BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-107, VOLUME 3

1 JUNE 1998

Communications and Information

STRATEGIC AUTOMATED COMMAND CONTROL SYSTEM-DATA TRANSMISSION SUBSYSTEM (SACCS-DTS) NETWORK SECURITY PLAN

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ AFSPC/SCMB (Mr. Schwiesow)

Certified by: HQ USAF/SCXX (Lt Col Webb)

Pages: 15

Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*. It prescribes detailed instructions for securely processing classified information on the SACCS-DTS Network. Compliance with all requirements of the network security plan is a condition of network accreditation. You must comply with all requirements in **Chapter 2**, **Section 2C**, and **Chapter 3**, **Section 2C** when beginning or ending classified processing. This instruction applies to all users of the SACCS-DTS network, either through direct input or interface systems. Failure to observe the prohibitions and mandatory provisions of this instruction in paragraphs **2.9.** through **2.12.**, and paragraphs **3.9.** through **3.15.** by military personnel is a violation of Article 92 (*Failure to Obey Order or Regulation*), Uniform Code of Military Justice (UCMJ). Violations of these paragraphs by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. When major commands (MAJCOM) and field operating agencies (FOA) supplement this instruction, they should provide a copy to Headquarters Air Force Space Command (HQ AFSPC/SCMB), 150 Vandenberg Street, STE 1105, Peterson AFB CO 80914-4730, with a copy to Headquarters Air Force Communications Agency (HQ AFCA/XPXP), 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5233. Refer recommended changes and conflicts between this and other publications to HQ AFCA/XPXP using AF Form 847, **Recommendation for Change of Publication,** with an information copy to HQ AFSPC/SCMB. See **Attachment 1** for a glossary of references and supporting information.

Chapter 1

APPLICABILITY AND REFERENCES

1.1. Applicability. This instruction applies to all organizations and units that use, interface, or support the SACCS-DTS Network. The SACCS-DTS Network provides commanders with information required for decisions affecting the control and direction of operational forces. In addition, it provides subscribers with direct interface to the Automatic Digital Network; Air Force Weather Agency (AFWA), Command Center Processing and Display System, Air Force Satellite Communications System, and Survivable Low Frequency Communications System. SACCS is two major subsystems electronically interconnected; the DTS and the Data Processing Subsystem.

1.2. Authority and Organization. AFSPC, as the lead command of the SACCS-DTS Network, is responsible for operation and maintenance of the network. HQ AFSPC provides operational direction and hardware support. Air Combat Command (ACC), 55th Computer Systems Squadron (CSS), and 55th Wing, provide operational and software support.

1.3. References, Abbreviations, and Acronyms. See **Attachment 1**.

1.4. Document Responsibility. The 55 CSS/CC is the office of collateral responsibility for this instruction. Address questions to:

55th Computer Systems Squadron

ATTN: SACCS-DTS CSSO (SCGS)

201 Lincoln Highway, Suite 206

Offutt AFB NE 68113-2040

Chapter 2

STRATEGIC AUTOMATED COMMAND CONTROL SYSTEM-DATA TRANSMISSION SUBSYSTEM OPERATIONAL NETWORK

Section 2A—Responsibilities.

2.1. Classified and Unclassified Processing. The SACCS-DTS Network is an accredited B3 multi-level secure telecommunications system. Primary responsibility for processing data at different security classification levels rests in the network software. System users and operators do not have active involvement in separating classified and unclassified processing.

2.2. Computer Systems Manager. The 55CSS/CC is responsible for all security requirements according to Air Force Instruction (AFI) 31-209, *The Air Force Resource Protection Program*; Department of Defense (DoD) Regulation 5200.1-R, *Information Security Program*, January 1997; AFI 31-401, *Managing the Information Security Program*; AFPD 31-5, *Personnel Security Program Policy*; AFI 31-501, *Personnel Security Program Management*; and AFI 31-101, Volume 1 (AFI 31-101V1), *The Air Force Physical Security Program*.

2.2.1. The 55CSS/CC appoints, in writing, a SACCS-DTS computer systems security officer (CSSO) for the SACCS-DTS Network. The commander will provide a copy of the appointment letter to the designated approval authority (DAA) at HQ AFSPC.

