

18 MARCH 2004



Communications and Information

FORTEZZA OPERATIONAL SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: HQ AFCA/WFPL
(Mr. James N. Plummer, Jr.)
Supersedes AFI33-277, 8 AUGUST 2003

Certified by: HQ USAF/XICI
(Lt Col Yolanda Cruz)
Pages: 38
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*) and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3028, *Operational Security Doctrine for the FORTEZZA User Personal Computer Memory Card International Association (PCMCIA) Card*, dated December 2001, and Assistant Secretary of Defense (NII)/Information Assurance Memo, *Defense Message System FORTEZZA Handling Policy Letter*, dated 10 October 2003. It provides guidance for the FORTEZZA Responsible Officers (FRO) and FORTEZZA users. This instruction contains minimum security standards for the protection and use of the FORTEZZA User PCMCIA card. This instruction applies to all Air Force military and civilian personnel, including civilians under contract by the Department of Defense (DoD), who handle, distribute, account for, or use the FORTEZZA card and associated Public Key Infrastructure (PKI) certificates. The users of this Air Force instruction (AFI) may extract information as deemed necessary to perform their duties. Additional security instructions and manuals are listed on the Air Force website at Uniform Resource Locator (URL): <http://www.e-publishing.af.mil> under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct any questions or comments concerning the contents of this instruction through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**. Provide an information copy to Headquarters United States Air Force (HQ USAF/XICI), 1800 Air Force Pentagon, Washington DC 20330-1800. Send supplements to this publication to HQ AFCA/WFP for review, coordination, and approval prior to publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with AFMAN 37-139, *Records Disposition Schedule*. Public Law 104-13, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Content Management Program--Information Management Tool (CMP-IMT)*, affect this publication. The use of the name or mark of any specific manufacturer, commer-

cial product, commodity, or service in this publication does not imply endorsement by the Air Force. See **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF REVISIONS

Adds the requirements from ASD/NII memo on removing FORTEZZA cards when not actively in use for message origination or reception and adds the memo as a reference. Added the AFMAN reference concerning records management. Adds the function of the Base Organizational Registration Authority (B-ORA) to the function of the Certification Authority (CA) for Certification Authority Workstations (CAW) that have been regionalized. Changes the PIN for the KOV-11 to unclassified. Changes retention of the custody log from 90 days to 20.5 years. Updates publication titles and terms. Changes the security check function from an FORTEZZA Responsible Officer (FRO) duty to a User responsibility.

Section A	General Information.	5
1.	Introduction.	5
2.	Scope.	5
3.	Policy.	5
Section B	FORTEZZA Card Implementation	6
4.	FORTEZZA Card Implementation.	6
Section C	Appointment of FORTEZZA Responsible Officer	7
5.	Appointing FORTEZZA Responsible Officers (FRO).	7
Section D	Responsibilities	7
6.	Certification Authority (CA).	7
7.	Commander.	8
8.	FORTEZZA Responsible Officers (FRO):	8
9.	FORTEZZA Users.	9
Section E	Administrative Security Procedures	9
10.	FORTEZZA Specific Forms.	9
11.	Records Maintenance and Disposition.	9
12.	Operating Instructions.	9
13.	Training.	10
14.	Emergency Procedures.	10
15.	Security Checks.	10
Section F	Security and Accountability.	10
16.	Card Classification.	10

17.	Card Nomenclature and Marking.	11
Table 1.	FORTEZZA Card Information.	12
18.	Safeguarding the KOV-11.	12
19.	Personal Identification Number (PIN) Length.	13
20.	Safeguarding PINs.	13
21.	Automatic Disabling.	13
22.	Accountability.	13
23.	Classified Information Security.	13
24.	Disposal/Destruction.	14
Section G	Restrictions	14
25.	FORTEZZA and FFC Incompatibility.	14
26.	Individual Certificates.	14
27.	Organizational Certificates	14
Table 2.	Custody Log for KOV-11.	15
28.	Storing Certificates.	15
Section H	Control Requirements.	15
29.	Access Controls.	15
30.	Removing FFC Card from Classified Enclave.	16
31.	Tampering.	16
32.	Loaning Cards.	16
33.	Inoperable KOV-11.	16
34.	Duplicate Cards.	17
35.	Protecting Workstations.	17
Section I	Information Systems Security	17
36.	Virus Detection.	17
37.	Configuration Management.	17
38.	FFC Architectural Approval.	17
39.	Authorized Computers.	17
40.	Classification Labeling.	18
Section J	Public Key Infrastructure Requirements	18
41.	User Registration.	18

