BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-212

15 DECEMBER 2000

Communications and Information

REPORTING COMSEC DEVIATIONS

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil.

OPR: HQ AFCA/GCI (SMSgt Harwell) Certified by: HQ USAF/SCXX (Lt Col L. Wilson)
Supersedes AFI 33-212, 26 July 1999. Pages: 53
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and applicable parts of National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4003, *Reporting and Evaluating COMSEC Incidents*. It sets up procedures for reporting incidents affecting the security of communications security (COMSEC) material to the Director, National Security Agency (DIRNSA), the Air Force Communications Agency (AFCA), appointed controlling authorities, and other cognizant authorities in established chains of command. It applies to all Air Force military and civilian personnel and Air Force contractors who get COMSEC support from the Air Force. This publication pertains to all COMSEC material, including controlled cryptographic items (CCI), electronic key, keyed common-fill devices, cryptographic equipment, and electronically generated keys (generated by field and electronic key management systems [EKMS]). The term major command (MAJCOM), when used in this publication, includes field operating agencies and direct reporting units. Send recommended changes or comments to Headquarters AFCA (HQ AFCA/ITPP), 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, using Air Force Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCI, 203 West Losey Street, Room 2040, Scott AFB IL 62225-5222. Send messages to: HQ AFCA SCOTT AFB IL//GCI//. Refer to Attachment 1 for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This change updates IC 99-1 (**attachment 14**). It corrects required reporting procedures for lost STU-III Seed Keys according to NSTISSI 4003. It deletes reference to STU-III Seed Key in **table 2.**, and deletes reference to STU-III Seed Key in **table 3.**, Rule 2B. See the last attachment of this publication, IC 2000-1, for the complete IC. A bar (|) indicates revision from the previous edition.

1. Introduction .

1.1. Scope. COMSEC deviations are reported so appropriate officials can determine if deviations have seriously affected the security of the cryptosystems involved or have the potential to do any harm to the security of the United States. Reporting COMSEC deviations also provides the basis for identifying trends in incident occurrences and for developing policies and procedures to prevent recurrence of similar incidents. ***NOTE***: Terms and acronyms in Air Force Directory (AFDIR) 33-303, *Compendium of C4 Terminology*, apply to this publication. Key terms are listed below:

1.1.1. COMSEC Deviation. An occurrence involving failure to follow established COMSEC instructions, procedures, or standards.

1.1.2. COMSEC Material Receipt Discrepancy. An occurrence where the contents of the COMSEC package do not agree with the shipping documents and no tampering of the package is evident.

1.1.3. Production Error/Defective Key. An occurrence where a reported discrepancy appears to be the result of a production error or a defect with the keying material. DIRNSA/Y265 is responsible for evaluating the material in question.

1.1.4. Codebook Incident. Occurrence involving material governed by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3260.01, (S) *Joint Policy Governing Positive Control Material and Devices (U)*. Incident reports are processed and filed in accordance with CJCS policy. HQ AFCA/GCIS is an information addressee on all codebook incident correspondence.

1.1.5. PDS. A procedure that has the potential to jeopardize the security of COMSEC material if allowed to continue. (**NOTE**: A PDS is not a COMSEC incident and does not have an Air Force COMSEC case number assigned.)

1.1.6. COMSEC Incident. Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information.

1.1.7. COMSEC Insecurity. COMSEC incident that was investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information. Incident was evaluated as "COMPROMISE."

1.2. Records Disposition. Records created as a result of processes prescribed in this instruction must be maintained and disposed of in accordance with AFMAN 37-139, *Records Disposition Schedule* (to become AFMAN 33-322V4).

2. Roles and Responsibilities .

2.1. National Security Agency (NSA) COMSEC Incident Evaluation Branch (DIRNSA/I413):

2.1.1. Evaluates all cryptographic, personnel, aircraft, and disaster COMSEC incidents, and incidents involving COMSEC equipment.

2.1.2. Evaluates all physical COMSEC incident reports involving keying material in transit or when the controlling authority cannot be identified.

2.1.3. Evaluates all physical COMSEC incidents involving multiple controlling authorities for more than one department or agency.

2.1.4. Evaluates all reported COMSEC incidents concerning tampering, sabotage, evidence of covert penetration of packages, evidence of unauthorized or unexplained modification of COMSEC equipment, security containers or vaults where COMSEC material is stored, and COMSEC material other than keying material (e.g., documents, algorithms, logic, etc.).

2.1.5. Evaluates, or coordinates evaluation of, COMSEC incidents having significant cryptologistic impact, and directs supersession of compromised future keying material that has not reached the COMSEC account.

2.1.6. Initiates or recommends appropriate action when COMSEC material is subjected to compromise, and notifies appropriate authorities of actions taken.

2.2. HQ AFCA/GCIS:

2.2.1. Manages the Air Force COMSEC Incident Program and serves as the Air Force COMSEC incident managing activity.

2.2.2. Assigns Air Force COMSEC incident case numbers.

2.2.3. Evaluates physical COMSEC incidents involving multiple Air Force controlling authorities.

2.2.4. Evaluates COMSEC incidents involving a single Air Force controlling authority when the Air Force controlling authority causes the incident.

2.2.5. Exercises adjudication authority on whether a reported COMSEC incident has resulted in a COMSEC insecurity. Closes incident reports and upgrades incidents to insecurities, if appropriate.

2.2.6. Provides case status information to all appropriate addressees.

2.2.7. Maintains Air Force database files to support the COMSEC incident trend analysis (CITA) database in collaboration with DIRNSA.

2.2.8. Furnishes NSA information about the CITA database for trends analysis and damage assessment associated with COMSEC incidents.

2.3. MAJCOMs:

2.3.1. Ensure all required reports are submitted according to the provisions of this instruction, and the controlling authority evaluation is completed before recommending case closure involving subordinate units. (***NOTE***: In Air National Guard [ANG] cases, the gaining MAJCOM is responsible for providing the recommendation for case closure.)

2.3.2. Provide comments on and assess the suitability and effectiveness of actions planned or implemented to prevent COMSEC incidents from recurring.

2.3.3. Make sure COMSEC incident report (amplifying and final) suspense dates are met.

2.3.4. Use trend analysis as a management tool, showing the possible need for additional training or adjustment of personnel duty assignments.

2.4. Controlling Authorities:

2.4.1. Evaluate the security impact involving material they control when physical incidents affect superseded, current, and future cryptonet keying material held by the COMSEC account and users (except as stated in paragraph **2.1.** and paragraph **2.2.**). See guidelines in **attachment 13**.

2.4.2. Inform all required COMSEC addressees of evaluation results, and when necessary, recommend upgrading the incident to an insecurity. See guidelines in **attachment 13**.

2.4.3. Direct emergency supersession of keying material held by the cryptonet members and immediately notify the appropriate agencies according to AFI 33-215, *Controlling Authorities for COMSEC Keying Material (KEYMAT)*. Each agency notified is responsible for notifying individual holders to whom distribution was made. This includes those in other departments, agencies, services, commands, or nations. When a system is declared compromised, do not use for further encryption unless it is operationally essential to send encrypted messages before the supersession date, and another suitable cryptosystem is not available.

2.4.4. Direct emergency extensions of keying material cryptoperiods when necessary according to AFI 33-215. (***NOTE***: For electronic key, the organization that directed its generation performs the controlling authority functions unless those functions are delegated to another organization.)

2.5. COMSEC Manager:

2.5.1. Reviews all known circumstances of the deviation and determines what type of violation has occurred and what reporting actions to take.

2.5.2. Prepares, in conjunction with the reporting CRO, any required initial report (COMSEC Incident, PDS, etc.) and transmits the report to the appropriate agencies.

2.5.3. Briefs the commander of the violating unit on options available regarding inquiry and/or investigation.

2.5.4. Provides assistance to the inquiry or investigating official.

2.5.5. Reviews final report and provides additional comments, including concurrence or nonconcurrence.

2.5.6. Prepares required reports/messages and forwards according to this AFI after receiving the information from the inquiry/investigating official or violating unit. (***NOTE***: Ensure reports are addressed correctly and include ALL case numbers assigned [beginning with the Air Force-assigned case number].)

2.6. Violating Unit's Commander:

2.6.1. When notified by the CRO that a deviation has occurred, provides the required information needed for the COMSEC manager to determine the deviation type.

2.6.2. When notified that a reported deviation is a COMSEC incident, provides any additional information required for the initial COMSEC incident report to the supporting COMSEC manager.

2.6.3. When notified that an incident has occurred, appoints, within 72 hours, an appropriately cleared and disinterested civilian (General Schedule-9 or above), senior noncommissioned officer, or commissioned officer to conduct the inquiry (see **attachment 11**).

2.6.4. If the seriousness of the incident warrants (e.g., suspected illegal activity, espionage, etc.), contacts the local Air Force Office of Special Investigations (AFOSI) and upgrades the inquiry to an investigation. Notifies the COMSEC manager of the status change and provides information for the amplifying report.

2.6.5. Provides the status of the inquiry or investigation, at least every 25 days, to the supporting COMSEC manager until the inquiry or investigation is complete.

2.6.6. Reviews, endorses, and forwards the inquiry/investigating officialÕs report (and the conclusions of the AFOSI investigation, if applicable) to the COMSEC manager. Endorsement must include comments, and concurrence or nonconcurrence in final reports.

2.6.7. Corrects unit deficiencies that contribute to COMSEC incidents and insecurities.

2.7. Inquiry or Investigating Official:

2.7.1. Conducts an inquiry or investigation using the guidance contained in this AFI. This AFI is used as the authority to conduct the inquiry or investigation.

2.7.2. Completes the inquiry or investigation without interruptions for temporary duty, leave, or other duties.

2.7.3. If unable to complete the inquiry or investigation within the time limit set forth in the appointment letter, advises the violating unit's commander of the status of the inquiry or investigation.

2.7.4. Provides the information for amplifying reports according to paragraph **10.1.2.**

2.7.5. Determines the organization and one or more individuals accountable for the incident and reports on the circumstances surrounding the incident.

2.7.6. Documents the results of the inquiry or investigation. The format for the inquiry or investigation report is shown in **attachment 12**.

2.7.7. Makes an evaluation recommendation based on the facts and information gathered from the inquiry or investigation. The official may recommend a finding of "compromise," "compromise cannot be ruled out," or "no compromise." Review **attachment 13** for guidelines on this recommendation.

2.7.8. Makes suitable recommendations to prevent recurrence and forwards the inquiry or investigation report to the violating unit's commander.

2.8. COMSEC Responsible Officers (CRO):

2.8.1. Know the types of deviations that could result from improper handling, control, and destruction of COMSEC material.

2.8.2. Know the types of reportable equipment malfunctions or operator errors for equipment held.

2.8.3. Report any known or suspected deviations to the COMSEC manager and violating unit's commander immediately.

2.8.4. Prepare, in conjunction with the COMSEC manager, any required initial reports (COMSEC Incident, PDS, etc.).

2.9. COMSEC Users:

2.9.1. Know the types of deviations that could result from improper handling, control, and destruction of COMSEC material.

2.9.2. Know the types of reportable equipment malfunctions or operator errors for equipment held.

2.9.3. Report any known or suspected deviations to the CRO, COMSEC manager, or violating unit's commander immediately.

3. Communications Security Material Receipt Discrepancy . A material receipt discrepancy report is processed by the account when a COMSEC package is received wherein the contents of the package do not agree with the shipping documents and the package shows no evidence of tampering. (***NOTE***: If the package shows evidence of tampering, report the occurrence as a physical COMSEC incident.)

3.1. Report material receipt discrepancies by message (see **attachment 2**). The package shipper is the action addressee. (See **table 1.** for action/info addressees.)

3.2. Upon receipt of the discrepancy report, HQ AFCA/GCIS will assign a tracking number. Tracking numbers are comprised of the package shipper (USNDA - NSA, TOBYHANNA - TOBY, HQ CPSG/ZJY or CA616600 - CPSG), followed by an "S" (for shipping), followed by the next unused tracking number for that shipper, and the calendar year the discrepancy took place (e.g., NSA-S-001-98).

3.3. AFKAG-2, *Air Force COMSEC Accounting Manual*, identifies further reporting and follow-on actions the COMSEC account must complete for this discrepancy. Further tracking of the discrepancy is the responsibility of HQ AFCA/GCIS.

