi-Annual Required Reading/Training Letter

MEMORANDUM FOR COMSEC ACCOUNT 632312 DATE

FROM: ***Unit and CRO Account Number***

SUBJECT: Semi-Annual Required Reading/Training Letter

1. The following individuals have performed EAP dry-runs and reviewed *Communications Security* (COMSEC) AFI 33-201 vol. 1, *Communications Security User Requirements* AFI 33-201 vol. 2, *Cryptographic Access Program*, AFI 33-201 vol. 4*, Controlled Cryptographic Items*, AFI 33-201, vol. 5, *Management of Manual Cryptosystems* AFI 33-201 vol. 7, *Operational Instructions for Secure Voice Devices* AFI 33-201 vol. 9, AFSSI 4212 *Reporting COMSEC Deviations*, *Operational Instruction for Network Encryption System* AFSSI-3014 (if applicable), AFSSI-3035 *Operational Systems Security Instruction for TACLANE* (if applicable), STE Users Guide and this local element's COMSEC operating instruction.

Print Name	**Signed Name**	**Date**

2. This letter supersedes all previous letters with the same subject. POC is ***Name and Rank of CRO*** at ***Duty Phone***.

CRO Signature Block

Attachment 6

INVENTORY PROCEDURES

A6.1. All Accounting Legend Code (ALC) 1 COMSEC material will be stored in a GSA approved safe (separated by non-COMSEC items by at least a divider), listed on AFCOMSEC Form 16 (inventory form) and inventoried when accessed. ALC 4 should be inventoried by quantity, ALC 6 and 7 material does not have to be inventoried; however, it should be protected commensurate with its classification level. Some non-ALC 1 Controlled Cryptographic Items (CCI) will also be accounted for on inventory. The CCIs required on inventory are all KG-44s, KG-144s, KGR-96s, MYK-7As, OMNI desktop secure phones, and secure cell sleeves. Fill devices such as KYK-15s will also be accounted for on inventory if stored in a keyed condition. ALC 1 COMSEC material will be identified on inventories by short title, edition, quantity and register number. CCI items will be identified on inventories by short title and serial number.

A6.2. When a safe containing COMSEC is opened, it must be inventoried; however, only 1 inventory per shift is required to be documented. In 24/7 duty sections, an inventory will be conducted at every shift change.

A6.3. When performing the inventory, look closely at each item to ensure the short title, edition, and register number match the listing on the inventory. If segments from a key tape are not present and have been destroyed, ensure you can account for these segments via entries on a DRC. Do not mark the inventory until you have properly accounted for all segments of the key tape. Additionally, inspect all protective technology (canisters, pink air-tight seals etc) for defects and/or tampering. Use only blue or black ink for markings and never use correction fluid or tape. If errors are made, explain with a Memorandum for Record (MFR). Failure to follow these set inventory procedures constitutes an improper inventory and increases the possibility for a COMSEC incident.

A6.4. Sealed containers containing COMSEC will be stored in a safe and annotated with an identifying number. This number and a short description of container will be recorded on the inventory. Generate an additional inventory, listing only the container's contents and place it inside the container before sealing. This inventory will be used to account for the container's contents if it is opened. A third inventory must be on the outside of this container, also listing its contents. This inventory will **not** be marked on and serves the purpose of listing the container's contents while it is sealed.

A6.5. Standard Form 702 will be annotated to reflect <u>all</u> opening and closing of safes. The safe will be locked by one individual, and checked by another, whenever possible. After a SF 702 has been completely filled out, it can be shredded and another SF 702 started.

A6.6. A Green pen or marker will be used to identify items added to the inventory, along with a handwritten MFR stating information such as date added, where material was received from (i.e. base COMSEC account, transferred from another local element, transferred from another safe etc) and the initials of the individual adding the material. Preferably, the entire contents of this MFR would be entered within the highlighted area, however, the details of the MFR can be written on the back of the inventory form. When doing this, please remember to number the MFR in the highlighted area and to then utilize the same number on the back of the inventory. <u>Ensure MFR entries are legible</u>.