42.	Card and PIN Distribution.	18
43.	User Advisory Statement and Receipt.	18
44.	KOV-11 Rekey and Certificate Renewal.	18
45.	Loss/Compromise Requirements.	19
46.	Certificate Revocation List (CRL) and Compromised Key List (CKL) Posting.	19
47.	User Departure.	19
48.	Digital Signature Verification.	19
Section K	Methods for Transporting Programmed KOV-11s	19
49.	Within the US, Its Territories, and Possessions.	19
50.	Outside the US, Its Territories, and Possessions.	20
Section L	Reportable Events	20
51.	Reportable Events.	20
52.	Reportable Information.	20
Section M	Information Assurance Assessment and Assistance Program (IAAP)	21
53.	Information Assurance Assessment and Assistance Program.	21
Section N	Exceptions	21
54.	Exceptions.	21
55.	Information Collections, Records, and Forms or Information Management Tools (IMT).	21
Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		22
Attachment 2— EXAMPLE OF APPOINTMENT LETTER FOR FORTEZZA RESPONSIBLE OFFICER (FRO) AND ALTERNATES		27
Attachment 3— FORTEZZA USER TRAINING		28
Attachment 4— FORTEZZA USER ADVISORY STATEMENT AND RECEIPT		29
Attachment 5— USE OF THE FFC CARD TO SEPARATE COMPARTMENTED DATA		30
Attachment 6—INTERIM CHANGE 2004-1 TO AFI 33-277, FORTEZZA OPERATIONAL SECURITY		31

Section A—General Information.

1. Introduction. This instruction replaces AFSSI 3034, dated 11 January 2000. Changes include deletion of the Remote Access Security Program (RASP) information, references to obsolete marking labels of FORTEZZA cards, and references to version 1 or version 3 certificates. It adds FORTEZZA Card implementation and changes the reference from PC card to PCMCIA. This instruction sets procedures for FROs and FORTEZZA users. It describes their duties and the minimum requirements for safeguarding, controlling, accounting for, and returning KOV-11s (FORTEZZA and FORTEZZA For Classified [FFC] user cards).

1.1. The combination of the KOV-11, FORTEZZA-enabled software and PKI provides the security services FORTEZZA offers. Users must take the approved measures as outlined in this instruction to maintain the security of both the KOV-11 and associated PKI.

2. Scope. This instruction applies to the FORTEZZA PCMCIA cards employing the Type 2 suite of algorithms (e.g., SKIPJACK, Key Encryption Algorithm (KEA), Secure Hash Algorithm (SHA), Digital Signature Algorithm (DSA), and commercial algorithms) only, and includes crypto cards and FORTEZZA-enabled PCMCIA modem cards. This instruction does not apply to PCMCIA cards employing a Type 1 suite of algorithms (e.g., FORTEZZA Plus). As other FORTEZZA implementations evolve, this instruction will be updated to include appropriate controls or they will be issued through a separate instruction. When the term KOV-11 is used, it is referring to both the FORTEZZA card (used to protect sensitive information) and the FFC card (used to protect SECRET or TOP SECRET information). **NOTE:** The minimum-security standards for protection and use of the Certification Authority (CA) cards are defined in AFSSI 3039, *Operational Security Instruction for the FORTEZZA Card Certification Authority Workstation (CAW)* .

3. Policy. The KOV-11 provides cryptographic functionality and storage of keying material, authorization, and user identification. When combined with FORTEZZA-enabled applications, the card, employing a Type 2 suite of algorithms, provides confidentiality, user identification and authentication, and nonrepudiation (proof of origin and receipt) in unclassified and classified environments.

3.1. **Unclassified Environment.** The FORTEZZA card with FORTEZZA-enabled applications provides confidentiality, user identification, authentication, and nonrepudiation sufficient to protect unclassified and sensitive information .