Table 1. Addressing COMSEC Material Receipt Discrepancy Reports.

If the Package Shipper is:	Send Action Message to:	Send Information Copy to:
USNDA	DIRNSA FT GEO G MEADE MD// Y13//	HQ AFCA SCOTT AFB IL//GCIS// DIRNSA FT GEO G MEADE MD// I413// HQ CPSG SAN ANTONIO TX// ZSKM// CONTROLLING AUTHORITY(IES) MAJCOM IA OFFICE
TOBYHANNA	CDR TYAD TOBYHANNA PA// CA5B1099//	SAME AS USNDA
HQ CPSG/ CA616600	HQ CPSG SAN ANTONIO TX// CA616600//	SAME AS USNDA
HQ CPSG/ZJY	HQ CPSG SAN ANTONIO TX//ZJY//	SAME AS USNDA

4. Production Errors, Defective Keying Material, and Damaged Protective Technology. The COMSEC manager inspects all incoming material for possible production errors, defective-keying material, or damaged protective technology. If an error or anomaly is detected by the CRO (after the material was issued by the COMSEC account), the CRO should notify the unit commander and immediately return COMSEC material that is unusable and is suspected to stem from a production problem to the COMSEC account. The COMSEC account sends a message (see **attachment 3**) to DIRNSA/Y265, info HQ AFCA/GCIS, DIRNSA/I413, HQ CPSG/ZSKM, Controlling Authority, and MAJCOM Information Assurance (IA) Office, explaining the circumstances of the defective material and requesting disposition instructions.

4.1. DIRNSA/Y265 is responsible for determining if the error or anomaly was the result of production or tampering.

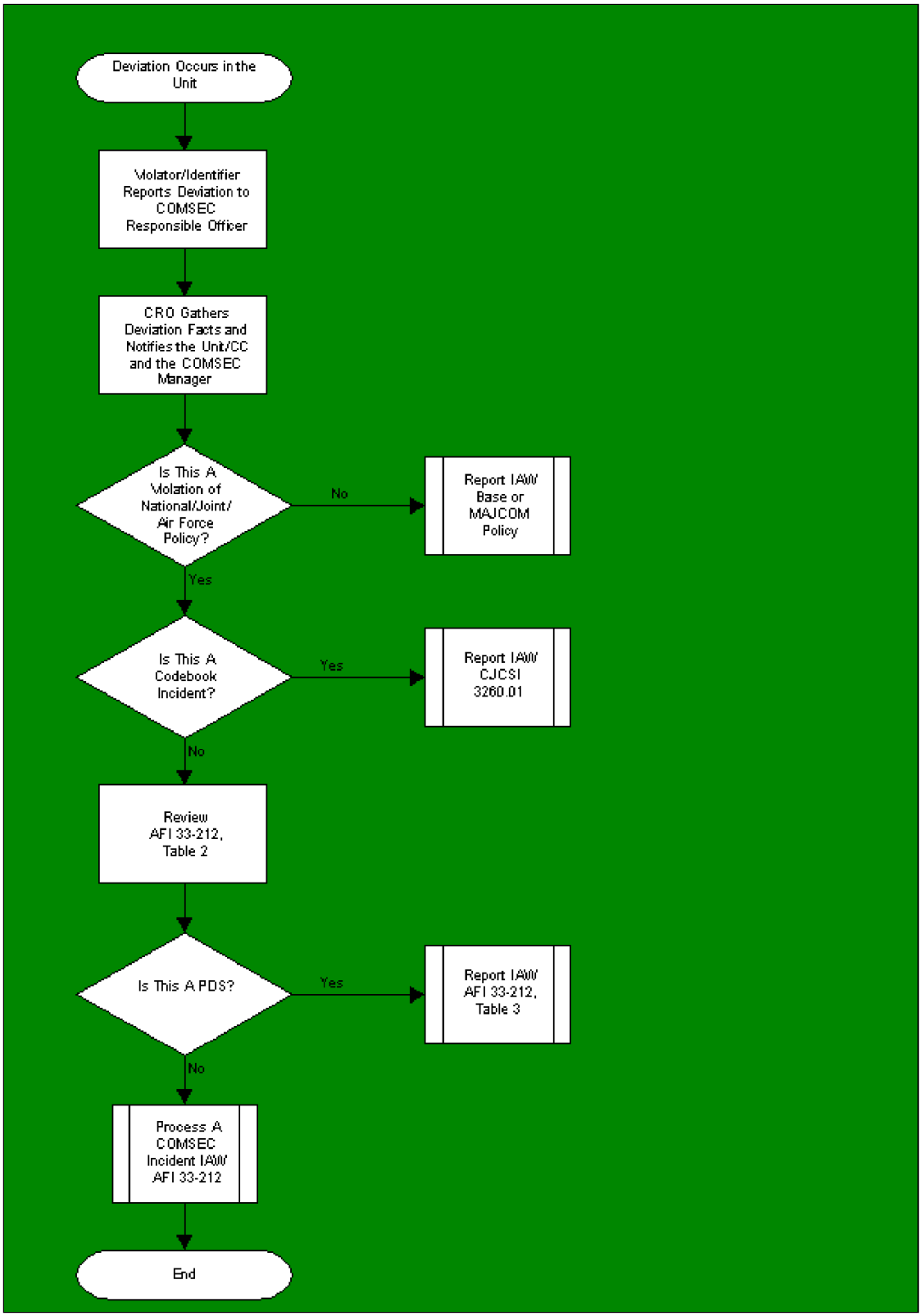
4.1.1. If tampering is determined, open a physical incident against the violating unit. The COMSEC account is responsible for processing the incident upon notification from DIRNSA/Y265.

4.2. Upon receipt of the production error message, HQ AFCA/GCIS will assign a tracking number comprised of NSA, followed by “E” (for production error), followed by the next unused tracking number, and the calendar year the error or anomaly was reported (e.g., NSA-E-01-98).

4.3. Further tracking of the discrepancy is the responsibility of HQ AFCA/GCIS.

5. Communications Security Deviation Identification and Reporting Process . See **figure 1.**

Figure 1. COMSEC Deviation Identification and Reporting Process.



5.1. When a user suspects a COMSEC deviation has occurred, report the deviation to the CRO immediately if the CRO is not already involved. If the COMSEC material involved is not secured, the violator/identifier must secure the material prior to reporting the deviation.

5.2. The CRO gathers all pertinent facts surrounding the deviation and notifies the violating unit's commander and the COMSEC manager. Do not delay reporting simply to gather more information. Limit fact finding to readily available information.

5.3. The COMSEC manager reviews all circumstances of the deviation to determine if a violation of base or MAJCOM policy, codebook incident, PDS, or COMSEC incident (see **table 2.** and **table 3.**) has occurred. After the deviation decision is made, the violating unit's commander, the CRO, and COMSEC manager complete the required actions for that decision.

Table 2. Incident or PDS (Quick Look).

Material Involved Is:	Accounting Legend Code (ALC) Is:	Report Under:
Classified	1 or 6	COMSEC or Codebook Incident
Classified Operational STU-III Key	1	COMSEC Incident
STU-III Terminal Only-Unkeyed (1)	CCI	COMSEC Incident
STU-III with CIK/Key Inserted (2)	1	COMSEC Incident
Classified	4 or 7	PDS
Unclassified	1 or 6	PDS
Unclassified	4 or 7	PDS (Local Report Only)
STU-III User CIK or Master CIK		PDS (Local Report Only)

NOTES:

(1) Generally involves the suspected loss, theft, or tampering of a STU-III terminal.

(2) Generally involves a Secure Telephone Unit (STU)-III left unattended with the key/crypto-ignition key (CIK) inserted.

6. Codebook Incident . CJCSI 3260.01 defines various conditions that may result in a compromise of positive control material (PCM) and describes the procedures for reporting and evaluating possible compromises. When one or more of these conditions exist, the CRO notifies the unit commander and the COMSEC manager. The CRO and COMSEC manager submit a report of possible compromise in accordance with CJCSI 3260.01 and info HQ AFCA/GCIS. If the material involved includes PCM as well as other COMSEC material, report the incident through Air Force and Joint Chiefs of Staff (JCS) channels concurrently. Report all personnel incidents through both channels (see paragraph **8.2.** for personnel incident procedures). HQ AFCA/GCIS will not assign an Air Force case number if only PCM material is involved in the incident.

7. Practice Dangerous to Security . A PDS is a COMSEC deviation that has the potential to jeopardize the security of COMSEC material if allowed to continue. See **table 3.** and **attachment 8** for reporting a PDS. (***NOTE***: If the deviation you are reporting does not appear in **table 3.** proceed to paragraph **8.**). PCM governed under CJCSI 3260.01 is still reported through JCS channels although it may be categorized as an Air Force PDS. The violating unit, through their COMSEC account, is required to respond to any and all questions put forth by the controlling authority or MAJCOM. An inquiry is not required for a PDS unless requested by the controlling authority, MAJCOM, violating unit's commander, or COMSEC

manager. A controlling authority may render an evaluation on a PDS. (***NOTE***: HQ AFCA/GCIS is not addressed on PDS traffic unless they are a controlling authority for material involved.)

8. Types of Communications Security Incidents . Cryptographic, personnel, physical, and aircraft accidents or disaster COMSEC incidents are identified below. Aircraft accidents or disasters where cryptographic equipment or material is lost or damaged beyond repair technically fall into the physical category; however, for the purpose of this AFI, treat aircraft accidents or disasters as their own type of COMSEC incident. Additional reportable incidents unique to a particular cryptosystem, or to an application of a cryptosystem, are normally listed in the AFI 33-2XX series, Air Force systems security instructions (AFSSI), operating instructions, and maintenance manuals for that specific cryptosystem. (NOTE: The reporting requirements in this section are exempt from licensing in accordance with AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* [will convert to AFI 33-324].)

8.1. Cryptographic Incidents. Cryptographic incidents include equipment malfunction or operator error that adversely affects the cryptosecurity of a machine, auto-manual or manual cryptosystem. Report cryptographic incidents by message (see **attachment 4** and **attachment 6**). Examples are:

8.1.1. Using a COMSEC key that is compromised, superseded, defective, previously used (and not authorized for reuse), or incorrect application of keying material. Examples are:

8.1.1.1. Using keying material produced without the authorization of NSA (e.g., unauthorized maintenance or data encryption standard key or locally contrived codes).

8.1.1.2. Using any keying material for other than its intended purpose without the authorization of NSA (e.g., use of test key for operational purposes or use of a key on more than one type of equipment).

8.1.1.3. Unauthorized extension of a cryptoperiod (e.g., using a superseded key on an active circuit where both ends of the circuit are synchronized and information is transmitted).

8.1.2. Using COMSEC equipment with defective cryptographic logic circuitry, or using unapproved operating procedures. Examples include:

8.1.2.1. Plain-text transmission resulting from COMSEC equipment failure or malfunction.

8.1.2.2. Any transmission, during or after an uncorrected failure, that may cause improper operation of COMSEC equipment.

8.1.2.3. Using COMSEC equipment without completing a required alarm-check test or after failure of a required alarm-check test.

Table 3. Reporting a Practice Dangerous to Security.