A6.7. Example of inventory with 2 items added on the 11th of the month and 1 item on the 30th. In this example, XXXX-XXX is entered in the Short Title block for three items – on your inventory, the actual short title would be entered there:

Table A6.1. Example 1

SHORT TITLE	QNTY	SERIAL NUMBER	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
XXXX-XXX DD	01	8972	MFR 1	X	X		X	X	X	X	X			X		X	X	X	X	X		X	X
XXXX-XXX DD	01	8973	MFR 1	X	X		X	X	X	X	X			X		X	X	X	X	X		X	X
AN PYQ-10	01	7721	3F	0R	O	NM	O	VC	O	RM	ES	CE	EC	I	VB	EW	DS					X	X

A6.8. A red pen or marker will be used to identify items that have been permanently removed from the inventory (destroyed material) along with a handwritten MFR stating information such as date removed, and reason for removal (e.g. transferred to another safe, destruction, etc…) and the initials of the individual who removed the material. Preferably, the entire contents of this MFR would be entered within the highlighted area, however, the details of the MFR can be written on the back of the inventory form. The destruction official will be responsible for annotating the AFCOMSEC Form 16, except in cases of TPI where both individuals are required to annotate the form. The MFR will state information such as date destroyed/converted, reason and the initials of the individual(s) destroying/converting the material. Please remember that all items destroyed must also have a SF 153 completed and filed appropriately. Ensure MFR entries are legible.

A6.9. Example of inventory with 1 item destroyed on the 15th, and another converted on the same date. In this example, XXXX-XXX is entered in the Short Title block for three items – on your inventory, the actual short title would be entered there:

Table A6.2. Example 2

SHORT TITLE	QNTY	SERIAL NUMBER	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
XXXX-XXX DD	01	8972	X	X	X	X	1PCR	5EOE	RNC	NTO	ODR	VIAD	RU	DETF	ECHI	STL	TIDE	ROED	ONS	YTB	EOW	DFS	
XXXX-XXX DD	01	8973	X	X	X	X	X		X		X	X		X		X	X	X	X	X		X	X
XXXX-XXX MS	01	5490	X	X	X	X	1IB	5NW	S	NS	OT	VU		CS	ON	N	V3	E2	R9	T5	E3	D	

Attachment 7

DEPLOYED COMSEC PROCEDURES

A7.1. In accordance with reference, the following deployed COMSEC procedures are hereby implemented for units deploying from Kadena Air Base. It should be noted that during deployments of COMSEC, every attempt should be made to utilize US military or US commercial air carriers for transportation. If non-US commercial air carriers are to be utilized, contact the COMSEC Office well in advance of deployment date for coordination and approval through AFNIC.

A7.2. Responsibilities

A7.2.1. Commanders will appoint couriers from within their units to transport COMSEC during deployments. Only individuals with appropriate clearance and training will be appointed as couriers. Appropriately cleared means the individuals hold the proper security clearance and are listed on their unit's COMSEC Access List. Appropriately trained means the individuals have the proper COMSEC training on file (AF Form 4168) within the unit. Appointment will consist of Commanders listing appointed personnel on a completed Authorization to Hand-Carry Classified Sealed Package letter (see **Attachment 8**).

A7.2.2. CROs will ensure appointed couriers are aware of their responsibilities for safeguarding and protecting COMSEC material before they deploy. CROs will ensure only COMSEC material specifically required during the deployment is taken. CROs will provide couriers with a copy of the unit's COMSEC Access List prior to their departure. If non-US commercial carriers are to be utilized for transportation of COMSEC, CROs will contact the COMSEC office well in advance of deployment date for coordination and approval through AFNIC.

A7.2.3. Couriers will be personally responsible for the safeguarding and protection of the COMSEC during transit to and from the deployment location. Couriers will maintain in their possession a copy of the Authorization to Hand-Carry Classified Sealed Package letter at all times during the transit of COMSEC material, and will keep the package which contains the COMSEC material in their personal possession and physical control at all times.

A7.2.4. The Base COMSEC Manager, 18 CS/SCXS, will provide technical advice to CROs whose units are deploying with COMSEC material.

A7.3. Packaging and Marking of Deployed COMSEC Material

A7.3.1. Packaging: Whenever COMSEC is deployed; it will be enclosed in two packages.

A7.3.1.1. Inner Package: The COMSEC material will be enclosed in an inner package. This package will consist of a 100% sealed envelope or wrapper. Before this package is sealed, an inventory (AFCOMSEC Form 16) will be enclosed listing all COMSEC material contained within the package. The wrapper on this package will be clearly stamped with the security classification of the COMSEC material and the identification of the unit deploying the COMSEC.