2.3. Strategic Automated Command Control System-Data Transmission Sub system Computer Systems Security Officer. The SACCS-DTS CSSO is responsible for development, implementation, and direction of the Network Security Program. The security program includes day-to-day operations, configuration management (CM), and systems integration. The SACCS-DTS CSSO will:

2.3.1. Ensure the following computer security positions are filled:

2.3.1.1. CSSO for each SACCS-DTS functional area (FA) with accountable processors (subnet communications processor [SCP] and base communications processor [BCP]).

2.3.1.2. Terminal area security officer (TASO) for each SACCS-DTS FA with non-accountable processors.

2.3.1.3. CSSO for each external system interfacing with the SACCS-DTS Network.

2.3.1.4. CSSO for the Computer Program Maintenance Facility (CPMF).

2.3.1.5. TASO for each CPMF remote terminal area.

2.3.2. Approve network security procedures to include local procedures established by CSSOs, and TASOs within the SACCS-DTS Network.

2.3.3. Monitor activities on the network, using audit capabilities, to verify compliance with established security procedures.

2.3.4. Perform initial evaluation of security problems. If necessary, recommend denial of access to the network (including disconnection of the interface systems) while problems are being evaluated. Report problems and findings to the network manager.

2.3.5. Review changes or modifications to network configuration or components to verify the integrity of network security features.

2.3.6. Review external interface accreditations and coordinate with the system's CSSO to ensure network security integrity while connected to the SACCS-DTS network.

2.3.7. Document and report any identified network deficiencies to the computer systems manager.

2.3.8. Chair the SACCS-DTS Security Working Group. Coordinate certification and accreditation activities.

2.4. Computer Systems Security Officer. The communications commander of units operating SCPs or BCPs will appoint a CSSO for their FA. The officer in charge (OIC) of organizations operating other SACCS-DTS FAs will appoint a TASO for their terminal. The OIC or system manager of external interface systems will appoint a CSSO for coordination with the SACCS-DTS CSSO. The CSSO or TASO will:

2.4.1. Ensure all classified processing meets all requirements, including Air Force Systems Security Instruction (AFSSI) 5102, *The Computer Security (COMPUSEC) for Operational Systems*; AFI 33-101, *Communications and Information Management Guidance and Responsibilities*, AFI 33-107V2, *Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS) Network Security Program*; and these guidelines.

2.4.2. Make sure each user learns and understands the security plan, and effectively implements proper procedures when processing classified data on the system. The CSSO/TASO will coordinate and document required computer security training with the unit security awareness, training, and education (SATE) manager.

2.4.3. Make sure proper markings are on all classified products and materials (e.g., diskettes, tapes, and printed copies).

2.4.4. Conduct spot checks of security procedures, materials, and computer output for effectiveness and integrity.

2.4.5. Network Security Notifications. Make these notifications to the Network Quality Control Center (NQCC) to inform the SACCS DTS CSSO and the computer security manager of possible security incidents. They are in addition to the "reports" that are required by other DoD regulations and AFIs. Report all suspected or actual incidents according to DoD 5200.1-R, AFI 31-401, and AFSSI 5102.

2.4.5.1. Report any system security violation messages (messages that exceed the recipient's authorized operating level of classification).

2.4.5.2. Report actual or suspected computer security incidents, including virus infections.

2.4.5.3. Report any system, environmental, or procedural changes affecting the system. Include an assessment of security impact and system operation.

2.4.5.4. As a minimum, forward hard copies of the notification to the following:

2.4.5.4.1. SACCS-DTS CSSO. Contact the SACCS-DTS CSSO through the NQCC.

2.4.5.4.2. FA CSSO.

2.4.5.4.3. Unit OIC or noncommissioned officer in charge.

2.5. System Users. The system users will:

2.5.1. Obtain initial and recurring computer security training.

2.5.2. Conduct all processing according to Air Force requirements and this instruction.

2.5.3. Report all suspected or actual information security violations per DoD 5200.1-R and AFI 31-401. Report actual or suspected computer security incidents, including virus infections, to the TASO/CSSO. Report any system, environmental, or procedural changes affecting the system to the TASO/CSSO.

Section 2B—System Controls.