RULE	If the PDS Involves:	The COMSEC Manager:
1	**A**. Premature or out of sequence use of keying material without the approval of the controlling authority (as long as the material was not reused). **B**. Inadvertent destruction of keying material. **C**. Destruction without authorization of the controlling authority as long as the destruction was properly performed and documented. **D**. Protective packaging inadvertently cut while unpacking the shipping container. **E**. Removing keying material from its protective technology before issue for use. **F**. Removing the protective technology without authorization, as long as the removal was documented and there is no evidence of espionage. **G**. Unclassified accounting legend code (ALC)-1 material. **H**. Classified ALC-4 material.	Sends a routine message:*Action* - Controlling Authority(ies).*Information* - Account's MAJCOM IA Office, Violating Unit's Commander and MAJCOM IA Office. Within 3 duty days of notification, or sooner if specified by controlling authority instructions or if circumstances warrant. Complete any actions requested by the controlling authority or MAJCOMs.
2	**A**. Failure to remove fill batteries from cryptographic equipment items prior to shipping.	Sends a routine message:*Action* - DIRNSA/I413.*Information* - Violating Unit's Commander, COMSEC Account, and MAJCOM IA Office.
3	**A**. Receiving a package with a damaged outer wrapper in which the inner wrapper is intact. **B**. Unclassified ALC-4 material. **C**. Activating the antitamper mechanism on or unexplained zeroization of COMSEC equipment when no other signs of unauthorized access or penetration are present. **D**. Failure to zeroize a common fill device within 12 hours of supersession of the effected keying material. **E**. Destruction of COMSEC material not performed within required time limits, but the material was properly stored or safeguarded. **F**. Loss of STU-III User CIK or Master CIK. **G**. Administrative/documentation errors on control and accountability records BUT 100 percent control of material maintained.	Does not report the PDS upchannel. Resolves the situation locally. Erase CIK from STU-III (Rule F only). Hold documentation for MAJCOM review during the Information Protection Assessment and Assistance Program (IPAP)(Rule G only).

8.1.3. Using a cryptosystem not approved by NSA.

8.1.4. Discussing the details of a COMSEC equipment failure or malfunction on nonsecured telecommunications equipment.

8.1.5. Reportable cryptographic security incident specifically identified in a system's security doctrine.

8.1.6. Any other occurrence that may jeopardize the cryptosecurity of a COMSEC system.

8.2. Personnel Incidents. Personnel incidents include the capture, attempted recruitment, or control of personnel by a known or suspected foreign intelligence entity, or the unauthorized absence or defection of personnel having knowledge of or access to COMSEC information or material. Report these incidents by message (see **attachment 4** and **attachment 7**).

8.3. Physical Incidents. Physical incidents include loss of control (material out of COMSEC channels but control is later restored), lost material, lost STU-III Seed Key, theft, capture, recovery by salvage, tampering, unauthorized viewing and access, photographing, or copying that can potentially jeopardize COMSEC material. Report physical incidents by message (see **attachment 4** and **attachment 5**). Examples include:

8.3.1. Unauthorized access to COMSEC material.

8.3.2. COMSEC material found outside required physical control. Examples include:

8.3.2.1. Finding COMSEC material documented as being destroyed.

8.3.2.2. COMSEC material left unsecured.

8.3.3. COMSEC material improperly packaged, shipped, or received with a damaged inner wrapper.

8.3.4. Destruction of COMSEC material by other than authorized means, not properly performed and documented (i.e., only one person destroying), or COMSEC material not completely destroyed and left unattended.

8.3.5. Actual or attempted unauthorized maintenance (including maintenance by unqualified personnel) or using a maintenance procedure that deviates from established standards.

8.3.6. Tampering with or penetration of a cryptosystem. Examples include:

8.3.6.1. Known or suspected tampering with, or unauthorized modification of, COMSEC material or its associated protective technology.

8.3.6.2. Finding an electronic surveillance or recording device in or near a COMSEC facility.

8.3.6.3. Activation of the antitamper mechanism on, or unexplained zeroization of, COMSEC equipment when other signs of unauthorized access or penetration are present. (***NOTE***: Hold information concerning tampering with COMSEC equipment, penetration of protective technologies, or clandestine devices on a strict need-to-know basis. Immediately report by the most secure means to NSA, AFOSI, or Federal Bureau of Investigation, the controlling authority, and HQ AFCA/GCIS. When tampering or penetration is known or suspected, wrap and seal the material along with all protective technologies and place the package in the most secure, limited-access storage available. Do not use or otherwise disturb the material until further instructions are received from NSA. When a clandestine surveillance or recording device is suspected do not discuss it in the area of the device, or anywhere else you suspect a device is installed. Take no action that will alert the clandestine activity, except on instruction from the applicable counterintelligence organization or NSA. Take no action that will jeopardize potential evidence.)

8.3.7. Unexplained removal of keying material from its protective technology.

8.3.8. Unauthorized reproduction or photographing of COMSEC material. (***NOTE***: You can locally reproduce manual cryptosystems as necessary to meet operational requirements per AFI 33-215.)

8.3.9. Deliberate falsification of COMSEC records.

8.3.10. Loss of two-person integrity or violation of COMSEC no-lone zone for TOP SECRET material (see AFKAG-1, *Air Force Communications Security [COMSEC] Operations*).

8.3.11. Incidents involving CCI. Include serial numbers for all CCI involved in all reports. Format and report the information according to **attachment 4** and **attachment 5**. Report those incidents where:

8.3.11.1. There is a determination that a CCI may be lost and cannot be accounted for. (***NOTE***: Get information for the final report from the results of the report of survey or conduct an inquiry according to this AFI.)

8.3.11.2. There is evidence of possible tampering or unauthorized access to or modification of a CCI.

8.3.11.3. There are indications of known or suspected theft of a CCI.

8.3.11.4. A CCI is shipped in anything other than a zeroized or unkeyed condition and the shipping activity failed to get prior authorization according to AFKAG-1.

8.3.12. Report of suspected tampering or penetration of a "protected distribution system."

8.3.13. Reportable physical security incident specifically identified in a system's security doctrine.

8.3.14. Any other incident that jeopardizes the physical security of COMSEC material.

8.4. Aircraft Accidents and Disasters (Natural or Man-made):

8.4.1. Use **attachment 4** and **attachment 5** to report aircraft accidents and disaster incidents.

8.4.2. Aircraft and disaster incidents are only assigned case numbers and tracked under the purview of this AFI to clear the accounting records of any COMSEC material or CCI involved and to follow any recovery efforts (if practicable).

8.4.3. A formal inquiry is not required for aircraft and disaster incidents. For aircraft incidents, the report must identify where the aircraft crashed, progress of recovery efforts, circumstances involving recovery, what material was recovered and the extent of damage, and what material was not recovered and the most likely disposition (e.g., destroyed in crash, retrieved by enemy, recovered by uncleared rescue personnel and turned over to security police, etc.) For disaster incidents, the report must identify progress of recovery efforts, circumstances involving recovery, the extent of damage to recovered material, what material was not recovered, etc.

9. Reporting Communications Security Incidents .

9.1. Additional Applicable Directives. Report incidents using this AFI. In addition, depending on the material involved in the incident, submit additional information/reports according to the requirements of the applicable directives shown below:

9.1.1. Report incidents involving North Atlantic Treaty Organization (NATO) COMSEC material as prescribed in Allied Military Security Guide 293, *NATO Cryptographic Instructions*.

9.1.2. Report incidents involving communications-electronics operating instructions and status information of keying material according to AFI 31-401, *Information Security Program Management*.

9.1.3. Refer to AFSSI 4001, *Controlled Cryptographic Items*, for additional instructions regarding COMSEC equipment designated CCI.

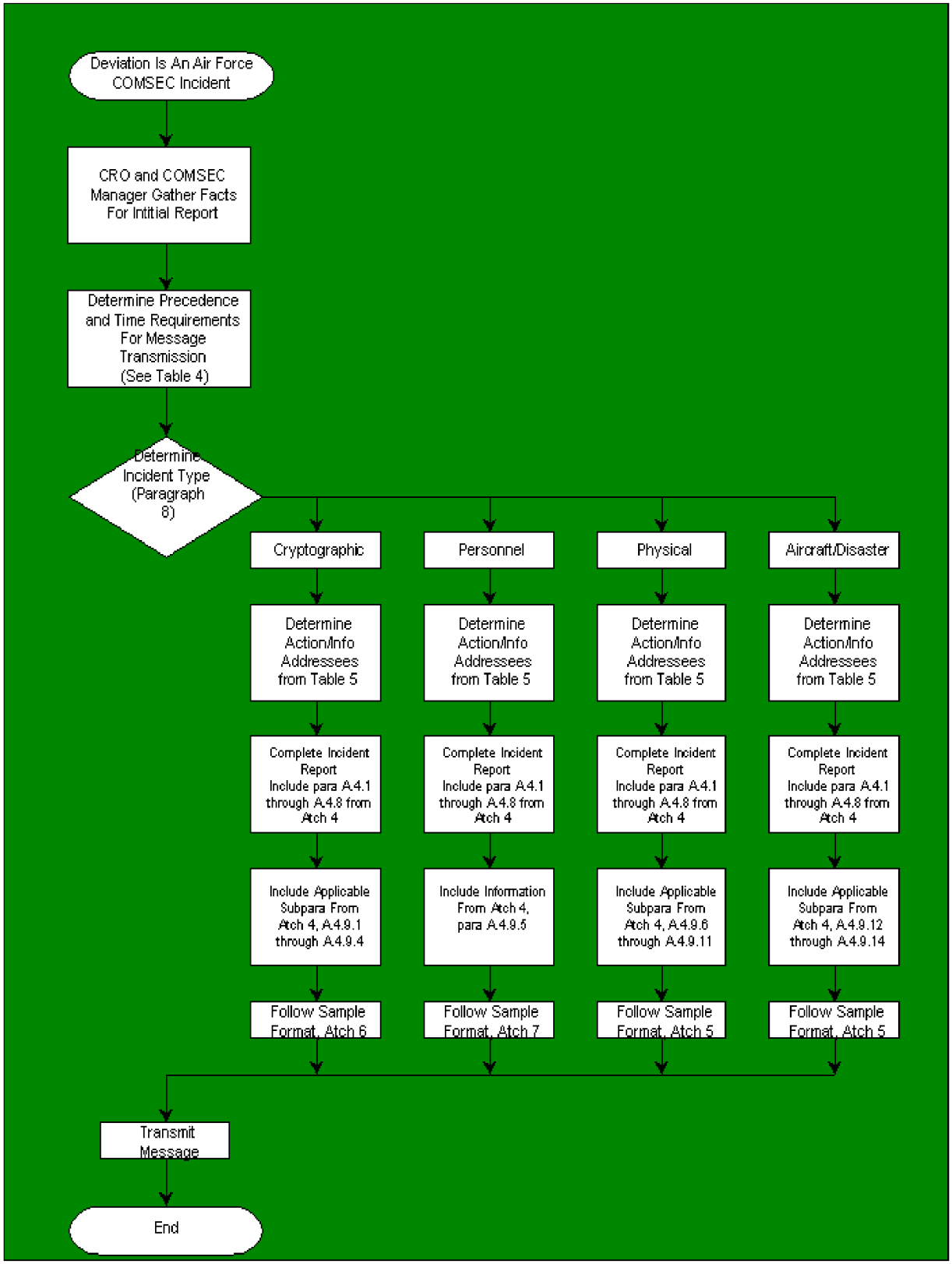
9.2. National COMSEC Incident Reporting System. Per NSTISSI 4003, "To be effective, the National COMSEC Incident Reporting System must receive prompt and clear information relating to the circumstances surrounding an incident. This information is critical to the rapid initiation of appropriate damage limitation or recovery measure by the evaluating authority." NSA continually evaluates the security of cryptosystems used by the United States Government. Each incident, regardless of how minor it may seem when compared to other reports or information, often reveals weaknesses in procedures, systems, or personnel that can result in compromises. Therefore:

9.2.1. Every person possessing, handling, operating, maintaining, or repairing COMSEC material/equipment must stay thoroughly familiar with applicable physical and cryptographic security rules and will immediately report COMSEC incidents to the CRO, the COMSEC manager, or the commander. Failure to promptly report an incident may seriously affect the security of the cryptosystem involved and the defense of the United States. The CRO reports the incident to the COMSEC manager. The COMSEC manager, using the information provided by the CRO, reports the incident as prescribed in this publication.

9.2.2. Any person or activity detecting or suspecting that an incident involving COMSEC has occurred is responsible for reporting it in accordance with this instruction.

9.3. AFOSI Involvement in COMSEC Investigations. When the commander of the violating unit determines that the AFOSI should assume the investigation of a COMSEC incident, the violating unit stops its inquiry or investigation. During this period, the commander of the violating unit submits amplifying reports, through the COMSEC account, every 30 days indicating the AFOSI investigation is still ongoing. When AFOSI provides its final report, the commander reviews it with the COMSEC manager and sends it through COMSEC incident channels.

Figure 2. COMSEC Incident Initial Report Process.