A7.3.1.1.1. Inventory: An audit trail for deployed COMSEC material is required and an inventory (AFCOMSEC Form 16) for the deployed COMSEC must be maintained. An inventory must be placed within the inner package listing all COMSEC material

enclosed prior to it being sealed. Upon arrival to the deployed location, and opening of the inner package, a complete inventory must be conducted utilizing this form.

A7.3.1.2. Outer Package. The inner package will be enclosed in an outer package. The outer package can be a briefcase, pouch or box and will have affixed a material exempt from examination notice (see **Attachment 9**). Other than the material exempt from examination notice, the outer package should bear no markings or notations which could indicate the classification or type of material enclosed in the inner package. This package will remain in their personal possession and physical control of an appointed courier at all times.

A7.3.1.2.1. Material Exempt from Examination Notice. The outer package will be marked with this notice.

A7.4. Safeguarding and Accounting for COMSEC Material During Deployment

A7.4.1. Storage of COMSEC: Deployed COMSEC material must be maintained in a GSA approved safe or kept under 24 hour guard at the deployed location.

A7.4.2. Access to COMSEC: Individuals not listed on the deployed unit's COMSEC Access List will be denied access to the material during the duration of the deployment. Couriers will be issued a copy of the COMSEC Access List by the unit's CRO prior to departure from home station.

A7.4.3. Inventory of COMSEC: Deployed COMSEC material must be inventoried on an AFCOMSEC Form 16 daily. Deployed inventories will be returned to the unit's CRO upon return from deployment. If any loss of accountability of COMSEC is experienced, the unit's CRO should be contacted immediately.

A7.5. Destruction of COMSEC Material during Deployment

A7.5.1. Destruction of COMSEC: Any COMSEC material that supersedes during the deployment must be appropriately destroyed. All destruction must be annotated on SF 153. When possible, copies of all completed SF 153s will be faxed to the unit's COMSEC Responsible Officer upon completion of destruction. If this is not possible, the SF 153s will be maintained and provided to the unit's CRO upon return from deployment.

Attachment 8

SAMPLE AUTHORIZATION TO HAND CARRY CLASSIFIED SEALED-PACKAGE LETTER

Figure A8.1. Sample Authorization to Hand Carry Classified Sealed-Package Letter

MEMORANDUM FOR WHOM IT MAY CONCERN DATE

FROM: ***Unit and Address***

SUBJECT: Authorization to Hand-Carry Classified Sealed Package

1. ***Name, rank and SSN of individual, Unit and MAJCOM*** is designated an official courier for the United States Government. ***He/She*** will be traveling aboard ***flight identification***, departing ***location and time*** and will arrive ***location and time***. Upon request ***he/she*** will present ***his/her*** official identification card.

2. Name and rank individual is hand carrying a sealed package sized ***provide dimensions***, with an address of ***address listed on outside of inner package***. The package is identified on the outside by the marking "OFFICIAL BUSINESS – MATERIAL EXEMPTED FROM EXAMINATION" bearing the signature of the undersigned.

3. ***Name and rank of individual*** will transit through ***location (if appropriate)*** enroute to ***his/her*** destination.

4. This courier authorization may be confirmed by contacting the undersigned at ***unit and phone number***. This authorization expires ***date.***

Designation Official Signature Block

PRIVACY ACT INFORMATION
This information is subject to the Privacy Act of 1974 and is **FOR OFFICIAL USE ONLY**

Attachment 9

SAMPLE MATERIAL EXEMPTED FROM EXAMINATION NOTICE

Figure A9.1. Material Exempted From Examination Notice

DEPARTMENT OF THE AIR FORCE
UNIT AND OFFICE SYMBOL
UNIT ADDRESS

- OFFICIAL BUSINESS -

"MATERIAL EXEMPTED FROM EXAMINATION"

Designation Official Signature Block

Attachment 10

COMSEC DESTRUCTION NOTES

A10.1. Destruction must be completed within a 12-hour window after COMSEC is superseded and must be documented (to include electronic key) on SF 153. In non 24/7 shops, if supersession occurs on a weekend or holiday, destruction will be performed on the morning of the first duty day that follows.

A10.2. If destruction is performed late, contact the COMSEC Office immediately. This will result in no less than a Practice Dangerous to Security. All late destruction will have a memorandum attached to the Destruction Report detailing the circumstances.

A10.3. Be keenly aware of supersession dates of electronic key. A problem frequently encountered at Kadena is late destruction of electronic key.