3.2. **Classified Environment.** The FFC is a FORTEZZA card programmed with PKI X.509 certificate(s) configured to protect classified information. The FFC card, with FORTEZZA-enabled applications, may be used on a secure system or network to provide user identification, authentication, nonrepudiation, and secondary confidentiality of classified information. The primary confidentiality of the network is ensured by a Type 1 product or a Protected Distribution System, or if the network exists completely within a physically secure space. The FFC card with FORTEZZA-enabled applications alone shall not be used as the primary means of providing confidentiality for classified information in any medium. A FFC card with certificates configured for use in a SECRET environment is called an “FFC card with certificates for SECRET.” A FFC card with certificates configured for use in a TOP SECRET environment is called an “FFC card with certificates for TOP SECRET.”

Section B—FORTEZZA Card Implementation

4. FORTEZZA Card Implementation. Under the DoD Information Assurance Solution (IAS) Program technology and components are being deployed in large numbers to protect valuable government information. The FORTEZZA card is a component of a network security solution and is intended to be used in conjunction with other IAS components (e.g., firewalls, high-assurance guards (HAG), and trusted database servers) to provide an appropriate and comprehensive network security solution. **NOTE:** The specification or description of other IAS components, including firewalls, HAGs, and trusted database servers, is beyond the scope of this instruction.

4.1. FORTEZZA. The FORTEZZA card, combined with FORTEZZA-enabled applications, provides security services appropriate for protecting unclassified and sensitive data. Additional IAS components (e.g., firewall, guards, and trusted database servers) may be required to protect sensitive information in a networked environment, and are encouraged whenever accessing the public internet. The cognizant Designated Approving Authority (DAA) may mandate additional components.

4.2. FORTEZZA for Classified (FFC). This paragraph provides the minimum system architecture requirements needed to securely process classified information with the FFC card. It is not intended to describe all system architecture requirements that must be met to create an approved system environment.

4.2.1. Information Segregation on a Single Level Secure System or Network. The DAA for a secure network may approve the use of the FFC card to segregate classified information for privacy or need-to-know consideration. This application includes use of the FFC card to maintain segregation between compartments or special handling categories on a common classified network approved to process information at any level up to TOP SECRET under conditions detailed in [Attachment 5](#). However, the secure network must already be protected with Type 1 encryption or a protected distribution system.

4.2.2. Information Exchange Between Secret Enclave and Sensitive Enclave over Unclassified Network. The DAA for a FORTEZZA supported workstation processing information classified up through SECRET in a protected enclave may authorize the exchange of sensitive or unclassified network (e.g., the internet) with FORTEZZA supported workstation processing sensitive information within a sensitive enclave, provided all of the following conditions are met :

4.2.2.1. A HAG is interposed between the classified enclave and the unclassified network. The HAG must perform a Crypto Invocation Check on any message leaving the classified enclave.

4.2.2.2. A firewall is interposed between the sensitive enclave and the unclassified network.

4.2.2.3. All communication from the classified enclave is encrypted with an unclassified certificate on the FFC card. That certificate must have been loaded on the FFC card by an unclassified Certification Authority Workstation (CAW).

4.2.2.4. FORTEZZA-enabled applications must be used.

4.2.2.5. A virus check must be performed prior to transferring information from an unclassified enclave to a classified enclave.

Section C—Appointment of FORTEZZA Responsible Officer

5. Appointing FORTEZZA Responsible Officers (FRO). Unit commanders (or equivalents) appoint, by letter, a primary FRO and at least one alternate to receive KOV-11s from the CA (see [Attachment 2](#)). The letter includes each individual's name, rank, social security number (SSN), security clearance, and duty telephone. Mark the letter as “For Official Use Only (FOUO).” Forward the original letter to the CA and a copy to the Sub-registration Authority (SRA). The FRO will maintain a copy for their local files. Review this letter at least annually or when changes occur .

5.1. Persons appointed as primary FROs must have a minimum grade of staff sergeant (E-5), General Schedule (GS)-5, or DoD contractors with approval from the unit commander. Alternates must have a minimum grade of Senior Airman (E-4) or GS-4.