NOTES:

(1) After determining that a COMSEC incident has occurred, the CRO and the COMSEC manager gather all remaining facts required to complete the initial report. Do not delay the initial report to get ALL facts; report what information is available and submit an amplifying report once relevant information is obtained.

(2) The COMSEC manager determines the message precedence and the time frame for message transmission based upon incident severity, effective period of material, and incident type (**table 4.**). After the COMSEC manager determines the incident type, the action and info addressees for the message are determined (**table 5.**).

(3) Different incident types require different information reporting. Refer to **attachment 4** (deviation information) and **attachment 5**, **attachment 6**, and **attachment 7** (sample message formats) for the requirements.

10. Communications Security Incident Reporting Procedures .

10.1. Reporting Procedures During Normal Operations. There are six required documents for each Air Force COMSEC incident assigned an Air Force COMSEC incident case number. These documents are: initial or amplifying (if applicable) report, case assignment, final report, evaluation report, MAJCOM closure recommendation, and HQ AFCA/GCIS case closure.

10.1.1. Initial Reports. (**figure 2.** defines the process for completing the COMSEC incident initial report.) When submitting initial COMSEC incident reports during normal operations, assign the appropriate precedence according to **table 4.**, and address the report according to **table 5.** Assign a higher precedence to reports that have a significant potential impact on security.

10.1.1.1. Format report according to the requirements in **attachment 4**, **attachment 5**, **attachment 6**, and **attachment 7**. Initial reports must include each of the paragraphs as shown in the applicable attachments. If the reporting requirements of the paragraph shown in the attachments do not apply, state “not applicable.” Submit reports only by message. Submit letter reports only if message capability is not available or if specifically requested.

10.1.1.2. Classify incident reports according to content. Mark incident reports CONFIDENTIAL when they reveal a unit’s complete or substantially complete (70 percent) holding, or reveal effective dates of classified COMSEC keying material (or reveal enough information to determine the effective date), or identify COMSEC material suspected of being compromised. Mark two-person-controlled material suspected of being compromised SECRET. As a minimum, mark unclassified reports FOR OFFICIAL USE ONLY. For guidance consult AFMAN 33-272, (S) Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information (U); Department of Defense (DoD) 5200.1-R, Information Security Program, January 1997; and AFI 31-401.

10.1.1.3. Do an initial report for each COMSEC incident. Do not delay reporting through administrative channels simply to gather more information. Initial reports are authorized for transmission during MINIMIZE. The initial report may serve as the final report if it contains all information required by paragraph **10.1.4.**, has sufficient information for the controlling authorities to evaluate the incident, and is accepted as a final report by HQ AFCA/GCIS. If the initial report is used as the final report, it must state “Request HQ AFCA/GCIS accept this report as the final report.” Only request the initial report accepted as final when an investiga-

tion would not turn up any additional information.

10.1.2. Amplifying Reports. If a final report is not completed within 30 days of the initial report, you must submit an amplifying report through COMSEC channels every 30 days until the final report is submitted. An amplifying report is submitted when new information is discovered, additional information is requested from within the reporting chain, or to provide the status of the final report. Format the report according to **attachment 9** and submit the report according to **table 3.** Amplifying reports are authorized for transmission during MINIMIZE.

Table 4. Assigning Precedence To and Time Requirements for Submitting Initial/Amplifying COMSEC Incident Reports.

RULE	If the Incident Involves:	Assign Action Addressees a Precedence of:	Assign the Information Addressees a Precedence of:	Submit Initial and Amplifying Reports as Soon as Possible, but no Later Than:
1	Currently effective keying material. Defection; espionage; foreign cognizant agent activity; clandestine exploitation; tampering; sabotage; or unauthorized copying, reproduction, or photographing.	IMMEDIATE	IMMEDIATE	24 hours after discovery of the incident or receipt of amplifying information.
2	Future keying material scheduled to become effective within 15 days.	IMMEDIATE	PRIORITY	48 hours after discovery of the incident or receipt of amplifying information.
3	Future keying material scheduled to become effective in more than 15 days. Superseded, reserved, or contingency keying material.	PRIORITY	ROUTINE	48 hours after discovery of the incident or receipt of amplifying information.
4	Material or information not identified above.	ROUTINE	ROUTINE	72 hours after discovery of the incident or receipt of amplifying information.

10.1.3. Case Assignment. Upon receipt of a COMSEC incident initial report, HQ AFCA/GCIS will assign a case number and respond with a case assignment message within five working days upon receipt of initial report.

10.1.3.1. Case numbers are comprised of the violating unit's MAJCOM acronym followed by "P" (for physical), "C" (for cryptographic), "H" (for personnel), "A" (for aircraft), or "D" (for disaster), followed by the next unused case number for that MAJCOM, and the year the incident took place (e.g., ACC-P-01-98). (***NOTE***: Air National Guard incidents will begin with ANG, followed in parenthesis by the gaining MAJCOM of the violating unit (e.g., ANG-(ACC)-P-00-00)).

Table 5. Addressing COMSEC Incident Reports.

RULE	If The Incident Is:	Send Action Message To:	Send Information Copy To:	The Incident Is Evaluated By:
1	A physical incident involving only one controlling authority.	Controlling Authority	HQ AFCA/GCIS DIRNSA/I413 Violating Unit Commander Violating Unit's MAJCOM Reporting Account's MAJCOM	Controlling Authority
2	A physical incident involving multiple Air Force controlling authorities.	HQ AFCA/GCIS	Controlling Authorities DIRNSA/I413 Violating Unit Commander Violating Unit's MAJCOM Reporting Account's MAJCOM	HQ AFCA/GCIS
3	A physical incident involving a protected distribution system.	HQ AFCA/GCIS	Violating Unit Commander Violating Unit's MAJCOM Reporting Account's MAJCOM	HQ AFCA/GCIS
4	A physical incident involving controlling authorities from more than one department or agency.	DIRNSA/I413	Controlling Authorities HQ AFCA/GCIS Violating Unit Commander Violating Unit's MAJCOM Reporting Account's MAJCOM	DIRNSA/I413
5	A physical incident and the controlling authority cannot be determined.	DIRNSA/I413	HQ AFCA/GCIS Violating Unit Commander Violating Unit's MAJCOM Reporting Account's MAJCOM	DIRNSA/I413
6	A cryptographic incident or involves COMSEC equipment.	DIRNSA/I413	HQ AFCA/GCIS Violating Unit's MAJCOM Violating Unit Commander Reporting Account's MAJCOM	DIRNSA/I413

7	A personnel incident.	DIRNSA/I413	Controlling Authorities for each item they had access HQ AFCA/GCIS Violating Unit Commander Violating Unit's MAJCOM Reporting Account's MAJCOM	DIRNSA/I413

10.1.3.2. If the initial report is relaying information relating to a PDS, HQ AFCA/GCIS will not assign a case number. If the MAJCOM/COMSEC account requests evaluation for a deviation determination, HQ AFCA/GCIS will either generate a case assignment message or notify the MAJCOM/COMSEC account that no case number was assigned.

10.1.4. Final Reports (see **attachment 10**). A final report is required for each COMSEC incident unless the initial or an amplifying report was accepted as the final report. Include verbatim the inquiry officialÕs report within the final report. The final report must identify corrective measures taken or a plan to minimize the possibility of recurrence. Additional actions required for the final report:

10.1.4.1. Do not send final reports during MINIMIZE. Assign ROUTINE precedence to final reports.

10.1.4.2. Submit the report through the violating unit's commander and COMSEC manager for their comments and concurrence or nonconcurrence. The COMSEC manager then transmits the report to all required addressees.

10.1.5. Incident Evaluation. Upon receipt of the report of inquiry or investigation, the controlling authority (if not previously determined from the initial or amplifying COMSEC incident report) evaluates the incident as (a) a compromise (may recommend upgrading the incident to an insecurity, if appropriate), (b) a compromise cannot be ruled out, or (c) no compromise. Incidents evaluated based on the information provided in the initial report must have a new evaluation if the findings of the investigation relayed in the final report substantially change the circumstances outlined in the initial report.

10.1.6. MAJCOM Closure Recommendation. Within five working days of receipt of the final report or controlling authority evaluation (whichever is received last), the MAJCOM sends a message addressing actions taken by the violating unit and the COMSEC account to prevent recurrence of the incident. If the actions taken are sufficient, the MAJCOM recommends closing the COMSEC incident. If actions are not sufficient, the MAJCOM sends a message to the COMSEC account recommending actions to take. The COMSEC account must submit an amplifying report requesting case closure once the additional action is complete. The MAJCOM once again must review the actions and recommend case closure before AFCA will close the incident case. MAJCOMs address their recommendation for case closure message action to HQ AFCA/GCIS and include the action and info addressee listed in **table 5.** (***NOTE***: MAJCOMs do not evaluate incidents.)

10.1.6.1. Do not submit a request for incident closure until the incident is evaluated by the controlling authority and the final report submitted to HQ AFCA/GCIS. MAJCOMs may pro-

vide direction/comments at any time during an inquiry/investigation. If 30 days has elapsed since receipt of the final report from the violating unit, and HQ AFCA/GCIS has not received an evaluation, HQ AFCA/GCIS will contact the controlling authority for an evaluation.

10.1.7. Case Closure. HQ AFCA/GCIS closes the case within 10 working days of receipt of all required correspondence (initial report, final report, controlling authority's evaluation, and MAJCOM comments).

10.2. Reporting During Tactical Deployments:

10.2.1. During time-sensitive tactical deployments, detailed reporting may not be possible. If so, submit abbreviated reports for physical incidents involving keying material where espionage is not suspected. The report must answer the "who, what, where, when, and how" questions, and provide enough detail to enable the evaluating authority to determine if a compromise has occurred.

10.2.2. Immediately report loss of keying material during actual hostile actions to each controlling authority by the fastest means available to allow supersession or recovery actions, if applicable. Use any available secure means.

10.2.3. In many cases, immediate reporting to the activities listed in **table 5.** other than the controlling authority will serve no purpose. Individual incident reports are not needed when keying material scheduled for supersession within 48 hours is lost during actual hostilities and espionage is not suspected. Submit a periodic summary of all previously unreported incidents at the earliest opportunity (see **table 4.**). The summary lists all material lost, dates, places, and a brief synopsis for the circumstances of loss.

10.3. Controlling Authority Evaluation. Use the guidelines in **attachment 13** to evaluate COMSEC incidents. Controlling authorities may render an evaluation of a PDS.

10.4. Disposal of Material Involved in a COMSEC Incident:

10.4.1. When material on hand is subjected to a physical or cryptographic incident, keep the material until receipt of HQ AFCA/GCIS case closure message as stated in paragraph **10.1.7.**, unless prior disposition instructions are received from the controlling authority.

10.4.2. When an incident involves use of superseded key, the violating unit must have the means to provide the controlling authority copies of all traffic transmitted using the key if a traffic review is directed per AFI 33-215.

10.5. Removing Material Involved in a Physical Loss from COMSEC Accounting Records. HQ AFCA/GCIS issues a case closure message when the inquiry or investigation is completed and all information required in this AFI is received. Use the case closure message as the authority for destruction and dropping accountability for the material from account records. If the material involved appears on the next semiannual inventory, line through the applicable items and cite the case number and case closure message date-time group (DTG), and state the case is closed in the remarks section to make sure the Air Force Central Office of Records can take the appropriate action.

11. Communications Security Incident and Insecurity Trends . HQ AFCA/GCIS will develop and send a COMSEC incident and insecurity trends summary to all MAJCOMs and HQ USAF/SCMIP semiannually (no later than 31 January for July through December, and 31 July for January through June).

11.1. The summary will include the different types of physical and cryptographic incidents/insecurities, the total number, and the major causes of incidents and insecurities. Personnel, aircraft, and disaster incidents are not included in the summary.

11.2. MAJCOMs must comment on the summaries and disseminate this information to their subordinate units and MAJCOM functional areas. COMSEC accounts must distribute this analysis to each CRO they service.