A10.4. Ensure the device you use to shred COMSEC documents and keying material is approved by NSA for COMSEC destruction. Contact the Wing COMSEC office with any questions or concerns involving destruction of COMSEC material. If you are not sure if your device is approved for COMSEC destruction, DO NOT USE IT and immediately contact the wing COMSEC office.

Attachment 11

NES/STE/STU DESTRUCTION AND CRYPTO IGNITION KEY LOG CHEAT SHEET

Table A11.1. NES/STE/STI Destruction and Crypto Ignition Key Log Cheat Sheet

	NES Key	**STE Key**	**STU Key (Operational)**	**STU Key (Seed)**
Destruction Report	When key is initialized When key fails initialization and determined to be bad When an initialized key is determined to be bad When non-initialized key has expired	When key is initialized When key fails initialization and determined to be bad When an initialized key is determined to be bad When non-initialized key has expired	When key is initialized When key fails initialization and determined to be bad When an initialized key is determined to be bad When non-initialized key has expired	When key fails initialization and determined to be bad When an initialized key is determined to be bad When non-initialized key has expired
Crypto Ignition Key Log	Complete and keep with key when initialized Turn into COMSEC with key after key goes bad	Complete and turn into COMSEC when initialized	Complete and turn into COMSEC when initialized	Complete and turn into COMSEC when initialized
Note: Please remember to return all bad keys to the COMSEC Office.				

Attachment 12

SAMPLE SECURE VOICE DEVICE KEY REQUIREMENT LETTER

Figure A12.1. Sample Secure Voice Device Key requirement Letter

MEMORANDUM FOR 18 CS/SCXS DATE

FROM: ***Unit, CRO/SVRO Account Number and DAO Code***

SUBJECT: ***IRIDIUM/STE/OMNI/SECTERA*** Key Requirement

1. Request the following ***STE/IRIDIUM/ OMNI/SECTERA*** key requirements.

Quantity	Classification	Display ID	Residence Y/N

2. This letter supersedes all previous letters with the same subject. POC is ***Name and Rank*** at ***Duty Phone***.

CRO/SVRO Signature Block

NOTES

1. Display ID is only required for STE orders.

2. IAW AFI 33-201, vol. 2, attach a copy of the CA/CRL citing the STEs, and/or any other secure voice devices that you're requesting keys for.

3. For STE cards, ensure you attach a copy of the MIPR Acceptance Letter (448-2…Contact Resource Advisor for assistance) proving purchase of the STE cards.

Attachment 13

SAMPLE SECURE VOICE DEVICE ACCESS LIST

Figure A13.1. Sample Secure Voice Device Access List

MEMORANDUM FOR 18 CS/SCXS DATE

FROM: ***Unit and CRO/SVRO Account Number***

SUBJECT: Secure Voice Device Access List

1. The following individuals have been granted access to the identified secure voice device. Their clearances have been verified through the Unit Security Manager and they have a valid need to know. They have been trained in accordance with AFI 33-201, vol. 9 and the appropriate user certification documentation is on file.

Name/Rank	SSN	Clearance	Bldg/Rm	STE, SECTERA, Iridium or OMNI SN

2. This letter supersedes all previous letters with the same subject. POC is ***Name and Rank*** at ***Duty Phone***.

CRO/SVRO Signature Block

1st Ind, (***Squadron/Security Managers Office Symbol***)

MEMORANDUM FOR 18CS/SCXS

I have verified the names, clearances, and U.S. citizenship of all individuals listed above using the unit Clearance and Access Verification System (CAVS).

Security Manager's Signature Block

VERIFY ALL INDIVIDUALS SECURITY CLEARANCES MONTHLY; ANNOTATE VERIFICATION BY INITIALING THE BOTTOM OF THE ACCESS LIST.

PRIVACY ACT INFORMATION
This information is subject to the Privacy Act of 1974 and is **FOR OFFICIAL USE ONLY**

Attachment 14

SAMPLE SECURE VOICE USER CERTICATIONS

A14.1. Secure Voice Responsible Officer (SVRO) Training. The SVRO must be trained on their responsibilities pertaining to secure voice user training, semi-annual KSV-21 inventory, and any other responsibilities prescribed by the COMSEC Manager, if any.

A14.2. User Training. The SVRO must train each user they support. This training must include responsibilities pertaining to secure voice devices, protection of KSV-21 cards, physical security requirements for the equipment and any other responsibilities prescribed by the COMSEC manager.