2.6. Physical Security. Secure all systems, software, data, and media whenever the system is not in use. Protect the system according to AFI 31-209; DoD 5200.1-R, AFI 31-401, and AFI 31-101. The following is the minimum physical security requirements for facilities housing SACCS-DTS FAs:

2.6.1. Authorize open storage for each area containing a SACCS-DTS node at the classification level of the processor. (The security level is determined by the unit's mission requirements.)

2.6.2. Secure each accountable SACCS-DTS processor (SCP or BCP) in a restricted area.

2.6.3. Secure each non-accountable SACCS-DTS node as a controlled area. (**NOTE:** Accountability requires that the node be capable of electronically inventorying messages processed. Only SCPs and BCPs are accountable.)

2.7. Data Security.

2.7.1. Inventory, control, and account for all removable media at the classification level of the SACCS-DTS processor according to DoD 5200.1-R. Assign a unique 4-digit identification number to each diskette or tape.

2.7.2. Prominently label all media with the appropriate Standard Form (SF) 700 series standard media label according to DoD 5200.1-R, AFI 31-401, and AFSSI 5102. Label SACCS-DTS 8-inch diskettes in accordance with AFI 33-107V2, Attachment 2. Label systems containing non-volatile, non-removable storage with the appropriate SF 700 series label. Mark hard copy output according to DoD 5200.1-R and AFI 31-401.

2.7.3. Control all media at the highest level of classified processed until the media is purged and classification administratively removed per AFSSI 5020, *Remanance Security*.

2.7.4. Do not introduce any unauthorized media into the SACCS-DTS FA. Use only media supplied by the SACCS Operations Library (55CSS/SCJ).

2.8. Procedural Security.

2.8.1. Processing on the SACCS-DTS Network is exclusively at the multi-level secure mode. Do not use the SACCS-DTS Network for any unofficial communications.

2.8.2. Restrict systems access to authorized personnel with a proper clearance and valid need-to-know for the highest level the processor is authorized to operate at within the system. Implement procedures to verify access permissions before access to the network terminal.

2.8.3. Continuously staff the immediate area of the SACCS-DTS terminal while the system is in operation. Implement and comply with unmanned terminal procedures (see AFI 33-107V2, Attachment 3) for any SACCS-DTS terminal that is unattended.

2.8.4. Do not move or rearrange the system in any manner without consulting the SACCS-DTS CSSO, automated data processing (ADP) equipment custodian (EC), and the wing information protection (IP) office.

2.8.5. Destroy system components or magnetic media according to requirements of AFSSI 5020.

2.8.6. Ensure a current emission security (EMSEC) evaluation for SACCS-DTS FA is on file before processing classified information.

Section 2C—System Operations.

2.9. Classified Processing. Systems processing procedures on a SACCS-DTS FA will include:

2.9.1. Procedures to keep uncleared or unauthorized personnel out of the immediate vicinity of the system. Permit only properly cleared personnel, with established need-to-know, access to the system and classified data.

2.9.2. Procedures to ensure all magnetic media and processing output are marked, controlled, and secured at the classification level of the processor. If systems tests are being performed and test data is used, protect all output as TOP SECRET/SINGLE INTEGRATED OPERATIONAL PLAN-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) until review by appropriate agencies determines it to be of lower classification or unclassified.

2.9.3. Actions and notifications if there are processing problems, possible compromise, or other situations involving security or operational aspects of the system.

2.9.4. Procedures to ensure that the system is always attended while processing classified information.

2.10. Purge and Take-Down Procedures. Conduct purge and take-down procedures in accordance with United States Strategic Command (USSTRATCOM) Directive 501-14, *Force Management Information System (FMIS) Reporting Procedures*, and local guidance whenever there is a need to clear the SACCS-DTS FA for maintenance or other actions. These procedures will include:

2.10.1. Notification of parent SCP/BCP and NQCC of taking the SACCS-DTS FA off-line.

2.10.2. Actions to purge and take-down the FA from classified (RED*)* to unclassified (BLACK*)* mode immediately upon the completion of classified processing.

2.10.3. Restricted to personnel permitted to configure FA systems from classified (RED) to unclassified (BLACK) processing mode.

2.10.4. Verification of correct unclassified system configuration by certified personnel before releasing the system to maintenance personnel. Configuration will verify that all classified media and materials are removed from the system before boot-up in the unclassified mode.