JOHN L. WOODWARD, JR., Lt Gen, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSI 3260.01, (S) *Joint Policy Governing Positive Control Material and Devices (U)*

DoD 5200.1-R, *Information Security Program*, January 1997

AFI 31-401, *Information Security Program Management*

AFPD 33-2, *Information Protection*

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

AFMAN 33-272, (S) *Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information (U)*

AFDIR 33-303, *Compendium of Communications and Information Terminology*

AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (will convert to AFI 33-324)

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-322V4)

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

AFKAG-2, *Air Force COMSEC Accounting Manual*

AFSSI 4001, *Controlled Cryptographic Items*

AMSG-293, *NATO Cryptographic Instructions*

NSTISSI 4003, *Reporting and Evaluating COMSEC Incidents*

Abbreviations and Acronyms

CAN—Accounting Control Number

AFCA—Air Force Communications Agency

AFDIR—Air Force Directory

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

AFSSI—Air Force Systems Security Instruction

ALC—Accounting Legend Code

ANG—Air National Guard

CCI—Controlled Cryptographic Item

CIK—Crypto-Ignition Key

CITA—COMSEC Incident Trend Analysis

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

COMSEC—Communications Security

CRO—COMSEC Responsible Officer

CRYPTO—Cryptographic

DIRNSA—Director, National Security Agency

DoD—Department of Defense

DSN—Defense Switched Network

DTG—Date-Time Group

E-mail—Electronic Mail

EKMS—Electronic Key Management System

IA—Information Assurance

IPAP—Information Protection Assessment and Assistance Program

JCS—Joint Chiefs of Staff

MAJCOM—Major Command

LMD/KP—Local Management Device/Key Processor

NATO—North Atlantic Treaty Organization

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

PCM—Positive Control Material

PDS—Practice Dangerous to Security

POC—Point of Contact

SSN—Social Security Number

STU—Secure Telephone Unit

Terms

Access—Capability and opportunity to gain knowledge of or to alter information or material. ***NOTE***: A person does not have access merely by being in a place where COMSEC material is kept as long as security measures (i.e., physical controls or authorized escort) deny opportunity to observe the material.

AFKAG—A short title used on general operational Air Force COMSEC publications. These publications are controlled in COMSEC channels.

Codebook Incident—An occurrence involving material governed by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3260.01, (S) *Joint Policy Governing Positive Control Material and Devices (U)*. Incident reports are processed and filed in accordance with CJCS policy. HQ AFCA/GCIS is an information addressee on all codebook incident correspondence.

COMSEC Deviation—An occurrence involving failure to follow established COMSEC instructions, procedures, or standards.

COMSEC Incident—An occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information.

COMSEC Insecurity—A COMSEC incident that was investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information. Incident was evaluated as "COMPROMISE."

COMSEC Material Receipt Discrepancy—An occurrence where the contents of the COMSEC package do not agree with the shipping documents and no tampering of the package is evident.

Cryptosecurity—Component of COMSEC that results from the provisions of technically sound cryptosystems and their proper use.

Date Stamped on Protective Technology—Each key tape canister is hot stamped with a date/line code consisting of four characters. Three of the characters are on the body's flat surface and one is on the adjacent edge of the cover. See protective technology pamphlets for more information.

Electronically Generated Key—Key produced only in non-physical form. (***NOTE***: An electronically generated key stored magnetically [e.g., on a floppy disk]) is not considered a hard copy key. Electronically generated keys are divided into two groups: 1. Field-Generated Electronic Keys. Used primarily for tactical communications nets in an operational environment. Normally used only to provide security for perishable, time-sensitive communications. Mobile facilities in the field or fixed COMSEC facilities may produce field-generated electronic keys. 2. Electronic Key Management System (EKMS)-Generated electronic keys used primarily for planned, static applications with well-defined net membership. Used to provide security for non-perishable information requiring a high degree of security. EKMS-generated key is produced or transferred by the local management device/key processor (LMD/KP) at a COMSEC account.

Emergency Supersession—Substantial evidence exist that the COMSEC material was compromised and the controlling authority directs the immediate use of the next edition/segment.

MINIMIZE—A condition where normal message and telephone traffic is drastically reduced so that messages connected with an actual or simulated emergency are not delayed.

Practice Dangerous to Security (PDS)—A procedure that has the potential to jeopardize the security of COMSEC material if allowed to continue. (***NOTE***: A PDS is not a COMSEC incident and does not have an Air Force COMSEC case number assigned.)

Physical Security—Component of COMSEC that results from all measures necessary to safeguard classified equipment, material, and information from access or observation by unauthorized persons.

Positive Control Material—Generic term referring to a sealed authenticator systems; permissive action link, coded switch system; positive enable system, or nuclear command and control documents, material, or devices.

Production Error/Defective Key—An occurrence where a reported discrepancy appears to be the result of a production error or a defect with the keying material. DIRNSA/Y265 is responsible for evaluating the material in question.

Protected Distribution System—Wireline or fiber optics telecommunications system that includes

terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information. ***NOTE***: This definition does not include intrusion detection optical communications systems approved by the National Security Agency.

Protective Packaging—Packaging techniques for COMSEC material that discourage penetration, reveal that a penetration has occurred or was attempted, or inhibit viewing or copying of keying material before it is exposed for use.

Protective Technologies—Special tamper-evident features and material employed to detect tampering and deter attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.

Supersession—Scheduled or unscheduled replacement of a COMSEC aid with a different edition.

Supersession Date—The date the material is scheduled for replacement by a new edition/segment.

Attachment 2

SAMPLE -- COMSEC RECEIPT DISCREPANCY REPORT

FM UNIT BASE//CAXXXXXX//

TO (See Table 1)

INFO HQ AFCA SCOTT AFB IL//GCIS//

DIRNSA FT GEO G MEADE MD//I413//

HQ CPSG SAN ANTONIO TX//ZSKM//

CONTROLLING AUTHORITY (IES)//

MAJCOM IA OFFICE//

U N C L A S S I F I E D

MSGID/GEN ADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC RECEIPT DISCREPANCY//

POC/NAME/TITLE/UNIT/LOC:/TEL (DSN and Commercial)/E-MAIL//

RMKS/1. THIS COMSEC ACCOUNT RECEIVED A COURIER SHIPMENT CONTAINING COMSEC DOCUMENTS WITH A MISSING PAGE. PACKAGE (number) WAS RECEIVED ON (date) AND SHOWED NO EVIDENCE OF TAMPERING. INSIDE THE PACKAGE WAS (short title), EDITION (XX), ACCOUNTING CONTROL NUMBERS (XX-XX). WHILE PAGE CHECKING, IT WAS DISCOVERED THAT BOOK NUMBER(S) (XX and XX) WERE MISSING (list what is missing). ALL OTHER COPIES HAVE BEEN CHECKED AND HAVE THE CORRECT NUMBER OF PAGES.

2. REQUEST DISPOSITION INSTRUCTIONS BE PROVIDED.//

(Sample paragraphs identifying receipt of COMSEC documents with missing pages)

-- (number) COMSEC DOCUMENTS THAT WERE NOT IDENTIFIED ON THE ENCLOSED SF153. PACKAGE (number) WAS RECEIVED ON (date) AND SHOWED NO EVIDENCE OF TAMPERING. INSIDE THE PACKAGE WAS A SF 153 IDENTIFYING (short title), EDITION (XX), ACCOUNTING CONTROL NUMBERS (XX-XX); HOWEVER, THE PACKAGE ACTUALLY CONTAINED (short title), EDITION (XX), ACCOUNTING CONTROL NUMBERS (XX-XX).

3. THE UNLISTED COPIES HAVE BEEN ADDED AS A LINE ITEM TO OUR VOUCHER (number)//.

(Sample paragraphs identifying receipt of COMSEC material not listed on SF 153):

-- SF 153 LISTING (number) LINE ITEMS BUT ONLY (number) WERE ACTUALLY IN THE PACKAGE. PACKAGE (number) WAS RECEIVED ON (date) AND SHOWED NO EVIDENCE OF TAMPERING. INSIDE THE PACKAGE WAS A SF 153, OUTGOING VOUCHER NUMBER (number), IDENTIFYING (short titles), EDITIONS (XX), ACCOUNTING CONTROL NUMBERS (XX-XX). ALL COPIES OF (short titles) WERE RECEIVED, HOWEVER, (short title), EDITION (XX), ACCOUNTING CONTROL NUMBERS (XX-XX) WERE NOT IN THE PACKAGE.

4. THE ITEMS THAT WERE NOT IN THE PACKAGE HAVE BEEN LINED OFF OUR VOUCHER (number).//

(Sample paragraphs identifying nonreceipt of COMSEC documents listed on SF 153)

Attachment 3

SAMPLE -- COMSEC PRODUCTION ERROR/DEFECTIVE KEYING MATERIAL FORMAT

FM UNIT BASE//CAXXXXXX//

TO DIRNSA FT GEO G MEADE MD//Y265//

INFO HQ AFCA SCOTT AFB IL//GCIS//

DIRNSA FT GEO G MEADE MD//I413//

HQ CPSG SAN ANTONIO TX//ZSKM//

CONTROLLING AUTHORITIES//

MAJCOM IA OFFICE//

C O N F I D E N T I A L

MSGID/GEN ADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC MATERIAL PRODUCTION ERROR/DEFECTIVE KEYING MATERIAL//

POC/NAME/TITLE/UNIT/LOC:/TEL (DSN and Commercial)/E-Mail//

RMKS/1. (U) COMSEC ACCOUNT: XXXXXX.

2. (C) MATERIAL INVOLVED: Short title, edition, accounting control numbers.

A. UNIT USING MATERIAL: (If the material has been issued to the user)

B. PERSONNEL INVOLVED:

C. CIRCUMSTANCES THAT UNCOVERED THE PROBLEM:

3. REQUEST DISPOSITION INSTRUCTIONS.

4. CLASSIFIED BY: AFMAN 33-272

DECLAS: X1//

Attachment 4

REQUIRED COMSEC DEVIATION REPORT INFORMATION

A4.1. Subject . Consists of only the words “Practice Dangerous to Security” or “COMSEC Incident” followed by “Initial Report” or the complete case number IF ALREADY ASSIGNED.

A4.2. References . Identify the reporting requirement and all previously related messages and correspondence. Initial report will identify the applicable paragraph from this AFI.

A4.3. Point of Contact (POC) . Include name, COMSEC account number, secure telephone number, Defense Switched Network (DSN) telephone number, commercial telephone number, and electronic mail (e-mail) address (if available) of an individual who is prepared to respond to questions concerning the incident.

A4.4. COMSEC Account . COMSEC account number supporting the unit responsible for the incident.

A4.4.1. Includes the violating unit and its MAJCOM.

A4.5. Material Involved .

A4.5.1. For Hard-Copy Keying Material, Hard-Copy Key-in Electronic Form, and Documents. List the short title, edition, register number, specific segments, ALC, classification of material, tables, pages, etc., if not a complete edition or document; and date stamped on the protective technology, if applicable. The controlling authority for each short title MUST BE stated by each piece of material on the initial COMSEC incident message report.

A4.5.2. For Electronically Generated Key. List the key designator, tag, or other identifier; type of cryptographic (crypto) equipment used to secure the circuit; type of key generator; ALC; and classification of material.

A4.5.3. For Equipment. List the system designator or nomenclature; modification number, if applicable; serial number of ALC-1 material (all other by quantity); serial number on the protective technology, if applicable; and associated or host equipment. If the equipment was keyed, provide the information required for keying material.

A4.6. Personnel Involved in the Deviation . For each individual, provide name and grade, citizenship, service component (if other than Air Force), duty position, military or civilian occupation specialty (i.e., Air Force Specialty Code [AFSC]), level of security clearance, and parent MAJCOM.

A4.7. Circumstances of the Deviation . Give a clear chronological account of the events that caused the incident. The chronology includes all dates, times, frequency of events, precise locations and organizational elements, etc. If the reason for the incident is not known, describe the events that led to the discovery of the incident. Include a description of the security measures in effect at the location and estimate the possibility of unauthorized personnel gaining access to the material.

A4.8. Possibility of Compromise . Provide an opinion as to the possibility of compromise (e.g., no compromise, compromise cannot be ruled out, compromise) and the basis for the opinion.

A4.9. Additional Reporting Requirements When Incident Involves :

A4.9.1. Incorrect Use of COMSEC Keying.

A4.9.1.1. Describe the communications activity (e.g., COMSEC keying on-line/off-line, simplex/half-duplex/full-duplex, point-to-point/netted operations).