A14.3. The following is a sample training list and can be tailored to meet local requirements.

A14.3.1. Placing Unsecure Unclassified Calls.

A14.3.1.1. When the STE is in the un-keyed mode, use it only for placing unsecure, unclassified calls. Removing the KSV-21 makes the terminal un-keyed.

A14.3.1.2. The IRIDIUM and FNBDT are keyed and may be used for unsecure unclassified calls if the PIN code has not been entered to activate the key.

A14.3.2. Placing Secure Calls.

A14.3.2.1. When the STE is in the keyed mode (KSV-21 in the STE), afford protection commensurate with the level of the key it contains and ensure use only by authorized personnel (individuals on Secure Voice Device Access List). When unauthorized personnel are in the area, the keyed STE must be under the operational control and within view of at least one appropriately authorized user. Unauthorized personnel will not be allowed access to the STE and no secure calls will be placed by anyone in the area while these individuals are present.

A14.3.2.2. When the IRIDIUM or FNBDT is in the keyed mode (PIN Code entered into the secure voice device), afford protection commensurate with the level of the key it contains and ensure use only by authorized personnel (individuals on Secure Voice Device Access List). When unauthorized personnel are in the area, keep keyed devices under the operational control and within the view of at least one appropriately authorized user. Unauthorized personnel will not be allowed access to the IRIDIUM or FNBDT and no secure calls will be placed by anyone in the area while these individuals are present.

A14.3.2.3. Pay strict attention to the authentication display to ensure the classification level of the conversation does not exceed the highest clearance classification displayed.

A14.3.2.4. Before discussing classified information, the person making/receiving the classified call must make sure all personnel in the area are cleared and have a need to know.

A14.3.2.5. Each STE user must call the Electronic Key Management System Central Facility (EKMS CF – by dialing 118) twice each year to update the STE. Recommend you call at least once a quarter to receive an updated compromise information message and update the key.

A14.3.2.6. Each SECTERA or OMNI user must call the Electronic Key Management System Central Facility (EKMS CF – by dialing 312-238-4470) twice each year to update the COMSEC key. Recommend you call at least once a quarter to receive an updated compromise information message and update the key.

A14.3.3. A STE not operational 24 hours a day will have the KSV-21 removed at the close of business. Annotate that this has been accomplished on the SF 701, *Activity Security Checklist***.** Store the KSV-21 in a GSA-approved security container, if kept in the same room as the STE. If the room in which the STE is used is authorized for open storage, the KSV-21 may remain in the phone. Only individuals on the Secure Voice Device Access List will have access to the container. If you store the KSV-21 in another room, keep it in a GSA-approved security container. If a security container is not available, store the KSV-21 in a locked cabinet, desk, etc. You may place the KSV-21 on your person. The adequacy of storage alternatives for the CIK is determined on a case-by-case basis by the unit security manager within each using organization.

A14.3.4. For IRIDIUM and FNBDT devices, keep the PIN Code separate from the associated devices. Do not write the PIN on the device or anywhere else accessible by an unauthorized person. The PIN will not be written or otherwise affixed to the device.

A14.3.5. If you lose your KSV-21, notify your SVRO immediately.

A14.3.6. The following are reportable COMSEC incidents that you must report to your CRO/SVRO:

A14.3.7. KSV-21 cards left in STE overnight (except 24-hour work center or area approved for open storage of classification of STE).

A14.4. Lost secure voice device.

A14.4.1. Loss of KSV-21 fill cards.

A14.4.2. Unauthorized personnel making a secure call on a secure voice device. An unauthorized individual is anyone not listed on the Secure Voice Device Access List.

A14.4.3. Secure call completed using expired key.

A14.4.4. Any instance where the authentication information displayed during a secure call is does not represent the distant terminal

A14.4.5. Failure to adequately protect or to erase a KSV-21 associated with a lost terminal.

A14.4.6. Any instance where the display indicates the distant terminal contains compromised key.

A14.4.7. STEs (KSV-21 inserted) left unattended (i.e., no authorized user present for more than five minutes). Exceptions to this are rooms with open storage authorization.

A14.4.8. Any instance where the display is inoperative and a secure call is completed.

A14.5. Emergency Procedures. In the event of fire, natural disaster, or covert threat, remove the KSV-21 from the STE and secure it or keep it in the personal possession of an authorized individual. Disable PINs in all FNBDT devices and secure or take all secure cellular phone devices. These procedures are listed in your unit's Emergency Action Plans (EAPs). See your CRO/SVRO for details. Example illustration provided below.