2.11. Restoral Procedures. Implement restoral procedures once the SACCS-DTS FA is ready to return to operation. Restoral procedures will include:

2.11.1. Actions to restore the FA from unclassified (BLACK) to classified (RED) mode once maintenance or other system actions are completed.

2.11.2. Restriction to personnel permitted to configure FA systems from unclassified (BLACK) to classified (RED) processing mode.

2.11.3. Verification of correct classified system configuration by certified personnel before returning the system to operation. Configuration will verify that all unclassified media and materials are clear of the system before boot-up in the classified mode.

2.11.4. Notification of parent SCP/BCP and NQCC of return of the SACCS-DTS FA to operational status.

2.12. System Malfunction During Classified Processing. Implement procedures to handle system malfunction during classified processing. These procedures must include:

2.12.1. Restriction to personnel authorized to trouble-shoot system malfunctions.

2.12.2. Recovery procedures to prevent or minimize loss of data, applications programs, and operating systems.

2.12.3. Actions and notifications for any processor malfunction or failure while in classified mode.

2.13. The procedures and requirements of this section are mandatory. Failure to comply with the requirements of Chapter 2, Section 2C, paragraphs 2.9 through 2.12 is a violation of Article 92 of the UCMJ.

Chapter 3

COMPUTER PROGRAM MAINTENANCE FACILITY

Section 3A—Responsibilities.

3.1. Classified and Unclassified Processing.

3.1.1. The Dump Analysis Computer. The Dump Analysis Computer is for classified processing only. Do not process unclassified materials on the Dump Analysis Computer.

3.1.2. The Software Test Facility (STF) can process unclassified materials and classified materials up to and including TOP SECRET/SIOP-ESI. Implement group periods processing for all classified processing on the STF. Handle all classified processing according to the requirements and procedures set out in this security plan.

3.1.2.1. Whenever using the STF for classified operations, protect the system and all diskettes introduced into the system at the TOP SECRET level.

3.1.3. The host handles unclassified processing. Do not process classified materials on the host.

3.2. Computer Systems Manager (Computer Program Maintenance Facility). The 55CSS/CC is responsible for ensuring all security requirements are met according to AFI 31-209, DoD 5200.1-R, AFI 31-401, AFPD 31-5, AFI 31-501, and AFI 31-101.

3.2.1. The 55CSS/CCappoints, in writing, a CSSO and alternate for all CPMF systems. Provide a copy of the appointment letter to the SACCS-DTS CSSO. One CSSO may cover multiple systems as long as they can maintain regular contact with each system and users during normal course of duties.

3.3. Computer Systems Security Officer. The CSSO will:

3.3.1. Ensure all classified processing meets all requirements, including AFSSI 5102, AFI 33-107V2, and these guidelines.

3.3.2. Ensure each user learns and understands the security plan, and effectively implements proper procedures when processing classified data on the system. The CSSO will coordinate and document required computer security training with the unit SATE manager.

3.3.3. Ensure proper markings on all classified products and materials (e.g., diskettes, tapes, and printed copies).

3.3.4. Conduct spot checks of security procedures, materials, and computer output for effectiveness and integrity.

3.3.5. Report all suspected or actual information security violations according to DoD 5200.1-R and AFI 31-401. Report actual or suspected computer security incidents, including virus infections, to the SACCS-DTS CSSO. Report any system, environmental, or procedural changes affecting the system to the SACCS-DTS CSSO. Include an assessment of security impact and system operation in the report. The SACCS-DTS CSSO will forward the report to the DAA.

3.4. Terminal Area Security Officer.

3.4.1. Each workcenter with remote terminals connected to the CPMF system will appoint a TASO for their area. Provide a copy of the appointment letter to the SACCS-DTS CSSO through the CSSO. Do not assign TASOs for terminals located within the SACCS operations facility.

3.4.2. The TASO serves as the CSSO's representative in the workcenter. The CSSO will assign duties and responsibilities to the TASO as necessary. Forward all documentation and reports to the CSSO for filing.