A4.9.1.2. Describe the operating mode of the cryptoequipment (e.g., clock start, message indicator).

A4.9.2. Use of Unapproved Operating Procedures.

A4.9.2.1. Estimate the amount and type of traffic involved.

A4.9.2.2. Estimate the length of time the key was used.

A4.9.3. Use of Malfunctioning COMSEC Equipment.

A4.9.3.1. Describe the symptoms of the malfunction.

A4.9.3.2. Estimate the likelihood that the malfunction was deliberately induced. If so, also refer to paragraph **a4.9.5.**

A4.9.3.3. Estimate how long the malfunctioning equipment was in use.

A4.9.3.4. Estimate the amount and type of traffic involved.

A4.9.4. Unauthorized Modification or Discovery of a Clandestine Electronic Surveillance or Recording Device in or Near a COMSEC Facility.

A4.9.4.1. Describe the modification or monitoring device, installation, symptoms, host maintenance of COMSEC equipment involved, and protective equipment technology, if applicable.

A4.9.4.2. Estimate how long the item was in place.

A4.9.4.3. Estimate the amount and type of traffic involved.

A4.9.4.4. Identify the counterintelligence organization (e.g., AFOSI), a POC, and telephone number.

A4.9.5. Known or Suspected Defection, Foreign Cognizant Agent Activity, Attempted Recruitment, Espionage, Sabotage, Treason, Capture, or Unauthorized Absence.

A4.9.5.1. Describe the individual's general background in COMSEC and the extent of knowledge of crypto principles and protective technologies.

A4.9.5.2. List the cryptosystems that the individual had access to and whether the access was to cryptographic logic or keying material. For logic, state whether access was too full or limited maintenance manuals; for keying material, list the short titles and editions involved.

A4.9.5.3. Identify the counterintelligence organization (e.g., AFOSI), a POC, and telephone number.

A4.9.6. Unauthorized Access to COMSEC Material.

A4.9.6.1. Estimate how long unauthorized personnel had access to the material.

A4.9.6.2. State whether espionage is suspected. If espionage is suspected, refer to paragraph **a4.9.5.**

A4.9.7. Loss of COMSEC Material.

A4.9.7.1. Describe the circumstances of last sighting. Provide all available information concerning the cause of disappearance.

A4.9.7.2. Describe actions taken to locate the material. ***NOTE***: Consider the possibility that authorized or unauthorized persons removed material.

A4.9.7.3. Describe the methods of disposal of classified and unclassified waste and the possibility of loss by those methods.

A4.9.8. COMSEC Material Discovered Outside of Required COMSEC Accountability or Control.

A4.9.8.1. Describe the action that restored accountability or physical control.

A4.9.8.2. Estimate the likelihood of unauthorized access.

A4.9.8.3. Estimate the time the material was unsecured.

A4.9.9. COMSEC Material Received With a Damaged Inner Wrapper.

A4.9.9.1. Give a complete description of the damage.

A4.9.9.2. Describe situations where damage occurred in transit and identify the mode of transportation. Include the package number and point of origin.

A4.9.9.3. Describe how the material was stored if the damage occurred in storage.

A4.9.9.4. Estimate the likelihood of unauthorized access or viewing.

A4.9.9.5. Retain all packaging containers, wrappers, etc., until destruction is authorized.

A4.9.10. Known or Evidence of Suspected Tampering With COMSEC Material.

A4.9.10.1. Describe the evidence of tampering.

A4.9.10.2. Identify the mode of transportation if the suspected tampering occurred in transportation. Include the package number and point of origin.

A4.9.10.3. Describe how the material was stored if the suspected tampering occurred in storage.

A4.9.10.4. Identify the counterintelligence organization (e.g., AFOSI), a POC, and telephone number.

A4.9.10.5. Identify the date stamped on the protective technology, or serial number on the protective technology, if applicable.

A4.9.11. Unauthorized Reproduction or Photography.

A4.9.11.1. Identify the material or equipment reproduced or photographed.

A4.9.11.2. Provide the reason for the reproduction and describe how the material was controlled.

A4.9.11.3. Specify how detailed the photographs of equipment internals were.

A4.9.11.4. State whether espionage is suspected. If espionage is suspected, refer to paragraph A4.9.5.

A4.9.11.5. Forward copies of each photograph or reproduction to DIRNSA/I413 and HQ AFCA/GCIS.

A4.9.12. Aircraft Crash or Disaster Incidents.

A4.9.12.1. Identify all damaged/lost/unaccounted for/unrecoverable CCIs involved. Specify equipment name, national stock number, and serial number.

A4.9.12.2. Identify the location and coordinates of the crash/site of disaster, and specify whether the crash/disaster incident was in friendly or hostile territory. If an aircraft incident is at sea, paragraph **a4.9.13.** lists the additional required information to report.

A4.9.12.3. State whether the aircraft or material involved in the disaster remained largely intact or if wreckage/material was scattered over a large area. Estimate the size of the area.

A4.9.12.4. State whether the area was secured. If the area was secured, state how soon after the crash/disaster incident and by whom.

A4.9.12.5. State whether recovery efforts for COMSEC material were made or are anticipated, and the circumstances involving recovery.

A4.9.12.5.1. State what material was recovered and the extent of damage.

A4.9.12.5.2. State what material was not recovered and the most likely disposition (e.g., destroyed in crash/disaster, retrieved by enemy, recovered by uncleared rescue personnel and turned over to security police, etc.).

A4.9.13. Material Lost at Sea.

A4.9.13.1. Provide the coordinates (when available) or the approximate distance and direction from shore.

A4.9.13.2. Estimate the depth of the water.

A4.9.13.3. State whether material was in weighted containers or was observed sinking.

A4.9.13.4. Estimate the sea state, tidal tendency, and the most probable landfall.

A4.9.13.5. State whether United States salvage efforts were made or are anticipated.

A4.9.13.6. State whether foreign vessels were in the immediate area and their registry, if known.

A4.9.13.7. Estimate the possibility of successful salvage operations by unfriendly nations.

A4.9.14. Space Vehicles.

A4.9.14.1. Provide the launch date and time.

A4.9.14.2. State whether the space vehicle was destroyed or lost in space.

A4.9.14.3. State whether the keying material involved was unique to the operation or is common to other operations.

A4.9.14.4. Estimate the probable impact point on the Earth’s surface, if applicable. If the impact point was on land refer to paragraph **a4.9.12.**, if at sea refer to paragraph **a4.9.13.**

Attachment 5

SAMPLE -- INITIAL PHYSICAL, AIRCRAFT, OR DISASTER COMSEC INCIDENT REPORT

FM UNIT BASE//CAXXXXXX//

TO (See **table 4.**)

INFO (See **table 4.**)

HQ AFCA SCOTT AFB IL//GCIS//

VIOLATING UNIT//CC//

SUPPORTING COMSEC ACCOUNT'S MAJCOM IA OFFICE//

VIOLATING UNIT'S MAJCOM IA OFFICE//

DIRNSA FT GEORGE G MEADE MD//I413//(unless an action addressee)

C O N F I D E N T I A L

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT -- INITIAL REPORT//

REF/A/AFI 33-212, PARA 7.3, AS APPLICABLE//

REF/B/Other applicable documents//

REF/C/Additional related correspondence and messages on incident//

POC/NAME/TITLE/UNIT/LOC:/TEL (DSN)/E-MAIL//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

A. VIOLATING UNIT:

B. MAJCOM OF VIOLATING UNIT:

2. (C) MATERIAL INVOLVED. List all material involved in incident including short title, edition, accounting control number (ACN), controlling authority, classification, and accounting legend code (ALC) for each item involved.

3. PERSONNEL INVOLVED IN THE INCIDENT.

4. CIRCUMSTANCES OF INCIDENT.

5. INITIAL INCIDENT ASSESSMENT: COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

6. ADDITIONAL REPORTING REQUIRED BY AFI 33-212 (see **attachment 4**).

7. CLASSIFIED BY: AFMAN 33-272

DECLASS: X1//

Attachment 6

SAMPLE -- INITIAL CRYPTOGRAPHIC COMSEC INCIDENT REPORT

FM UNIT BASE//CAXXXXXX//

TO DIRNSA FT GEORGE G MEADE MD//I413//

INFO HQ AFCA SCOTT AFB IL//GCIS//

ACTUAL CONTROLLING AUTHORITIES//

VIOLATING UNIT//CC//

SUPPORTING COMSEC ACCOUNT'S MAJCOM IA OFFICE//

VIOLATING UNIT'S MAJCOM IA OFFICE//

C O N F I D E N T I A L

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT -- INITIAL REPORT//

REF/A/AFI 33-212, PARA 7.1//

REF/B/OTHER APPLICABLE DOCUMENTS//

REF/C/Additional related correspondence and messages on incident//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN/E-MAIL//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

A. VIOLATING UNIT:

B. MAJCOM OF VIOLATING UNIT:

2. (C) MATERIAL INVOLVED: List all material involved in incident, including short title, edition, accounting control number (ACN), controlling authority, classification, and accounting legend code (ALC) for each item involved.

3. PERSONNEL INVOLVED IN THE INCIDENT:

4. CIRCUMSTANCES OF INCIDENT:

5. INITIAL INCIDENT ASSESSMENT: COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

6. ADDITIONAL REPORTING AS REQUIRED BY AFI 33-212 (see **attachment 4**).

7. CLASSIFIED BY: AFMAN 33-272

DECLASS: X1//

Attachment 7

SAMPLE -- INITIAL PERSONNEL COMSEC INCIDENT REPORT

FM UNIT BASE//CAXXXXXX//

TO DIRNSA FT GEORGE G MEADE MD//I413//

INFO HQ AFCA SCOTT AFB IL//GCIS//

VIOLATING UNIT//CC//

SUPPORTING ACCOUNT'S MAJCOM IA OFFICE//

VIOLATING UNIT'S MAJCOM IA OFFICE//

CONTROLLING AUTHORITIES//

C O N F I D E N T I A L

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT -- INITIAL REPORT//

REF/A/AFI 33-212, PARA 7.2

REF/B/Additional related correspondence and messages on incident.//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN/E-MAIL//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

2. (C) MATERIAL INVOLVED: List all material involved in incident including short title, edition, accounting control number (ACN), controlling authority, classification, and accounting legend code (ALC) for each item involved.

3. PERSONNEL INVOLVED IN THE INCIDENT:

4. CIRCUMSTANCES OF INCIDENT:

5. INITIAL INCIDENT ASSESSMENT: COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

6. ADDITIONAL REPORTING REQUIRED BY AFI 33-212 (see **attachment 4**).

7. CLASSIFIED BY: AFMAN 33-272

DECLAS: X1//

Attachment 8

SAMPLE -- PRACTICE DANGEROUS TO SECURITY (PDS) REPORT

FM UNIT BASE//CAXXXXXX//

TO (See **table 3.**)//

INFO (See **table 3.**)//

C O N F I D E N T I A L

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/PRACTICE DANGEROUS TO SECURITY//

REF/A/AFI 33-212, TABLE 3, RULE X//

REF/B/Additional related correspondence and messages on the PDS.//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN/E-MAIL//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

2. (C) MATERIAL INVOLVED: List all material involved in PDS including short title, edition, ACN, controlling authority, classification, and ALC for each item involved (if CCI is involved, report equipment serial number).

3. PERSONNEL INVOLVED IN THE PDS:

4. CIRCUMSTANCES OF PDS://

5. CLASSIFIED BY: AFMAN 33-272

DECLAS: X1//

Attachment 9

SAMPLE -- AMPLIFYING COMSEC INCIDENT REPORT

FM UNIT BASE//CAXXXXXX//

TO Same as Initial Report

INFO ALL INFO ADDRESSEES (Same as on Initial Report)//

C L A S S I F I C A T I O N (NOTE: As a minimum, mark “FOR OFFICIAL USE ONLY”)

MSGID/GENADMIN/SENDERS OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT (Air Force-assigned case number and all other agencies assigned case numbers) AMPLIFYING REPORT//

REF/A/Reference the DTG of initial report and unit identifier//

REF/B/Additional messages/correspondence relating to the incident//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN/E-MAIL//

RMKS/1. Amplifying reports should provide any new information, or any information that was omitted from the initial report, which can help evaluate the incident.