Figure A14.1. Example 3

Printed Name	Signature	Date

Attachment 15

KSV-21 CARD HANDLING AND ORDERING PROCEDURES

A15.1. The following COMSEC procedures are implemented for the handling and ordering of KSV-21s for STE phones at Kadena Air Base.

A15.2. Ordering KSV-21s.

A15.2.1. SVRO identifies requirement for STE card (KSV-21).

A15.2.2. SVRO's unit Resource Advisor (RA) purchases the KSV-21 on a MIPR.

A15.2.3. SVRO receives the 448-2 MIPR Acceptance Letter from their RA.

A15.2.4. SVRO fills out the STE Key Requirement Letter.

A15.2.5. SVRO turns in the 448-2, STE Key Requirement letter and Standard Base Supply System (SBSS) printout to COMSEC Office.

A15.2.6. COMSEC office drafts an order for the KSV-21 and faxes it to EKMS/Central Facility (CF).

A15.2.7. EKMS/CF ships the KSV-21 to COMSEC account.

A15.3. Handling/Accountability.

A15.3.1. COMSEC office receives the KSV-21 and accounts for them as ALC-1 COMSEC.

A15.3.2. COMSEC office issues the KSV-21 to the SVRO on a SF-153 as Hand Receipt.

A15.3.3. SVRO adds the KSV-21 to their AFCOMSEC Form 16 inventory and accounts for it as ALC-1 COMSEC.

A15.3.4. SVRO associates the KSV-21 to a STE.

A15.3.5. SVRO removes the KSV-21 from AFCOMSEC Form 16, and makes annotation on the inventory that it is associated to a STE.

A15.3.6. SVRO annotates on the SF-153 for Hand Receipt that the KSV-21 is associated.

A15.3.7. SVRO adds the KSV-21 and its associated STE to their SEMIANNUAL CIK/KSV-21 inventory.

A15.3.8. SVRO completes a new SF 153, checking the OTHER block, and annotates "LOADED, ZEROIZED or FAILED LOAD" in the REMARKS column, depending on what transaction they're completing.

A15.3.9. SVRO fills out the yellow card and attach it to the SF 153.

A15.3.10. SVRO turns yellow card and SF 153 in to the COMSEC Office.

A15.4. Returning KSV-21s for reprogramming.

A15.4.1. SVRO turns in to COMSEC office bad/expired KSV-21 for reprogramming, along with a STE Key Requirement letter detailing how they would like the KSV-21 programmed.

A15.4.2. SVRO removes the KSV-21 from their AFCOMSEC Form 16 and Semi-annual CIK/KSV-21 inventory.

A15.4.3. SVRO clears SF 153 for Hand Receipt that the KSV-21 was issued to them on.

A15.4.4. COMSEC Office creates a KSV-21 order per the SVRO's STE Key Requirement request.

A15.4.5. COMSEC Office ships bad/expired KSV-21 back to EKMS/CF.

Attachment 16

KSV-21 CARD RE-KEYING PROCEDURES

Figure A16.1. Setting Up a New KSV-21

1. Zeroizing STE

Press "Menu"
STE Displays “TERMINAL MANAGEMENT”
Press "Scroll" twice
STE Displays “ZEROIZE TERMINAL”
Press "Select"
Press "Confirm"

2. Establish TPA (Administrative Card Function)

Insert new KSV-21 Card into STE to become the TPA

3. Create a User Card (Enables Secure Communications)

Insert TPA Card
Press “Menu”
STE Displays “TERMINAL MANAGEMENT
Press “Select”
STE Displays “NETWORK SETTING”
Press “Scroll”
STE Displays “TERMINAL PRIVILEGE”
Press “Modify”
STE Displays “TERMINAL CONFIGURATION CONTROL”
Press “Scroll” 3X
STE Displays “CREATE A NEW ASSOCIATION”
Press “Create”
Press “FULL CIK”

4. Miscellaneous Setting A

Press “Menu”
STE Displays “TERMINAL MANAGEMENT”
Press “Select”
STE Displays “NETWORK SETTING”
Press “Select”
STE Displays “ACTIVE NETWORK PORT”
Depend on the setting of the STE (PSTN/ISDN)
Press “Change” to reflect on the correct output
*Please note: If your STE is using ISDN you’ll need to contact Telephone @ 634-2336
Option: 2, 2 to get the SPID #