3.5. System Users. The system users will:

3.5.1. Obtain initial and recurring computer security training.

3.5.2. Conduct all processing according to Air Force requirements and this plan.

3.5.3. Report all suspected or actual information security violations per DoD 5200.1-R and AFI 31-401. Report actual or suspected computer security incidents, including virus infections, to the TASO/CSSO. Report any system, environmental, or procedural changes affecting the system to the TASO/CSSO and to the Commander, SACCS-DTS Operations Flight, as soon as possible.

Section 3B—System Controls.

3.6. Physical Security. Secure all systems, software, data, and media whenever the system is not in use. Protect the system according to AFI 31-209, DoD 5200.1-R, AFI 31-401, and AFI 31-101.

3.6.1. Comply with all entry control, escort, and other restricted area procedures whenever working within the SACCS Operations Facility (Building 501, Room U116/U120).

3.6.2. During periods of classified processing, restrict systems access to authorized personnel with a proper clearance and valid need-to-know for the highest level currently on the system.

3.6.3. Continuously staff the immediate area of the system while the system is in classified configuration. Each user will contact the on-duty shift supervisor to ensure the STF is ready for classified (RED) processing before starting classified operations. The user will notify the on-duty shift supervisor when finished with classified operations, so the STF can be purged and re-configured to unclassified (BLACK) status. Purge procedures will include disconnecting all patches, removing all media, and performing a system initial program load.

3.6.4. Secure all systems and facilities when not in use. Host terminal users will log-off their terminal and shut the terminal off at the completion of processing. TASOs will conduct periodic checks to ensure compliance. End-of-day security checks will verify all host terminals and peripherals are off.

3.7. Data Security.

3.7.1. Inventory, control, and account for all removable media containing classified data. Assign a unique 4-digit identification number to each diskette or tape.

3.7.2. Prominently label all media with the appropriate SF 700 series standard media label according to DoD 5200.1-R, AFI 31-401, and AFSSI 5102. Label SACCS-DTS 8-inch diskettes IAW AFI 33-107V2, Attachment 2. Label systems containing non-volatile, non-removable storage with the appropriate SF 700 series label. Mark hard copy output according to DoD 5200.1-R and AFI 31-401.

3.7.3. Control all media at the highest level of classified processed until purged and classification administratively removed per AFSSI 5020.

3.7.4. Accomplish backup files for host on a daily, weekly, and monthly basis. Label, inventory, and control backup media as UNCLASSIFIED/FOR OFFICIAL USE ONLY (FOUO).

3.8. Procedural Security.

3.8.1. The host computer is a developmental system in support of the operational on-line system, personnel requiring access to the host system must have at least a SECRET clearance. The SACCS-DTS CSSO will verify personnel security clearance before allowing the issuance of user identification (userID) and log-on password. The SACCS-DTS system administrator will maintain records of all user access authorizations.

3.8.2. Processing on the host is exclusively on the UNCLASSIFIED/FOUO level. Do not conduct any classified processing on host.

3.8.3. Processing on the Dump Analysis Computer is exclusively on the classified level. Do not permit any unclassified processing on the Dump Analysis Computer.

3.8.4. Implement group periods for processing different levels of classified and unclassified processing on the STF. Maintain a separate set of operating systems and applications software media for a classified processing and unclassified processing. Purge the system in accordance withUSSTRATCOM Directive 501-14, local operating procedures, and AFSSI 5020 whenever ending classified processing.

3.8.5. Whenever using the STF for classified operations, protect the system and all diskettes introduced into the system at the TOP SECRET level.

3.8.6. Ensure a current EMSEC evaluation is on file for the Dump Analysis Computer and the STF before processing classified information.

3.8.7. Do not move or rearrange the system in any manner without consulting the SACCS-DTS CSSO, ADP EC, and the wing IP office.

3.8.8. Destroy system components or magnetic media according to requirements of AFSSI 5020.

Section 3C—System Operations.

3.9. Host Set-Up Procedures.

3.9.1. SACCS-DTS operations personnel will handle physical configuration of the host system accordance to mission requirements. This includes tape back-ups, reloading of archive files and tapes, and maintenance actions.

3.9.2. SACCS-DTS CM personnel maintain master libraries on the host computer. Implement strict control over access to the master level libraries.

3.9.3. SACCS-DTS CM system administrator will maintain control over system access through the assignment of virtual machine userIDs and passwords. Control userIDs and passwords as UNCLASSIFIED/FOUO.

3.10. Software Test Facility Set-Up Procedures. Implement procedures for positive configuration of the STF for any classified processing. Procedures will include:

3.10.1. Specific scheduling of periods for classified processing and unclassified processing.

3.10.2. Restricting to personnel permitted to configure STF systems from unclassified (BLACK) to classified (RED) mode processing.

3.10.3. Verification of correct system configuration for classified processing by certified operations personnel before processing start. Configuration will ensure all unclassified media and materials are removed from the system before boot-up in the classified mode.

3.10.4. Verification of classification and system configuration before releasing software to programming or testing personnel.

3.11. Classified Processing. While operating the STF in classified (RED) mode, or while conducting dump analysis, systems procedures will include:

3.11.1. Procedures to keep uncleared or unauthorized personnel out of the immediate vicinity of the system. Permit only properly cleared personnel with established need-to-know to have access to the system and classified data.

3.11.2. Procedures to ensure all magnetic media and processing output are marked, controlled, and secured as TOP SECRET/SIOP material. Protect all output as TOP SECRET/SIOP until review by appropriate agencies determines it to be of lower classification or unclassified.

3.11.3. Actions and notifications to be completed if there is processing problems, possible compromise, or other situations involving security or operational aspects of the system.

3.11.4. Procedures to ensure that the system is continuously attended whenever in a classified (RED) configuration.

3.12. Purge and Take-Down Procedures. Whenever classified processing on the STF is completed initiate purge and take-down procedures in accordance with USSTRATCOM Directive 501-14 and local procedures. These procedures will include:

3.12.1. Procedures to purge and take-down the STF from classified (RED*)* to unclassified (BLACK*)* mode immediately upon the completion of classified processing.

3.12.2. Restriction to personnel permitted to configure STF systems from classified (RED) to unclassified (BLACK) processing mode.

3.12.3. Verification of correct system configuration for unclassified processing by certified operations personnel before processing starts. Configuration will ensure all classified media, materials, and accessories are removed from the system before boot-up in the unclassified mode.

3.12.4. Verification of classification and system configuration before releasing software to programming or testing personnel.

3.13. Restoral Procedures. Implement restoral procedures once a CPMF system is ready to return to operation. Restoral procedures will include:

3.13.1. Actions to restore the system from unclassified (BLACK) to classified (RED) mode once maintenance or other system actions are completed.

3.13.2. Restriction to personnel permitted to configure systems from unclassified (BLACK) to classified (RED) processing mode.

3.13.3. Verification of correct classified system configuration by certified personnel prior to returning the system to operation. Configuration will verify that all unclassified media and materials are removed from the system before boot-up in the classified mode.

3.13.4. Notification of functional manager and appropriate offices of return of the CPMF system to operational status.

3.14. System Malfunction During Classified Processing. Implement procedures to handle systems malfunction during classified processing. These procedures must include:

3.14.1. Restriction to personnel authorized to trouble-shoot system malfunctions.

3.14.2. Recovery procedures to prevent or minimize loss of data, applications programs, and operating systems.

3.14.3. Actions and notifications to be completed if there is processor malfunction or failure while in classified mode.

3.15. Remote Processing. Whenever processing on a remote terminal to the host, all personnel will comply with the following procedures:

3.15.1. Use of remote terminals (any terminal outside of the SACCS operations facility) is restricted to regular duty hours (Monday through Friday, 0600 to 1700). Conduct any processing on the host after normal duty hours in the SACCS operations facility. If this is not feasible, coordinate with the SACCS operations facility at least 24 hours in advance. Short-notice taskings (less than 24 hours) require the approval of applicable flight commander or element chief.

3.15.2. Use of script files in the IRMAWIN program for automated log-on is strictly forbidden. The use of script file or any macro to automate log-on makes it vulnerable to compromise.

3.15.3. Do not leave open, logged-on terminals unattended at any time. For IBM Terminals, the user must log off and turn off the terminal before leaving. For PCs, the user must log off the host and close the IRMAWIN program before leaving the system. You can use a password-locked screen saver on PCs, but only for short breaks. Activate the screen saver before leaving, do not use the timer activation.

3.16. The procedures and requirements of this section are mandatory. Failure to comply with the requirements of Chapter 3, Section 3C, paragraphs 3.9 through 3.15 is a violation of Article 92 of the UCMJ.

Chapter 4

SYSTEMS MAINTENANCE

4.1. Network Maintenance Actions. Implement procedures for maintenance actions on the SACCS-DTS Network. Procedures must include:

4.1.1. Specific instructions on the level of troubleshooting and fault isolation permitted to each level of network user: local operator, network operations personnel, SACCS maintenance personnel.

4.1.2. Purging and taking down the system to the fullest extent possible prior to performing maintenance. Include measures to protect classified data and programs on the system.

4.1.3. Limiting maintenance actions to personnel with appropriate clearances, as necessary.

4.1.4. Notifications to complete if maintenance of the system is necessary, to include as a minimum:

4.1.4.1. NQCC.

4.1.4.2. SACCS-DTS CSSO/CSSO/TASO, as applicable

4.1.4.3. Wing EMSEC manager. (The SACCS-DTS CSSO will normally make this notification.)

4.1.4.4. OIC, user organization.

4.1.5. Restricting issue of programs or data for maintenance testing to unclassified materials.

4.2. Computer Program Maintenance Facility Maintenance Actions. Implement procedures for maintenance of CPMF systems, to include:

4.2.1. Specific instructions on the level of troubleshooting and fault isolation permitted to each level of systems user: programmer/tester, operations personnel, SACCS maintenance personnel.

4.2.2. Purging and taking down the system to the fullest extent possible before performing maintenance. Procedures must also include measures to protect classified data and programs on the system.

4.2.3. Limiting maintenance actions to personnel with appropriate clearances, as necessary.

4.2.4. Notifications to complete if maintenance of the system is necessary, to include as a minimum:

4.2.4.1. CSSO.

4.2.4.2. Wing EMSEC manager. (This notification will normally be made by the CSSO.)

4.2.4.3. Commander or superintendent, SACCS operations flight.

4.2.5. Restricting issue of programs or data for maintenance testing to unclassified materials.

WILLIAM J.DONAHUE, Lt Gen, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 31-5, *Personnel Security Program Policy*

AFPD 33-2, *Information Management*

AFI 31-101V1, *The Air Force Physical Security Program*

AFI 31-209, *The Air Force Resource Protection Program*

AFI 31-401, *Managing the Information Security Program*

AFI 31-501, *Personnel Security Program Management*

AFI 33-101, *Communications and Information Management Guidance and Responsibilities*

AFI 33-107V2, *Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS) Network Security Program*

AFSSI 5020, *Remanance Security*

AFSSI 5102, *The Computer Security (COMPUSEC) for Operational Systems*

Article 92 (*Failure to Obey Order or Regulation*), UCMJ

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

USSTRATCOM Directive 501-14, *Force Management Information System (FMIS) Reporting Procedures*

Significant References

CJCSI 3231-01, (S) *Safeguarding the Single Integrated Operational Plan*, with Change 1, April 1995

DoD 5200.28-M, *ADP Security Manual*, January 1995

DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985

AFI 33-203, *The Air Force Emission Security Program*

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

AFSSI 5013, *Identification and Authentication*

Abbreviations and Acronyms

ADP—Automated Data Processing

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

AFSPC—Air Force Space Command

AFWA—Air Force Weather Agency (formerly AFGWC)

BCP—Base Communications Processor

CM—Configuration Management

CPMF—Computer Program Maintenance Facility

CSSO—Computer Systems Security Officer

CSS—Computer Systems Squadron

DAA—Designated Approval Authority

DoD—Department of Defense

DTS—Data Transmission Subsystem

EC—Equipment Custodian

EMSEC—Emission Security

ESI—Extremely Sensitive Information

FA—Functional Area

FOUO—For Official Use Only

HQ AFCA—Headquarters Air Force Communications Agency

IP—Information Protection

NQCC—Network Quality Control Center

OIC—Officer in Charge

SACCS—Strategic Automated Command Control System

SATE—Security Awareness, Training, and Education

SCP—Subnet Communications Processor

SF—Standard Form (used on forms only)

SIOP—Single Integrated Operational Plan

STF—Software Test Facility

TASO—Terminal Area Security Officer

UCMJ—Uniform Code of Military Justice

UserID—User Identification

USSTRATCOM—United States Strategic Command