Where information has not changed, each item is annotated with “N/A.” Include any new information.

This report can be used for status of the ongoing report if not completed in the required time limit.//

Attachment 10

SAMPLE -- FINAL COMSEC INCIDENT REPORT

FM UNIT BASE//CAXXXXXX//

TO Same as Initial Report//

INFO Same as Initial Report//

C L A S S I F I C A T I O N (NOTE: As a minimum mark "FOR OFFICIAL USE ONLY")

MSGID/GENADMIN//SENDERS OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT (Complete case number and all other agencies assigned case numbers)--FINAL REPORT//

REF/A/Reference the DTG and unit identifier of initial report//

REF/B/Reference all other messages/correspondence relating to the incident//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN/E-MAIL//

RMKS/1. PART 1: The inquiry officer's report verbatim (including any attachments).

2. PART 2: Must include the violating unit commander's comments (CONCUR /NONCONCUR is not acceptable).

3. PART 3: Must include the COMSEC manager's comments.//

Attachment 11

SAMPLE -- APPOINTMENT MEMORANDUM OF INQUIRY (OR INVESTIGATING) OFFICIAL

MEMORANDUM FOR (Rank, Full Name of Inquiry/Investigating Official)

FROM: (Violating Unit)/CC

SUBJECT: Appointment of COMSEC Inquiry (or Investigating) Official

1. You are appointed to perform the duties of an inquiry (or investigating) official as outlined in AFI 33-212, *Reporting COMSEC Deviations.* As the appointed official, you are my personal representative in this matter. Your primary duties are to conduct an inquiry (or investigation) into the (state reason for appointment), to determine if a compromise has occurred, and to prepare a report according to AFI 33-212, **attachment 12**. Second, you are to determine if COMSEC weaknesses exist that need to be addressed.

2. You are to gather the facts surrounding the incident and to make recommendations based on those facts. You DO NOT evaluate COMSEC incidents; the controlling authority makes that decision.

3. Process your report through me. The report is due by (15 days from the date of the initial report). If you cannot meet the deadline, contact my office immediately.

4. Point of contact throughout this inquiry is (name of POC) at extension XXXX.

(FULL NAME, RANK), USAF

Commander

Attachment 12

SAMPLE -- INQUIRY (OR INVESTIGATING) OFFICIAL'S REPORT

MEMORANDUM FOR (VIOLATING UNIT/CC) (Date)

(COMSEC OFFICE)

IN TURN

FROM: (Inquiry Official Unit/Office Symbol)

SUBJECT: Report of COMSEC Incident (Case Number) Inquiry (or Investigation)

1. This report is the result of the inquiry (or investigation) conducted regarding the COMSEC incident (Case Number) where (background information of the incident to include: violating unit and workcenter, date of incident discovery, whom it was reported to, and all suspected COMSEC and security violations).

2. The following individuals were interviewed/contacted regarding this incident: (Full Name, Rank, SSN, Squadron, AFSC, and Duty Title).

3. (Individual statements and other pertinent information regarding the incident.)

4. The following conclusions are drawn from the information disclosed throughout this inquiry (or investigation):

(List each individual (a., b., c., etc.) violation that did occur and why/how it occurred, were actions of individual's involved negligent, intentional, etc.)

(State whether there was compromise, compromise cannot be ruled out, or no compromise of classified information and why.)

5. The following recommendations are made to preclude recurrence of this incident:

a. (List any recommendations and suggested means of implementation.)

6. If you have any questions regarding this report contact me at (phone number).

(FULL NAME, RANK), USAF

(Duty Title)

1st Ind, (Violating Unit/CC)

MEMORANDUM FOR (Base COMSEC)

I have reviewed the results of the inquiry (or investigation) into COMSEC incident (Case Number) and (concur/do not concur) with the findings. I have taken the following actions as a result: (list changes implemented, additional training, etc.)

(***NOTE***: Do not include disciplinary action taken against individuals responsible for incident occurrence in this report. However, if an individual is removed from a COMSEC position (e.g., CRO) or if removal from the Cryptographic Access Program is recommended, please state so here.)

Attachment 13

COMSEC INCIDENT EVALUATION GUIDE

A13.1. Guidelines for Evaluating Communications Security Incidents .

A13.1.1. COMSEC incident evaluation and compromise recovery are two separate, distinct actions. Take compromise recovery actions as soon as possible according to AFI 33-215. Evaluation is an administrative adjudication accomplished according to the time limits listed in **a13.2.**, and not excessively influenced by any recovery actions already taken. For example, if a controlling authority initiated precautionary supersession based on an initial report, and subsequent reports presented mitigating circumstances, the evaluating authority is not required to evaluate the incident as a compromise. Conversely, a controlling authority is not required to initiate precautionary supersession when an incident is evaluated as "compromise" or "compromise cannot be ruled out," if in the evaluating authority's opinion, supersession is not warranted or is not feasible.

A13.1.2. When evaluating incidents, consider the information stated in the report, the cryptosystem security characteristics, and the effect on the cryptosystem involved. Evaluate COMSEC incidents by using one of the following terms:

A13.1.2.1. Compromise. The material was irretrievably lost or available information clearly proves that the material was made available to an unauthorized person.

A13.1.2.2. Compromise Cannot Be Ruled Out. Available information indicates that the material could have been made available to an unauthorized person, but there was no clear proof that it was made available.

A13.1.2.3. No Compromise. Available information clearly proves that the material was not made available to an unauthorized individual.

A13.1.3. COMSEC incident evaluation is often a subjective process, even when the controlling authority has all pertinent facts. While it is not possible to discuss in this publication all possible types of COMSEC incidents that controlling authorities need to assess, the following guidelines are provided for consistency in assessing commonly encountered types. Complete guidelines for evaluating incidents involving JCS PCM are contained in CJCSI 3260.01.

A13.1.3.1. Lost keying material, including keying material believed destroyed without documentation, and material temporarily out of control (i.e., was believed lost but later recovered under circumstances where continuous secure handling was not assured or was found in an unauthorized location) is evaluated as "compromise."

A13.1.3.2. Unauthorized access to keying material is evaluated as "compromise." Access exists when an individual has the capability and opportunity to gain detailed knowledge of, or to alter information or material. An individual does not have access if that individual is under escort or under the observation of a person authorized access, or if physical controls prevent detailed knowledge or altering of information or material.

A13.1.3.3. Unauthorized absences of personnel with access to keying material are evaluated as "compromise cannot be ruled out" unless there is evidence of theft, loss of keying material, or defection. However, when an individual with prior access to keying material is officially reported by the commander as an unauthorized absentee, an immediate inventory is made of all material

that individual had access to. If there is evidence of theft or loss of keying material, or defection of personnel, the controlling authority considers the material compromised and initiates emergency supersession.

A13.2. Time Limits for Evaluating Communications Security Incidents .

A13.2.1. Evaluate COMSEC incident reports within the time limits specified below. Time limits begin upon receipt of the initial or amplifying report if the initial report does not contain sufficient information to make an evaluation. The evaluating authority must solicit any information required to make an evaluation.

A13.2.2. Evaluate initial reports of the following incidents or respond within 24 hours:

A13.2.2.1. Currently effective keying material or keying material scheduled to become effective within 15 days.

A13.2.2.2. Defection; espionage; foreign cognizant agent activity; clandestine exploitation, tampering, penetration, or sabotage; or unauthorized copying, reproduction, or photography.

A13.2.3. Evaluate initial reports of the following incidents or respond within 48 hours:

A13.2.3.1. Future keying material scheduled to become effective beyond the next 15 days.

A13.2.3.2. Superseded, reserve, or contingency keying material.

A13.2.4. Evaluate initial reports of COMSEC incidents not covered above or respond within 5 duty days.

Attachment 14

IC 99-1 TO AFI 33-212, REPORTING COMSEC DEVIATIONS

26 JULY 1999

SUMMARY OF REVISIONS

This change incorporates IC 99-1 (Attachment 14). It corrects the National Security Agency (NSA) COMSEC Incident Evaluation Branch address from (DIRNSA/1413) to (DIRNSA/I413). See the last attachment of this publication, IC 99-1, for the complete IC. A bar (|) indicates revision from the previous edition.

2.1. National Security Agency (NSA) COMSEC Incident Evaluation Branch (DIRNSA/I413):

Table 1. Addressing COMSEC Material Receipt Discrepancy Reports.

If the Package Shipper is:	Send Action Message to:	Send Information Copy to:
USNDA	DIRNSA FT GEO G MEADE MD// Y13//	HQ AFCA SCOTT AFB IL//GCIS// HDIRNSA FT GEO G MEADE MD// I413// HQ CPSG SAN ANTONIO TX// ZSKM// CONTROLLING AUTHORITY(IES) MAJCOM IA OFFICE
TOBYHANNA	CDR TYAD TOBYHANNA PA// CA5B1099//	SAME AS USNDA
HQ CPSG/ CA616600	HQ CPSG SAN ANTONIO TX// CA616600//	SAME AS USNDA
HQ CPSG/ZJY	HQ CPSG SAN ANTONIO TX//ZJY//	SAME AS USNDA

4. Production Errors, Defective Keying Material, and Damaged Protective Technology. The COMSEC manager inspects all incoming material for possible production errors, defective-keying material, or damaged protective technology. If an error or anomaly is detected by the CRO (after the material was issued by the COMSEC account), the CRO should notify the unit commander and immediately return COMSEC material that is unusable and is suspected to stem from a production problem to the COMSEC account. The COMSEC account sends a message (see Attachment 3) to DIRNSA/Y265, info HQ AFCA/GCIS, DIRNSA/I413, HQ CPSG/ZSKM, Controlling Authority, and MAJCOM Information Assurance (IA) Office, explaining the circumstances of the defective material and requesting disposition instructions.

Table 3. Reporting a Practice Dangerous to Security.

RULE	If the PDS Involves:	The COMSEC Manager:
1	**A**. Premature or out of sequence use of keying material without the approval of the controlling authority (as long as the material was not reused). **B**. Inadvertent destruction of keying material. **C**. Destruction without authorization of the controlling authority as long as the destruction was properly performed and documented. **D**. Protective packaging inadvertently cut while unpacking the shipping container. **E**. Removing keying material from its protective technology before issue for use. **F**. Removing the protective technology without authorization, as long as the removal was documented and there is no evidence of espionage. **G**. Unclassified accounting legend code (ALC)-1 material. **H**. Classified ALC-4 material.	Sends a routine message: Action - Controlling Authority(ies). Information - Account's MAJCOM IA Office, Violating Unit's Commander and MAJCOM IA Office. Within 3 duty days of notification, or sooner if specified by controlling authority instructions or if circumstances warrant. Complete any actions requested by the controlling authority or MAJCOMs.
2	**A**. Failure to remove fill batteries from cryptographic equipment items prior to shipping. **B**. Loss of STU-III Seed Key or STU-III unclassified Operational Key. (***NOTE***: SUBJ/LOST STU-III SEED KEY)	Sends a routine message: Action - DIRNSA/I413. Information - Violating Unit's Commander, COMSEC Account, and MAJCOM IA Office.
3	**A**. Receiving a package with a damaged outer wrapper in which the inner wrapper is intact. **B**. Unclassified ALC-4 material. **C**. Activating the antitamper mechanism on or unexplained zeroization of COMSEC equipment when no other signs of unauthorized access or penetration are present. **D**. Failure to zeroize a common fill device within 12 hours of supersession of the effected keying material. **E**. Destruction of COMSEC material not performed within required time limits, but the material was properly stored or safeguarded. **F**. Loss of STU-III User CIK or Master CIK. **G**. Administrative/documentation errors on control and accountability records BUT 100 percent control of material maintained.	Does not report the PDS upchannel. Resolves the situation locally. Erase CIK from STU-III (Rule F only). Hold documentation for MAJCOM review during the Information Protection Assessment and Assistance Program (IPAP)(Rule G only).