5. Miscellaneous Setting B

Press “Menu”
STE Displays “TERMINAL MANAGEMENT”
Press “Select”
STE l Displays “NETWORK SETTING”
Press “Scroll”
STE Displays “TERMINAL PRIVILEGE”
Press “Modify”
STE Displays “TERMINAL CONFIGURATION CONTROL”
Press “Select”
STE Displays “INITIAL SECURE MODE”
Press “Change” until it show “TRADITIONAL”

6. Setting up Rekey Phone Number (needed in order to re-key your card)
Press “Menu”
STE Displays “TERMINAL MANAGEMENT”
Press "Scroll"
STE Displays “CRYPTO CARD MANAGEMENT”
` Press “Select”
STE Displays “CARD MANAGEMENT PRIVILEGES”
Press “User”
STE Displays “REKEY FUNCTIONS”
Press “Select”
STE Displays “UPDATE REKEY PHONE NUMBER”
Press “Update”
STE Displays “UPDATE STORED PHONE NUMBER”
Press “SDNS”
STE Displays “SDNS REKEY PHONE NUMBER”
Press “SCIP”
Enter “94-312-238-4470”
Press “Store”

7. Re-keying KSV-21 Card

Press “Menu”
STE Displays “TERMINAL MANAGEMENT”
Press "Scroll"
STE Displays “CRYPTO CARD MANAGEMENT”
` Press “Select”
STE Displays “CARD MANAGEMENT PRIVILEGES”
Press “User”
STE Displays “REKEY FUNCTIONS”
Press “Select”
STE Displays “UPDATE REKEY PHONE NUMBER”

Press “Rekey”
STE Displays “PERFORM REKEY”
Press “SDNS”
STE Displays “SDNS REKEY MODE”
Press “SCIP”
STE Displays “SDNS REKEY MODE”
Press “Go”

NOTE: If there is no rekey number listed please follow step 6 and manually enter the rekey dial in number to the phone.

Attachment 17

SECTERA AND OMNI PROCEDURES

A17.1. The following COMSEC procedures are implemented for the SECTERA and OMNI devices.

A17.2. Handling and accountability of SECTERA Wire line Terminals and PIN:

A17.2.1. Terminal:

A17.2.1.1. Storage and Handling: SECTERA terminals must be located in areas where access to the device can be controlled, users can maintain continuous physical control of the terminal and the possibility of loss, theft, unauthorized use, or tampering is minimized. Any loss, theft, unauthorized use or tampering must be reported immediately to the COMSEC office. The selected location must also adhere to a common-sense approach in regards to acoustic security concerns. When the secure capability of the terminal has been activated by entering the User PIN code, the terminal must be protected to the classification level of the key it contains. All personnel assigned to the area where the SECTERA is located should have a security clearance at least equivalent to the key contained within the SECTERA. **When the terminal is not being used, the PIN code must be disabled.**

A17.2.1.2. Accountability: Each SECTERA will be accounted for daily on a SF-701, Activity Security Checklist. Each terminal will be listed individually on the SF-701 by its serial number. Entries on the SF-701 will also include reminders to ensure SECTERA PIN codes have been disabled. Semi-annually, the COMSEC Manager will inventory all terminals at each local element and ensure daily accountability via SF701 has been conducted.

A17.2.2. PIN:

A17.2.2.1. Storage and Handling: Each terminal's T1DSW PIN and all User PINs will be stored in a GSA approved safe when not being utilized. User PINs are generated by the SECTERA itself. Once a User PIN is generated, it may be recorded on a SF-700. T1DSW PINs will never be written down and User PINs will only be recorded on a SF-700.

A17.2.2.2. Accountability: CROs/SVROs must devise a method to account for T1DWS and User PINs. The method used is left up to these individuals (AFCOMSEC Form 16 listing COMSEC material, separate AFCOMSEC Form 16). Whichever method is used, each PIN will be listed by the serial number of the phone to which it is assigned.

A17.3. Handling and accountability of OMNI Terminals and PIN:

A17.3.1. Terminal:

A17.3.1.1. Storage and Handling: OMNI terminals must be located in areas where access to the device can be controlled, users can maintain continuous physical control of the terminal and the possibility of loss, theft, unauthorized use, or tampering is minimized. Any loss, theft, unauthorized use or tampering must be reported immediately to the COMSEC office. The selected location must also adhere to a common-sense approach in regards to acoustic

security concerns. When the secure capability of the terminal has been activated by entering the User PIN code, the terminal must be protected to the classification level of the key it contains. All personnel assigned to the area where the OMNI is located should have a security clearance at least equivalent to the key contained within the OMNI. **When the terminal is not being used, the PIN code must be disabled.**

A17.3.1.2. Accountability: Each OMI will be accounted for daily on a SF-701, Activity Security Checklist. Each terminal will be listed individually on the SF-701 by its serial number. Entries on the SF-701 will also include reminders to ensure OMNI PIN codes have been disabled. Semi-annually, the COMSEC Manager will inventory all terminals at each local element and ensure daily accountability via SF701 has been conducted.

A17.3.2. PIN:

A17.3.2.1. Storage and Handling: Each terminal's TA PIN and all User PINs will be stored in a GSA approved safe when not being utilized. The TA and User PINs are generated by the OMNI itself. Once these PINs are generated, they may be recorded on a SF-700. The only place TA and User PINs may be recorded is on a SF-700.

A17.3.2.2. Accountability: CROs/SVROs must devise a method to account for TA and User PINs. The method used is left up to these individuals (AFCOMSEC Form 16 listing COMSEC material, separate AFCOMSEC Form 16). Whichever method is used, each PIN will be listed by the serial number of the phone to which it is assigned.

Attachment 18

SAMPLE STE PRIVATE RESIDENCE LETTER

Figure A18.1. Sample STE Private Residence Letter

MEMORANDUM FOR 18 CS/SCXS DATE

FROM: ***Unit and CRO/SVRO Account Number***

SUBJECT: Authorization Allowing Secure Telephone in Living Quarters

1. The individuals listed below are authorized to use a Secure Telephone in their residence. They have been briefed on all physical security protection requirements designated in AFI 33-201, vol. 9.

Name/Rank	Address	STE Phone Number	STE SN

2. This letter supersedes all previous letters with the same subject. POC is ***Name and Rank*** at ***Duty Phone***.

Signature of Commander

Attachment 19

SAMPLE SEMI-ANNUAL KSV-21 INVENTORY LETTER

Figure A19.1. Sample Semi-Annual KSV-21 Inventory Letter

MEMORANDUM FOR 18 CS/SCXS DATE

FROM: ***Unit and CRO/SVRO Account Number***

SUBJECT: Annual KSV-21 Inventory

1. In accordance with AFI 33-201, vol. 9, the following KSV-21 inventory is submitted. In preparing this inventory, ***CRO/SVRO name*** ensured that all physical security protection requirements designated in AFI 33-201, vol. 9 are in place for these devices and their associated KSV-21 Cards.

STE S/N	REGISTER NUMBER	KSV-21 S/N	Bldg/Rm	Phone Number

2. Semi-annual rekeys have been performed on all listed STE KSV-21s.

3. This letter supersedes all previous letters with the same subject. POC is ***Name and Rank*** at ***Duty Phone***.

CRO/SVRO Signature Block

Attachment 20

UPLOADING AUDIT TRAILS FROM SKL TO DMD

A20.1. Preparing the DMD for audit trail transfer.

A20.1.1. Log into the DMD and open DMD Power Station.

A20.1.2. Click “Xmit/Recv” on the top menu bar.

A20.1.3. Select “Receive CoreLib Audit”

A20.1.4. Connect the SKL to the DMD laptop with a link cable.

A20.2. Uploading the audit trail from the SKL.

A20.2.1. Verify link cable is connected to both the SKL and the DMD.

A20.2.2. Log onto the SKL as “SSO”

A20.2.3. Switch to the “CoreLib” desktop

A20.2.4. Click “Tools” from the top menu and select SSO > Audit Functions > Upload Audit DMD.

A20.3. Receiving the audit trail on the DMD laptop.

A20.3.1. Click “receive” in the CoreLib window that was opened in A20.1.3.

A20.3.2. The SKL should now upload its audit trail data to DMD Power Station. Once the audit data is displayed, click “Export Archive”

A20.3.3. Select a location to save your archived audit trail data. NOTE: Name the archived file with the current date.

A20.3.4. Click “Save”

A20.3.5. Verify that the file saved correctly by navigating to the saved location and confirming the file exists. In the DMD Power Station click “Clear”.