



TELEPHONE SYSTEMS SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

This instruction establishes the Air Force Telephone Systems Security Program to provide security procedures for Electronic Telephone Switches. It applies to all Air Force MAJCOMs/Wings/Units. Security of the base telephone system is of paramount importance to the protection of base communications. There is a need to safeguard telephone service to the customer, billing records, and telephone plant by restricting switch access to telephone maintenance personnel and other authorized persons or organizations. This document outlines the security measures to be used by maintenance personnel as an application guide to implementing security. While these guidelines are about the digital switches in the Air Force inventory, the concepts apply to all telephone switches (including telephone key systems). **NOTE:** If this document conflicts with other Air Force publications (directives, instructions, and manuals), the other publications will take precedence.

SUMMARY OF REVISIONS

This is the first issuance of this AFSSI.

	Paragraph
Chapter 1--Roles and Responsibilities	
Roles and Responsibilities	1.1.
MAJCOMS.....	1.1.1.
Wings	1.1.2.
Unit Commander	1.1.3.
Unit Chiefs of Maintenance	1.1.4.
Maintenance Personnel	1.1.5.
Superintendent.....	1.1.6.
NCOICs.....	1.1.7.
Chapter 2--Implementation	
Minimum Security Policy Implementation	2.1.
Chapter 3--Passwords	
Procedures	3.1.
Composition	3.1.1.
Length	3.1.2.
Change Rate	3.1.3.
Grace Period.....	3.1.4.
Security	3.1.5.
Chapter 4--Physical Access	
Procedures	4.1.
Switchroom Access	4.1.1.
Maintenance Terminal Access	4.1.2.
Identification and Authentication General Guidelines	4.1.3.
Discretionary Access General Guidelines	4.1.4.
Specific Command Access Guidelines.....	4.1.5.
Chapter 5--Banner	
Security Banner.....	5.1.

Chapter 6--Remote Access

Procedures.....	6.1.
Positive Barriers.....	6.1.1
Remote Access User Identification.....	6.1.2.
Remote Login	6.1.3.
Maintenance Contractors	6.1.4.
Remote Switch Access (RSA)	6.1.5.
Remote Ports.....	6.1.6.
Disconnect Equipment.....	6.1.7.
RSA Personnel Listing.....	6.1.8.
Requesting RSA.....	6.1.9.
Dial-Up Access Log	6.1.10.
RSA Security	6.1.11.

Chapter 7--Audit Requirements

Procedures.....	7.1.
Review Report	7.1.1.
Record Security Events.....	7.1.2.
Record Userid	7.1.3.

Chapter 8--Recovery

System Recovery	8.1.
-----------------------	------

Chapter 1

Roles and Responsibilities

1.1. ROLES AND RESPONSIBILITIES:

- 1.1.1. MAJCOMs will manage a command level Telephone Systems Security Program ensuring worldwide implementation for all installations under their command.
- 1.1.2. Wings will implement the Telephone Systems Security Program and ensure telephone systems security is included in their Wing Information Protection Assessment and Assistance Program.
- 1.1.3. Unit Commanders responsible for Telephone Systems Security will ensure this AFSSI is implemented at their location.
- 1.1.4. Mission Systems Flight Commander responsible for Telephone Systems O & M will assign the responsibilities outlined in this AFSSI to qualified personnel.
- 1.1.5. Responsible Telephone Systems maintenance personnel will implement security procedures and perform the Audit review as outlined in this AFSSI.
- 1.1.6. Superintendents will review the Audit Report weekly.
- 1.1.7. NCOICs will review the Audit Report daily.

Chapter 2

IMPLEMENTATION

2.1. MINIMUM SECURITY POLICY IMPLEMENTATION.

- 2.1.1. Be familiar with the security features available in your telephone system and how they are employed.
- 2.1.2. Evaluate all components of the telephone system for security risks in order to minimize the vulnerability of unauthorized access. These components include the switchroom, telephone system, and auxiliary processors, such as fax machines, modems, recorded announcement equipment, printers, terminals, and computers.
- 2.1.3. Establish a Telephone Systems Security Administrator responsible for establishing, implementing, monitoring, and controlling the telephone system's security program.
- 2.1.4. Implement a Telephone Systems Security Program that addresses computer security and controlled area security concerns. Ensure the program follows current COMPUSEC and resource protection guidance.
- 2.1.5. Evaluate the security program using a self-inspection checklist at least semi-annually.
- 2.1.6. Ensure the integrity and efficacy of the protective measures with a regular program of security inspections.

- 2.1.7. Ensure access to central office features is controlled by use of subscriber class of service or class of restrictions.
- 2.1.8. To safeguard against unauthorized use, ensure the telephone switch is frequently monitored to identify changing calling patterns, system uses, and possible security issues. You must then modify the routing and calling privileges to support changing user and mission requirements.
- 2.1.9. Provide internal and external users access only to the facilities, functions, commands, and calling privileges their jobs require. For example, limit access to the telephone system database only to a specific few users. This will greatly decrease the potential of system abuse and fraud.
- 2.1.10. Telecommunications managers must select and implement the combination of features that best meet mission needs, while recognizing the trade off between security and convenience (i.e., level of risk).
-

Chapter 3

PASSWORDS

3.1. PROCEDURES.

- 3.1.1. Password Composition: The password must be alpha-numeric with at least one special character. Where technically feasible, the password must also consist of a combination of uppercase and lowercase letters. It is also best to randomly generate the password in the system, where technically and procedurally feasible. If user-generated passwords are used, ensure they meet the basic criteria outlined in this chapter. Avoid passwords that are either all numbers or all letters to the greatest extent possible.
- 3.1.2. Password Length: Password length will be a *minimum* of 6 alpha-numeric characters with 8 being the recommended length where technically feasible. Passwords of greater length are encouraged because they provide better protection, but they could become cumbersome for the user. NOTE: Most telephone systems have a default parameter of 6.
- 3.1.3. Password Change Rate: Passwords require periodic change to maintain integrity of the password system. There must be time parameters and procedures established to ensure periodic changes of passwords as well as whenever a password compromise is suspected or confirmed. Repeated reuse of the same passwords is prohibited.
- 3.1.3.1. To protect against unknown threats, the *maximum* lifetime of a password must be no greater than 180 days with 90 days being the recommended lifetime. The shorter the life of the password, the less likely a compromise will occur due to a valid password being used by an unauthorized user. However, if a less frequent change rate is used, the minimum password length must be made longer to maintain the low probability of the password being guessed. For example, if a 360-day expiration rate is used in conjunction with the previous parameters the *minimum* password length would be 9 characters--if the system allows.
- 3.1.3.2. Change the password as soon as possible (maximum within 1 duty day) if a password compromise is suspected or confirmed. Also, change the password as soon as possible (maximum within 1 duty day) if a user's access is removed due to punitive action or at the user's commander's request.
- 3.1.3.3. Disable the password as soon as possible (maximum within 3 duty days) if the user no longer requires access for a period greater than 90 days (e.g., TDYs).
- 3.1.3.4. Remove the user name and password immediately when a person no longer requires access for the performance of their job, i.e., PCS, move to another section, discharged. Procedures must be put in place to ensure this is accomplished.
- 3.1.4. Password Grace Period: Password grace period is the number of logins into the system after a password has expired. The password grace period must be set to 3. This forces the maintenance technicians to change their password after 3 grace period logins or be locked out of the system until the Telephone Systems Security Administrator can reinstate them.
- 3.1.5. Password Security: Do not write down passwords or store them in any easily accessible location (e.g., a function key). This minimizes the likelihood of them being used by unauthorized personnel. Also passwords must not be shared. Maintenance and administrative personnel who have access to system modification commands must be briefed semi-annually on the importance of password security.
-

Chapter 4

PHYSICAL ACCESS

4.1. PROCEDURES.

4.1.1. **Switchroom Access:** Physical access to the switchroom is limited by the local communications unit to the fewest personnel required to accomplish the mission. This must apply to remote telephone switching facilities, also. Cypher locks, or similar device, must be installed on all doors that allow access to telephone switching facilities for access control.

4.1.2. **Maintenance Terminal Access:** Access to maintenance terminals must be limited by the local communications unit to only the personnel that require access in the performance of their jobs. If possible, automatically log out terminals when idle for over 10 minutes or not in use.

4.1.3. **Identification and Authentication General Guidelines:**

4.1.3.1. The system design must contain no means of bypassing the identification and authentication mechanisms.

4.1.3.2. After successful logon, the user must be presented with the date and time of the last successful logon plus the number of unsuccessful attempts since that logon.

4.1.3.3. The switch must cease to respond to login attempts from any user (remote or otherwise) after three consecutive failed logon attempts. The user will be locked out of the system until the Telephone Systems Security Administrator can reinstate them.

4.1.3.4. The switch must issue a real-time alarm to notify the switch administrator of all repeated failed login attempts.

4.1.3.5. Establish procedures on how to deal with periods of inactivity on terminals. It is recommended, as a minimum, that remote terminals be disconnected after a specified period of inactivity.

4.1.4. **Discretionary Access General Guidelines:** Use discretionary access to control access to the objects in the switch such as data tables and executable code modules after the users have gained access to the switch. This will usually be the authorized users such as maintainers and administrators. Discretionary access will limit the damage an unauthorized user who has defeated the identification and authentication mechanisms might do.

4.1.4.1. The switch must authorize access to objects based on individual user identification, user's authority or role, and no group accesses must be permitted.

4.1.4.2. Newly created objects must, by default, be protected at the level of authorization of the creating user.

4.1.4.3. Access to objects must be authorized by mode, such as Read Data Table, Update Data Table, Create a File, Delete a File, Write a File, Create or Delete a Directory, or Change Access Privileges (e.g., allow a user or process previously unauthorized access to an object).

4.1.4.4. The switch must provide the capability to restrict access by time of day, day of week, and calendar date. If technically feasible, implement restricted access for non-duty hours.

4.1.4.5. The switch must provide a separation of low-privileged and highly-privileged users. The switch's security mechanisms must provide the ability to restrict low-privileged users to only the minimum privileges required to perform their jobs.

4.1.4.6. The switch must restrict access based on terminal identifier to the minimum needed by the user's function such as Applications, Operating System Commands, or Data Tables. Also, restrict access to commands used to mount removable media to specific users such as the system administrator.

4.1.4.7. Any switch services provided to subscribers, such as direct inward system access (DISA), must be protected by password or other authentication mechanisms.

4.1.5. **Specific Command Access Guidelines:** Restrict access to telephone system commands based on the functions of the user. This can be accomplished through class marking commands according to their level of importance and criticality. All commands must be class marked to prevent unauthorized system access. Do not use any manufacturer commands class mark defaults. NOTE: In digital telephone systems, class marking commands permit or deny access to software commands. Care must be taken not to class mark commands to allow global use of certain commands for ease of operation.

4.1.5.1. Maintenance terminals in the telephone switch room must have all privileges. This is to allow any level of maintenance to be performed from any device. Class marking user passwords and system commands can provide the level of protection required.

4.1.5.2. Maintenance terminals placed apart from telephone switch room must be class marked to only allow execution of commands needed to accomplish their function (e.g., subscriber feature changes, network analysis).

4.1.5.3. Administrative User: This is the most powerful user class available. It has unlimited access to all system commands, users and resources; can override all other users and carries the highest priority. Assign this function to only a few personnel -- recommend no more than 2 or 3. This is usually the office and/or workcenter supervisor to prevent compromise and security violations.

4.1.5.4. Maintenance User: This must be the most common user class in the central office. This user has access to all commands and resources necessary to perform the assigned maintenance action(s) (e.g., trunk maintenance, line maintenance, switch maintenance). It must not be allowed access to other user classes nor be able to manipulate any secure logs or reports. This function is assigned to as many maintenance personnel as required to perform maintenance.

4.1.5.5. Security Administrative User: This user must be assigned access to all user accounts, system monitoring commands, devices and any secure logs or reports. It must not be allowed access to maintenance functions or other areas not required for the performance of this function. This function must be limited to the Telephone System Security Administrators only.

4.1.5.6. Contractor User: This user must only be assigned to the dial-up ports that are dedicated for contractor access. Contractors usually require a broad range of access, but are physically controlled by the on-site maintenance personnel.

Chapter 5

BANNER

5.1. SECURITY BANNER.

5.1.1. A security banner will appear immediately upon logging into the telephone system. No one must be allowed further access into the system until the security banner has been read and acknowledged, if technically feasible.

NOTE: The security banner must state the following: ***Official United States Government System for authorized use only. Do not discuss, enter, transfer, process, or transmit classified/sensitive national security information of greater sensitivity than this system is authorized. Using this system constitutes consent to security testing and monitoring. Unauthorized use could result in criminal prosecution.***

5.1.2. As long as a banner appears (even if not acknowledgeable), any access to the system via any terminal (remote or otherwise) implies consent to monitoring.

Chapter 6

REMOTE ACCESS

6.1. PROCEDURES.

6.1.1. Positive barriers must exist to prevent all system modifications, except those for specific emergency or directed maintenance actions.

6.1.2. Remote Access User Identification:

6.1.2.1. The validity of the identification of remote users will be limited to a time window during which the remote user is expected to log in.

6.1.2.2. When a remote user is communicating with the switch from an intermediate site, the computer at the intermediate site must be identified and authenticated in a manner similar to a remote user.

6.1.2.3. The switch must provide the capability to open and close a time window for the remote maintenance access port(s) of the switch. This will prevent repeated login attempts by "hacking" if the modem is left turned on.

6.1.2.4. Remote users passwords will be used one time only. Subsequent logons will require a new password for each session.

6.1.3. Remote login via modem is discouraged for routine maintenance procedures. Also, do not use remote login for planned maintenance functions. Remote login must *always* make use of automatic dial-back capabilities, if technically possible. This provides an extra measure of security that is not available with standard dial-up modem ports. Never configure the telephone system to allow access without dial-back unless maintenance personnel are on-site to authenticate the caller and maintenance requirement. This helps to prevent someone from finding out the number of the maintenance modem(s).

6.1.4. Maintenance contractors not assigned to the duty section must not be allowed access to the telephone system unless specifically requested by on-site personnel or there is specific need for data collection outlined in an agreement between the contractor and the government. There must be authorized maintenance personnel on-site for the duration of the access. Assign dedicated modems for contractor access. Off-line, turn-off or physically disconnect dedicated contractor modems when not in use. The contractor must provide a list of authorized personnel who require access to the telephone system in the performance of their job. Government representatives will use this list to authenticate contract personnel. The contractor must periodically update this list to help prevent unauthorized access.

6.1.5. There must be no way for remote switch access (RSA) except through a dedicated port.

6.1.6. Keep remote ports disconnected from all trunks and lines leaving the central office when not in use.

6.1.7. Keep modems, telephones, or other ancillary equipment disconnected or off-line from the RSA port leaving the central office, except during RSA.

6.1.8. Maintain a list of personnel that require RSA (government and contractor personnel).

6.1.9. When RSA is required, it can only be requested by personnel on the RSA list. Establish the connection from a designated telephone.

6.1.10. Maintain a log of all requests for RSA.

6.1.11. Central office personnel are responsible for ensuring the security of the RSA. Their duties consist of performing the following minimum sequence each time the telephone system is accessed via RSA.

6.1.11.1. Verify that there is an immediate need for RSA.

6.1.11.2. When a request for RSA is received, log the request and verify personnel against the access list

6.1.11.3. Unless you called for maintenance support, authenticate and call back to verify the validity of their phone number.

6.1.11.4. Once authenticated, establish the necessary connections between the remote access user, the ancillary equipment (modem and port), and the trunk and/or line.

6.1.11.5. Verify the RSA connection between the user and telephone system.

6.1.11.6. If possible, monitor activities of the remote user in real-time. This can be accomplished by recording remote activity, with hard copy printout or other comparable means. Terminate the session immediately if any improper activity is observed.

Chapter 7

AUDIT REQUIREMENTS

7.1. PROCEDURES.

7.1.1. The audit report must be reviewed in accordance with paragraphs 1.1.6 and 1.1.7 of this document. If discrepancies are noted, appropriate actions and reporting must be done in accordance with governing guidance.

7.1.2. If technically feasible, the following security events, as a minimum, must be recorded in the audit files:

7.1.2.1. Login attempts (failed or otherwise).

7.1.2.2. Remote login attempts (failed or otherwise).

7.1.2.3. Password changes.

7.1.2.4. Creation of user accounts.

7.1.2.5. Critical table modifications (e.g., audit mechanisms deactivations, alarm table changes, etc.).

7.1.3. If technically feasible, the audit will, as a minimum, record the userid involved, time and date of the event, the event, and the success or failure of the event.

CHAPTER 8

RECOVERY

8. SYSTEM RECOVERY

8.1. Ensure that restoring the telephone system to operational status (including activating security functions) is part of system recovery planning and is incorporated in the appropriate plans.

8.2. After system recovery, security functions must be restored to the minimum levels as outlined in this document.

RONALD G. GOESSMAN
Chief, Information Protection Division