Attachment 2

SAMPLE -- COMSEC RECEIPT DISCREPANCY REPORT

FM UNIT BASE//CAXXXXXX//

TO (See Table 1)

INFO HQ AFCA SCOTT AFB IL//GCIS//

DIRNSA FT GEO G MEADE MD//I413//

HQ CPSG SAN ANTONIO TX//ZSKM//

CONTROLLING AUTHORITY (IES)//

MAJCOM IA OFFICE//

U N C L A S S I F I E D

MSGID/GEN ADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC RECEIPT DISCREPANCY//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN and Commercial/E-MAIL//

RMKS/1. THIS COMSEC ACCOUNT RECEIVED A COURIER SHIPMENT CONTAINING -- COMSEC DOCUMENTS WITH A MISSING PAGE. PACKAGE (number) WAS RECEIVED ON (date) AND SHOWED NO EVIDENCE OF TAMPERING. INSIDE THE PACKAGE WAS (short title), EDITION (XX), ACCOUNTING CONTROL NUMBERS (XX-XX). WHILE PAGE CHECKING, IT WAS DISCOVERED THAT BOOK NUMBER(S) (XX and XX) WERE MISSING (list what is missing). ALL OTHER COPIES HAVE BEEN CHECKED AND HAVE THE CORRECT NUMBER OF PAGES.

2. REQUEST DISPOSITION INSTRUCTIONS BE PROVIDED.//

(Sample paragraphs identifying receipt of COMSEC documents with missing pages)

-- (number) COMSEC DOCUMENTS THAT WERE NOT IDENTIFIED ON THE ENCLOSED SF153. PACKAGE (number) WAS RECEIVED ON (date) AND SHOWED NO EVIDENCE OF TAMPERING. INSIDE THE PACKAGE WAS A SF 153 IDENTIFYING (short title), EDITION (XX), ACCOUNTING CONTROL NUMBERS (XX-XX); HOWEVER, THE PACKAGE ACTUALLY CONTAINED (short title), EDITION (XX), ACCOUNTING CONTROL NUMBERS (XX-XX).

3. THE UNLISTED COPIES HAVE BEEN ADDED AS A LINE ITEM TO OUR VOUCHER (number)//.

(Sample paragraphs identifying receipt of COMSEC material not listed on SF 153):

-- SF 153 LISTING (number) LINE ITEMS BUT ONLY (number) WERE ACTUALLY IN THE PACKAGE. PACKAGE (number) WAS RECEIVED ON (date) AND SHOWED NO EVIDENCE OF TAMPERING. INSIDE THE PACKAGE WAS A SF 153, OUTGOING VOUCHER NUMBER (number), IDENTIFYING (short titles), EDITIONS (XX), ACCOUNTING CONTROL NUMBERS (XX-XX). ALL COPIES OF (short titles) WERE RECEIVED, HOWEVER, (short title), EDITION (XX), ACCOUNTING CONTROL NUMBERS (XX-XX) WERE NOT IN THE PACKAGE.

4. THE ITEMS THAT WERE NOT IN THE PACKAGE HAVE BEEN LINED OFF OUR VOUCHER (number).//

(Sample paragraphs identifying nonreceipt of COMSEC documents listed on SF 153)

Attachment 3

SAMPLE -- COMSEC PRODUCTION ERROR/DEFECTIVE KEYING MATERIAL FORMAT

FM UNIT BASE//CAXXXXXX//

TO DIRNSA FT GEO G MEADE MD//Y265//

INFO HQ AFCA SCOTT AFB IL//GCIS//

DIRNSA FT GEO G MEADE MD//I413//

HQ CPSG SAN ANTONIO TX//ZSKM//

CONTROLLING AUTHORITIES//

MAJCOM IA OFFICE//

C O N F I D E N T I A L

MSGID/GEN ADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC MATERIAL PRODUCTION ERROR/DEFECTIVE KEYING MATERIAL//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN and Commercial/E-Mail//

RMKS/1. (U) COMSEC ACCOUNT: XXXXXX.

2. (C) MATERIAL INVOLVED: Short title, edition, accounting control numbers.

A. UNIT USING MATERIAL: (If the material has been issued to the user)

B. PERSONNEL INVOLVED:

C. CIRCUMSTANCES THAT UNCOVERED THE PROBLEM:

3. REQUEST DISPOSITION INSTRUCTIONS.

4. CLASSIFIED BY: AFMAN 33-272

DECLAS: X1//

Attachment 4

REQUIRED COMSEC DEVIATION REPORT INFORMATION

A4.9.11.5. Forward copies of each photograph or reproduction to DIRNSA/I413 and HQ AFCA/GCIS.

Attachment 5

SAMPLE -- INITIAL PHYSICAL, AIRCRAFT, OR DISASTER COMSEC INCIDENT REPORT

FM UNIT BASE//CAXXXXXX//

TO (See Table 4)

INFO (See Table 4)

HQ AFCA SCOTT AFB IL//GCIS//

VIOLATING UNIT//CC//

SUPPORTING COMSEC ACCOUNT'S MAJCOM IA OFFICE//

VIOLATING UNIT'S MAJCOM IA OFFICE//

DIRNSA FT GEORGE G MEADE MD//I413// (unless an action addressee)

C O N F I D E N T I A L

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENTÑINITIAL REPORT//

REF/A/AFI 33-212, PARA 7.3, AS APPLICABLE//

REF/B/Other applicable documents//

REF/C/Additional related correspondence and messages on incident//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN/E-MAIL//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

A. VIOLATING UNIT:

B. MAJCOM OF VIOLATING UNIT:

2. (C) MATERIAL INVOLVED. List all material involved in incident including short title, edition, accounting control number (ACN), controlling authority, classification, and accounting legend code (ALC) for each item involved.

3. PERSONNEL INVOLVED IN THE INCIDENT.

4. CIRCUMSTANCES OF INCIDENT.

5. INITIAL INCIDENT ASSESSMENT: COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

6. ADDITIONAL REPORTING REQUIRED BY AFI 33-212 (See Attachment 4).

7. CLASSIFIED BY: AFMAN 33-272

DECLASS: X1//

Attachment 6

SAMPLE -- INITIAL CRYPTOGRAPHIC COMSEC INCIDENT REPORT

FM UNIT BASE//CAXXXXXX//

TO DIRNSA FT GEORGE G MEADE MD//I413//

INFO HQ AFCA SCOTT AFB IL//GCIS//

ACTUAL CONTROLLING AUTHORITIES//

VIOLATING UNIT//CC//

SUPPORTING COMSEC ACCOUNT'S MAJCOM IA OFFICE//

VIOLATING UNIT'S MAJCOM IA OFFICE//

C O N F I D E N T I A L

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENTÑINITIAL REPORT//

REF/A/AFI 33-212, PARA 7.1//

REF/B/OTHER APPLICABLE DOCUMENTS//

REF/C/Additional related correspondence and messages on incident//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN/E-MAIL//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

A. VIOLATING UNIT:

B. MAJCOM OF VIOLATING UNIT:

2. (C) MATERIAL INVOLVED: List all material involved in incident, including short title, edition, accounting control number (ACN), controlling authority, classification, and accounting legend code (ALC) for each item involved.

3. PERSONNEL INVOLVED IN THE INCIDENT:

4. CIRCUMSTANCES OF INCIDENT:

5. INITIAL INCIDENT ASSESSMENT: COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

6. ADDITIONAL REPORTING AS REQUIRED BY AFI 33-212. (See Attachment 4.)

7. CLASSIFIED BY: AFMAN 33-272

DECLASS: X1//

Attachment 7

SAMPLE -- INITIAL PERSONNEL COMSEC INCIDENT REPORT

FM UNIT BASE//CAXXXXXX//

TO DIRNSA FT GEORGE G MEADE MD//I413//

INFO HQ AFCA SCOTT AFB IL//GCIS//

VIOLATING UNIT//CC//

SUPPORTING ACCOUNT'S MAJCOM IA OFFICE//

VIOLATING UNIT'S MAJCOM IA OFFICE//

CONTROLLING AUTHORITIES//

C O N F I D E N T I A L

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT Ð INITIAL REPORT//

REF/A/AFI 33-212, PARA 7.2

REF/B/Additional related correspondence and messages on incident.//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN/E-MAIL//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

2. (C) MATERIAL INVOLVED: List all material involved in incident including short title, edition, accounting control number (ACN), controlling authority, classification, and accounting legend code (ALC) for each item involved.

3. PERSONNEL INVOLVED IN THE INCIDENT:

4. CIRCUMSTANCES OF INCIDENT:

5. INITIAL INCIDENT ASSESSMENT: COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

6. ADDITIONAL REPORTING REQUIRED BY AFI 33-212. (See Attachment 4.)

7. CLASSIFIED BY: AFMAN 33-272

DECLAS: X1//

Attachment 15

IC 2000-1 TO AFI 33-212, REPORTING COMSEC DEVIATIONS

15 DECEMBER 2000

SUMMARY OF REVISIONS

This change updates IC 99-1 (Attachment 14). It corrects required reporting procedures for lost STU-III Seed Keys according to NSTISSI 4003. It deletes reference to STU-III Seed Key in Table 2, and deletes reference to STU-III Seed Key in Table 3, Rule 2B. See the last attachment of this publication, IC 2000-1, for the complete IC. A bar (|) indicates revision from the previous edition.

Table 2. Incident or PDS (Quick Look).

Material Involved Is:	**Accounting Legend Code (ALC) Is:**	**Report Under:**
Classified	1 or 6	COMSEC or Codebook Incident
Classified Operational STU-III Key	1	COMSEC Incident
STU-III Terminal Only-Unkeyed (1)	CCI	COMSEC Incident
STU-III with CIK/Key Inserted (2)	1	COMSEC Incident
Classified	4 or 7	PDS
Unclassified	1 or 6	PDS
Unclassified	4 or 7	PDS (Local Report Only)
STU-III User CIK or Master CIK		PDS (Local Report Only)
NOTES: (1) Generally involves the suspected loss, theft, or tampering of a STU-III terminal. (2) Generally involves a Secure Telephone Unit (STU)-III left unattended with the key/ crypto-ignition key (CIK) inserted.		

Table 3. Reporting a Practice Dangerous to Security.

RULE	**If the PDS Involves:**	**The COMSEC Manager:**

1	**A**. Premature or out of sequence use of keying material without the approval of the controlling authority (as long as the material was not reused). **B**. Inadvertent destruction of keying material. **C**. Destruction without authorization of the controlling authority as long as the destruction was properly performed and documented. **D**. Protective packaging inadvertently cut while unpacking the shipping container. **E**. Removing keying material from its protective technology before issue for use. **F**. Removing the protective technology without authorization, as long as the removal was documented and there is no evidence of espionage. **G**. Unclassified accounting legend code (ALC)-1 material. **H**. Classified ALC-4 material.	Sends a routine message:*Action* - Controlling Authority(ies).*Information* - Account's MAJCOM IA Office, Violating Unit's Commander and MAJCOM IA Office. Within 3 duty days of notification, or sooner if specified by controlling authority instructions or if circumstances warrant. Complete any actions requested by the controlling authority or MAJCOMs.
2	**A**. Failure to remove fill batteries from cryptographic equipment items prior to shipping.	Sends a routine message:*Action* - DIRNSA/I413.*Information* - Violating Unit's Commander, COMSEC Account, and MAJCOM IA Office.
3	**A**. Receiving a package with a damaged outer wrapper in which the inner wrapper is intact. **B**. Unclassified ALC-4 material. **C**. Activating the antitamper mechanism on or unexplained zeroization of COMSEC equipment when no other signs of unauthorized access or penetration are present. **D**. Failure to zeroize a common fill device within 12 hours of supersession of the effected keying material. **E**. Destruction of COMSEC material not performed within required time limits, but the material was properly stored or safeguarded. **F**. Loss of STU-III User CIK or Master CIK. **G**. Administrative/documentation errors on control and accountability records BUT 100 percent control of material maintained.	Does not report the PDS upchannel. Resolves the situation locally. Erase CIK from STU-III (Rule F only). Hold documentation for MAJCOM review during the Information Protection Assessment and Assistance Program (IPAP)(Rule G only).

8.3. Physical Incidents. Physical incidents include loss of control (material out of COMSEC channels but control is later restored), lost material, lost STU-III Seed Key, theft, capture, recovery by salvage, tampering, unauthorized viewing and access, photographing, or copying that can potentially jeopardize COMSEC material. Report physical incidents by message (see Attachment 4 and Attachment 5). Examples include: