

**BY ORDER OF THE COMMANDER
NIAGARA FALLS AIR RESERVE
STATION**



**NIAGARA FALLS AIR RESERVE
STATION INSTRUCTION 33-201**

30 APRIL 2010

Certified Current 16 June 2014

Communications and Information

**PROTECTION/USE OF SECURE
TELECOMMUNICATIONS DEVICES**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 914 CS/SCBS

Certified by: 914 CS/SC
(LtCol David P. Jaacks)

Pages: 5

This publication implements AFD 33-2, *Information Assurance Program* and AFI 33-201, Volume 9, *Operational Instruction for Secure Voice Devices*. This instruction provides guidance regarding the use and protection of secure telephone devices. It applies to all members assigned to Niagara Falls Air Reserve Station (NFARS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force Form 847, *Recommendation for Change of Publication*; route AF Form 847 directly to 914 CS/SCB at Niagara Falls Air Reserve Station. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with the Air Force Manual (AFMAN) 33-363, *Management of Records*, and dispose of in accordance with the Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-61a/afirms.afirms/>.

1. Responsibilities: Each Secure Telecommunications Device user will ensure that the procedures outlined in this instruction are adhered to at all times.

2. Procedures:

2.1. Use the Secure Telecommunications Device in the unkeyed mode/logged off mode to place unsecured, unclassified calls. Remove the Fortezza Card or Personal Identification Number (PIN) to log off the terminal.

2.2. When the terminal is in the keyed mode (Card/PIN in the device), it must be afforded protection commensurate with the level of clearance authorized and may only be used by authorized personnel. When unauthorized personnel are in the area, the keyed device must be under the operational control and within the view of at least one known, appropriately cleared, and authorized person.

2.3. Secure telecommunications devices not operational 24 hours a day will have the Card/PIN removed no later than the close of business. The Card must be listed as an item on the end of day security checklist (Standard Form (SF) Form 701 or suitable alternate). The Card will be stored in a GSA approved security container, if kept in the same room as the Secure Telecommunications Device. Only authorized Secure Telecommunications Device users will have access to the container. When the Card is stored in another room, it will be kept in a GSA approved security container. If a security container is not available, store the Card in a locked cabinet, desk, etc. The adequacy of storage alternatives is determined on a case-by-case basis, by the unit security manager within each using organization. PINs will never be written down outside of the COMSEC Manager's Vault.

2.4. Strict attention must be paid to the authentication display to ensure the classification level of the conversation does not exceed the highest clearance classification displayed. Recommend users scroll the distant end to ensure the distant end key is current and not expired.

2.5. Before discussing classified information on the Secure Telecommunications Device, the person making the classified call must ensure all personnel in the area are cleared and those remaining have a need to know.

2.6. Users should pay close attention to the authentication information displayed in the terminal during each secure call. When two terminals communicate in the secure mode, each terminal automatically displays the authentication information of the distant terminal. The information displayed indicates the organization reached, the approved level of the call, and when there is foreign access of the terminal, but does not authenticate the person using the terminal. Therefore, users must use judgment in determining need-to-know when communicating classified information.

2.7. Report a lost Card or device to the base COMSEC manager, immediately. You will be instructed by the COMSEC manager on what actions to take.

2.8. Ensure the equipment custodian has all Secure Telecommunications Device assigned to the section listed on the CA/CRL.

2.9. If any problems are experienced with the Secure Telecommunications Device, call the COMSEC Manager's Office (SCBS).

3. Emergency Action Procedures: In the event of fire, natural disaster, or covert threat, the Card will be removed from the Secure Telecommunications Device and locked up, or kept in the personal possession of an authorized individual. PIN activated units will be logged off prior to departure.

4. Training: Each user agency shall ensure all personnel with access to a secure telecommunications device will be trained annually in accordance with AFI 33-201, Volume 9. This responsibility falls to the Secure Voice Responsible Officer (SVRO) or COMSEC Responsible Officer (CRO) in each agency possessing Secure Telecommunications Devices.

5. Adopted Form:

AF Form 847, Recommendation for Change of Publication

SF-701, *Activity Security Checklist*

ALLAN L. SWARTZMILLER, Colonel,
USAFRC Commander

Attachment 1**GLOSSARY OF REFERENCES AND OTHER INFORMATION*****References***

AFPD 33-2, *Information Protection*, 19 Apr 2007

AFI 33-201 Volume 9, *Operational Instruction for Secure Voice Devices*, 13 March 2005

AFMAN 33-363, *Management of Records*, 1 March 2008

Abbreviations and Acronyms

AFCA—Air Force Command Authority

AFMAN—Air Force Manual

AW—Airlift Wing

CA/CRL—Custodian Authorization/Custody Receipt Listing

COMSEC—Communication Security

CRO—COMSEC Responsible Officer

GSA—General Services Administration

NFARS—Niagara Falls Air Reserve Station

PIN—Personal Identification Number

RDS—Records Disposition Schedule

SF—Standard Form

SVRO—Secure Voice Responsible Officer

Terms

Adopted Form—A form used (required) in a publication other than the prescribing publication.

Approval Authority—Senior leader responsible for contributing to and implementing policies and guidance/procedures pertaining to their functional area(s) (e.g., heads of functional two-letter offices).

Certifying Official—A minimum of one organizational level above the OPR, this individual certifies the need for the publication, to include currency of information, applicability to the Air Force, and propriety of content.

Office of Primary Responsibility—The originating office for a publication; the author of the publication is an individual within the OPR. OPRs are solely responsible for the accuracy, currency, and integrity of their publications and forms.

Publication—An officially produced, published, and distributed document issued for compliance, implementation, and or information.

Records Disposition Schedule (RDS)—The official schedule that authorizes/governs the disposition of Air Force records, which contains National Archives and Records Administration (NARAA) approval authority.

Records Management—The planning, controlling, directing, organizing, training, promoting, and any other managerial activity related to records creation, records maintenance and use, and records disposition for the sake of achieving adequate and proper documentation of the policies and transactions of the Federal government and effective economical management of agency operations.