5.2. FROs must have at least a final SECRET clearance; or a final TOP SECRET if access to TOP SECRET cards.

5.3. Commanders must also consider the following criteria when appointing an FRO:

5.3.1. Units With An Established Communications Security (COMSEC) Responsible Officer (CRO). The CRO is an individual within an office or unit responsible for COMSEC material received from the COMSEC account. CRO duties and appointment criteria are located in AFI 33-211, *Communications Security (COMSEC) User Requirements*. The CRO should also function as the FRO.

5.3.2. Units With An Established Secure Telephone Unit (STU)-III Responsible Officer (SRO). The SRO is an individual within an office or unit responsible for STU-III material received from the COMSEC account. SRO duties and appointment criteria are located in AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type 1*. The SRO should also function as the FRO .

5.3.3. Units with an Established Registration Authority (RA). The RA is a local administrative authority who performs the registration function by gathering end-user registration information and forwarding it to the CA. AFI 33-127, *Electronic Messaging Registration and Authority*, lists additional RA functions. The RA will also function as the FRO.

5.4. Unit commanders approve waivers for personnel with lower grades. Waiver approval will be incorporated in a separate paragraph on the individual's appointment letter. Security clearance requirements cannot be waived.

Section D—Responsibilities

6. Certification Authority (CA). The CA is responsible for programming KOV-11s on the CAW. Specific duties and responsibilities for CAW operations are defined in AFSSI 3039. The CA:

6.1. Ensures all programmed KOV-11s intended for use are issued to the appropriate FROs and are signed for by the FRO on the FRO Receipt Log. An example of the FRO Receipt Log is located within AFSSI 3039.

6.2. Ensures FROs are provided information on KOV-11 implementation, use, storage, restrictions, administrative procedures, transport, issue, controls, marking, accountability, reportable events, and physical security requirements before issuing KOV-11s .

- 6.3. Provides FRO and all alternate FROs initial and refresher training according to paragraph [13](#).
- 6.4. Ensures another FRO or alternate signs for KOV-11s, when an FRO transfers or if their security clearance is suspended .
- 6.5. Assess semiannually FROs according to [Section M](#).
- 6.6. For MAJCOMs who have regionalized CAWs, the CA acts as the Base Organizational Registration Authority (B-ORA).

7. Commander. The commander of each unit that uses KOV-11s:

- 7.1. Appoints, in writing, an FRO and at least one alternate to receive KOV-11s. May appoint more than one FRO in large units, depending on the number of FORTEZZA users and the volume of KOV-11s handled. Appoint FROs according to paragraph [5](#).
- 7.2. Ensures approved security containers or facilities are available for storing FFC Personal Identification Numbers (PIN).
- 7.3. Takes action on reportable events according to [Section L](#).
- 7.4. May appoint an Approving Official (AO) to approve all X.509 Certificate Request Forms used to create organizational certificates. The AO maintains a list of current organizational office symbols authorized to perform organizational messaging with the privileges and clearance associated with each organization. This is an optional appointment and commanders may combine this responsibility with other duties of the FRO.

8. FORTEZZA Responsible Officers (FRO):

- 8.1. Ensure all users granted access to FFC cards have proper final security clearance and a valid need-to-know.
- 8.2. Conduct initial and refresher training of all FORTEZZA users according to paragraph [13](#). and [Attachment 3](#) .
- 8.3. Take responsibility for receiving, accounting for, handling, using, and safeguarding all KOV-11s until returned to the CA.
- 8.4. Develop local operating instructions (OI) according to paragraph [12](#).
- 8.5. Ensure X.509 Certificate Request Forms are properly completed, assisting users as needed, and verifying with the SRA that requested distinguished names (DN) are unique .
- 8.6. Perform annual inventories of FFC cards, per paragraph [22.1](#).
- 8.7. Issue KOV-11s and PINs to users using [Attachment 4](#).
- 8.8. Return all KOV-11s as the CA directs.
- 8.9. **DELETED.**
- 8.10. Report all known or suspected events to the CA according to [Section L](#).
- 8.11. Coordinate with the CA the transfer of responsibilities to another FRO prior to leaving their current assignment or duties.
- 8.12. Carry out additional duties requested by the CA.

9. FORTEZZA Users. FORTEZZA users are responsible for safeguarding their KOV-11s and their PINs to the level of the certificate in the KOV-11s. Ultimate success or failure rests with the individual users. The careless user or the user who fails to follow procedures for using and safeguarding KOV-11s wastes all security efforts. FORTEZZA users must make sure only authorized individuals have access to shared organizational cards. Users must follow security rules at all times. Report to the FRO or the CA any circumstances or intentional or inadvertent acts which could lead to the disclosure of classified information, including its loss, improper use, unauthorized viewing, or any other instance that could possibly jeopardize the security of KOV-11 and the information it protects. FORTEZZA users:

- 9.1. Safeguard KOV-11s according to this instruction and control the cards locally.
- 9.2. Return KOV-11s to the FROs on request, when no longer required, and prior to permanent departure from the unit.
- 9.3. Report immediately any reportable event of KOV-11s and their PINs to the FRO or CA according to [Section L](#).
- 9.4. Remove KOV-11s from their card readers when they are not actively in use for message origination or reception and safeguard according to paragraph [18](#).
- 9.5. Ensure security checks are performed according to paragraph [15](#).

Section E—Administrative Security Procedures

10. FORTEZZA Specific Forms. X.509 Certificate Request Form.

11. Records Maintenance and Disposition. Dispose of all records per AFMAN 37-139.

11.1. Do not use correction fluid or correction tape on records that affect control and accountability of KOV-11s. Use only original forms and complete using only blue or black ink. For errors, neatly line through errors, initial, and date. Record explanatory remarks on the back of the form. This includes the X.509 Certificate Request Form, FORTEZZA Receipt ([Attachment 4](#)); Standard Form (SF) 700, **Security Container Information**; SF 701, **Activity Security Checklist**; and SF 702, **Security Container Check Sheet**.

11.2. Archive the User Advisory Statements and FORTEZZA Receipt ([Attachment 4](#)). The original is retained by the CA and maintained according to AFMAN 37-139. The CA determines if a copy is to be maintained by the FRO.

11.3. Retain the custody log for KOV-11s at the using organization for three years from the date of the last entry, after which the logs will be forwarded to the cognizant CA for archiving, which will be kept for 20.5 years, See [Table 2](#).

12. Operating Instructions. Each FRO must write an OI and coordinate it with the CA. The procedures and instructions in the OI are specific to the user's activity. The OI includes procedures for handling, controlling, storing, transporting, and protecting the KOV-11s and PIN, as well as conducting an annual inventory, identifying training requirements, card rekey, access restriction, emergency procedures, reporting reportable events, user departures, remote users (if applicable), and the transfer of responsibilities to another FRO.

13. Training. Read and sign **Attachment 3**, FORTEZZA User Training, to document initial and refresher training for all persons with access to a KOV-11. Provide annual refresher training to all personnel who use KOV-11s by having them read and sign **Attachment 3**. Maintain only the most current documentation.

14. Emergency Procedures.

14.1. For fire, natural disaster, bomb threats, and covert threat, the authorized user will remove the KOV-11 from the card reader and secure it or keep it in their possession until order returns. During emergencies, these procedures are exempt from paragraph **30**.

14.2. When evacuating the area, keep the KOV-11s in personal possession.

14.3. For emergency destruction procedures for the KOV-11s, see paragraph **24.2**.

15. Security Checks. Perform daily security checks at the end of each workday (or beginning of each shift for 24-hour operations) to ensure proper storage and accountability is maintained for all KOV-11s. Record the security checks on either the SF 701 (for daily operations) or DD Form 1753, **Master Station Log** (for 24-hour operations). At a minimum, the security checks must include:

15.1. Checking all card readers to ensure KOV-11s are removed.

15.2. Making sure all KOV-11s are properly safeguarded according to paragraph **18**.

15.3. Making sure physical security systems or devices (e.g., door locks, vent covers, etc.) work, and that safes, locking devices, outer doors, windows, and so forth, are locked. If available, ensure alarms are set.

Section F—Security and Accountability.

16. Card Classification.

16.1. FORTEZZA. The FORTEZZA card is unclassified both when locked by a PIN and when unlocked. **NOTE:** The FORTEZZA card and the FFC card are identical except for the classification of certificates loaded onto each. Therefore, the nomenclature “KOV-11” applies to both.

16.2. FORTEZZA for Classified (FFC). The FFC card is unclassified when locked by the PIN. When unlocked by the PIN the FFC card is classified at the level of the highest classification to be protected by certificates on the card.

16.2.1. The implementing organization may, in order to further mitigate risk to its information, elect to handle the FFC card as classified material when not in use and locked with the PIN. Any change from the default marking of UNCLASSIFIED assigned to all user cards by the CAW (see paragraph **17.1**.) would require that custom labeling be placed on the FFC card.

16.2.2. An FFC card with both certificates for classified information from a classified CAW and certificates for unclassified information from an unclassified CAW is called a “dual-certificate” card. A dual-certificate card is classified when unlocked and can only be used on a computer authorized to process classified information. Dual-certificate card supports the environment described in paragraph **4.2.2**.

16.2.3. Each user's public key certificates for FFC use which are stored on the workstation, remain unclassified. Do not mark or handle the FORTEZZA or the FFC cards as CRYPTO or Controlled Cryptographic Item (CCI).

17. Card Nomenclature and Marking.

17.1. Nomenclature. KOV-11 is both the National Security Agency (NSA) assigned short title and the Federal Stock System nomenclature for all FORTEZZA user cards. Since the FORTEZZA user card is not controlled within the COMSEC Material Control System (CMCS), this instruction will refer to "KOV-11" as a nomenclature. **NOTE:** The FORTEZZA card and the FFC are identical except for the classification of certificates loaded onto each. Therefore, the nomenclature "KOV-11" applies to both.

17.1.1. FORTEZZA nomenclature use evolved during its deployment. FORTEZZA and FFC cards with X.509 Version 1 certificates were assigned nomenclatures as shown in [Table 1](#). However, the multiple nomenclatures created inventory and accounting difficulties. As a result, the KOV-12 nomenclature is no longer used and cards bearing this nomenclature shall be phased out.

17.1.2. As the FORTEZZA PKI transitions to X.509 Version 3 certificates, user card nomenclature is standardized to KOV-11. Old labels not reflecting Version 3 certificates will be replaced when the user card is returned to the CA for rekey/certificate renewal, but no later than December 31, 2004.

17.2. KOV-11 Label. The CAW prints a card label that uniquely identifies each card. This label contains the nomenclature (KOV-11), unique internal chip serial number, user name, card classification, and indicates if it is programmed with certificates for unclassified or classified information. A FORTEZZA card with certificates to protect unclassified information has a white label, and an FFC card with certificates for SECRET information has a red label. An FFC card with certificates for TOP SECRET information has a yellow label. Label colors follow the same scheme regardless of which X.509 certificate version is loaded on the card. The user will not remove the card label. [Table 1](#), provides approved nomenclature and labeling guidance for FORTEZZA user cards.

17.3. FORTEZZA-enabled PCMCIA-card Modem. The FORTEZZA-enabled PCMCIA-card modem (e.g., Palladium modem card) uses the similar PKI certificates as a FORTEZZA card, and must have these certificates loaded by a CAW in the same manner as a standard FORTEZZA or FFC card. The CAW treats the FORTEZZA modem card as a standard FORTEZZA card or FFC card, and so prints a label as discussed above. See AFSSI 3038, *Operational Security Instruction for the Remote Access Security Program (RASP) Secret Dial-In Solution*, for more information.

Table 1. FORTEZZA Card Information.

FORTEZZA Card Information				
Type	X.509 Ver 1 Nomenclature	X.509 Ver 3 Nomenclature	Label and Type Color	Marking
Organizational and personal FORTEZZA user card	None	KOV-11	White Label Black Type	Unclassified
Organizational and personal FFC user (with FFC certificates up through SECRET)	KOV-11 or KOV-12	KOV-11	Red Label Black Type	Unclassified (See 18.2.2.)
Organizational and personal FFC user (for compartmented on TOP SECRET networks - see Attachment 5)	KOV-12	KOV-11	Yellow Label Black Type	Unclassified (See 18.2.2.)

NOTE: FORTEZZA card labeling is distinct and different from federal magnetic media labeling. The FFC card is classified only when unlocked and in use, so a federal standard magnetic media label indicating a permanent classification (e.g., the orange SF 706) is inappropriate.

18. Safeguarding the KOV-11.

18.1. FORTEZZA User Cards. Protect FORTEZZA cards (*KOV-11s with only unclassified certificates loaded*) in a manner similar to a credit card or high value item to limit the possibility of loss, unauthorized use, substitution, tampering or breakage. Individuals may carry KOV-11s in their possession, provided the cards are given the level of protection discussed in this paragraph.

18.2. FORTEZZA for Classified.

18.2.1. Physically protect a locked FFC card (i.e., a card that is not in use) in a manner similar to a credit card or high value item to limit the possibility of loss, unauthorized use, substitution, tampering, or breakage. Individuals may carry KOV-11s, provided the cards are given the level of protection discussed in this paragraph.

18.2.2. An unlocked FFC card (i.e., an FFC card that is in use) must be afforded the protection commensurate with the certificates. At no time will an FFC be left in an unattended terminal. If the FFC card is not in active use, the user must log out of the application, remove the FFC card from its reader, and protect it as described in paragraph [18.2.1.](#)

18.2.3. An unlocked FFC card may be left in a continuously operating unstaffed infrastructure component (e.g., a Defense Message System Message Transfer Agent) provided the component or the space in which it is located provides protection commensurate with the classification of the information the component is authorized to process.

18.3. FORTEZZA PCMCIA Modem Card. Afford protection to a FORTEZZA or FFC Modem card inside a secure facility at least equal to that given the same type of user card.

19. Personal Identification Number (PIN) Length. The minimum requirement for a FORTEZZA or FFC user card (any KOV-11) is seven numeric characters. The maximum length is 12 numeric characters.

20. Safeguarding PINs.

20.1. Memorize the PIN. Do not write the PINs on the KOV-11 card or record in any manner in the vicinity of the host system for any reason.

20.2. Do not share the PIN for individual cards. Apply the requirements in paragraph 27.3. when sharing the PIN for organizational cards and duplicate cards for infrastructure components.

20.3. The PIN for a KOV-11 is unclassified.

20.3.1. For FORTEZZA cards, securely store the PIN or PIN letter physically separate from the card to prevent loss or unauthorized access .

20.3.2. At the discretion of the implementing organization the following steps are provided to further mitigate risk to operational information. For FFC cards, record the PIN on an SF 700 and store in a GSA-approved container at the level of the certificate in the FFC. Destroy the PIN letter as classified waste. An alternative to the SF 700 would be to store the PIN in a sealed opaque envelope with initials over the envelope's seal in such a way that tampering will be obvious.

21. Automatic Disabling. The KOV-11 will disable itself after ten consecutive failed attempts to enter the PIN. Users must then contact their FRO (who will contact the CA) to arrange for card reactivation and new PIN assignments. The CA will provide a new PIN and reactivate the card. **NOTE:** If the KOV-11 has several certificates, the first CA who programmed a certificate onto the card is the only one who can reactivate the card.

22. Accountability. Programmed KOV-11s are unclassified but locally accountable by the FRO to the CA. Track and identify KOV-11s by means of the card's internal chip serial number and by the user's distinguished name, printed on the card label by the CAW as described above. **Do not track the KOV-11s by the manufacturer's external serial numbers, because these numbers are not unique.** The CA will affix the label identifying unique internal chip serial number and user name to the card. Users will not remove the label.

22.1. Inventory. The FRO conducts a physical inventory of all FFC cards (including duplicate cards) annually according to guidance provided by the CA. The inventory must include physically viewing the card and rechecking the identity of the FFC owner. FROs report the results of the inventory to the CA. If an FFC card cannot be accounted for within 15 days of the required annual inventory, then the certificates associated with the missing FFC cards will be added to the Compromised Key List (CKL) and Certification Revocation List (CRL). To avoid unnecessary revocation actions, ensure FFC cards are inventoried in a timely manner.

22.2. Additional Accountability. KOV-11s remain the property of the issuing organization. Local policy may also require additional accountability of the cards.

22.3. Change of FRO. Prior to departure, the new FRO and the current FRO will jointly perform a physical inventory of all KOV-11s under their control.

23. Classified Information Security. Users must safeguard and control all classified information transmitted with the FFC card in accordance with AFI 31-401, *Information Security Program Management* .

24. Disposal/Destruction.

24.1. Routine Disposal.

24.1.1. KOV-11. Return excess or no longer required programmed KOV-11s to the issuing CA who will determine if the card can be reused. If cards are not returned in person to the CA, the cards must be returned via controlled methods (those methods which provide a continuous chain of accountability, as described in [Section K.](#))

24.1.2. PIN Letters. Destroy the PIN letter as you would classified waste for FFC cards. Destroy the PIN letters for FORTEZZA cards by tearing them up and throwing them into two separate trash containers.

24.2. Emergency Destruction. If the capability exists and the time is available, return the KOV-11 to the CA who will zeroize as an alternative to physical destruction. If time is not available, destroy KOV-11s by smashing or breaking, ensuring the card is unusable. Destroy organizational cards prior to individual user cards.

Section G—Restrictions

25. FORTEZZA and FFC Incompatibility. Certificates loaded by an unclassified CAW are not cryptographically compatible with any certificates loaded by an FFC CAW .

26. Individual Certificates. KOV-11s with certificates programmed for individual messaging accounts must not be shared. The authenticity of messages is based on individuals using only the card assigned to them.

27. Organizational Certificates . KOV-11s with certificates programmed for organizational use (“organizational certificates”) carry additional requirements, as follows :

27.1. Indicated on the X.509 Certificate Request Form, the primary individual who will control the KOV-11.

27.2. The FRO must track the names of primary individuals to whom organizational certificates were issued.

Table 2. Custody Log for KOV-11.

Example of Custody Log for Shared Organizational Cards				
Custody Log for KOV-11				
Internal Serial Number		Distinguished Name on Organization Card		
000000003ad4458d		123ABW/FM		
Name of User	Date/Time Issued	Initials	Date/Time Returned	Initials
TSgt Donald A. Davis	3 Aug 02/0910	<i>DAD</i>	3 Aug 02/0945	<i>DAD</i>
SSgt Martha O. Mathis	4 Aug 02/1015	<i>MOM</i>	4 Aug 02/1056	<i>MOM</i>
MSgt Kyle I. Donaldson	4 Aug 02/1320	<i>KID</i>	4 Aug 02/1425	<i>KID</i>

27.3. The FRO, who signs for the shared organizational certificates, must ensure control of these certificates, including accounting for which individual had control of the keys at all times.

27.3.1. A listing of individuals having access to the organization card must be created and maintained. Limit the access list to only those users who have a need and the authority to send messages on behalf of the organization .

27.3.2. A custody log ([Table 2.](#)) noting the KOV-11 serial number, the name of the user, date and the time issued and returned meets the minimum requirement.

27.3.3. **DELETED.**

28. Storing Certificates. Storage on the KOV-11 is limited to certificates, keying material and security-critical information. Users are not authorized to write any information to the KOV-11 .

Section H—Control Requirements.

29. Access Controls. The primary access control for the KOV-11 is having the proper security clearance, a need-to-know, supervisor's approval, and any other security standards imposed by the CA in order to issue a card and associated certificates to a given user. The FRO will only issue FFC cards to properly cleared users. The user must be cleared to a level equal to or greater than the card's highest certificate clearance. **NOTE:** This instruction refers only to granting access to a KOV-11. All other requirements must be met prior to granting access to a KOV-11. Requirements such as foreign disclosure, investigation, security clearance, and foreign national access, still apply when granting access to the local area network (LAN) and the information contained in the systems connected to the LAN .

29.1. United States (U.S.) Citizens. U.S. citizens (military, civilian employees of the government, and employees of a U.S. Government Contractor or Vendor) may be issued KOV-11s if an operational need is validated by an appropriate individual.

29.2. Permanently Admitted Resident Aliens. KOV-11s may be issued to permanently admitted resident aliens who are civilian employees of the U.S. Government, employees of a U.S. Government Contractor or Vendor, or are active duty or reserve component members of the U.S. Armed Forces. The decision to issue a KOV-11 shall be made by the unit commander based on a determination that the official duties of the permanently admitted resident alien require this access .

29.3. Foreign Nationals. KOV-11s may be issued to foreign nationals who are civilian employees of the U.S. Government, or employees of a U.S. Government Contractor or Vendor. The decision to issue a KOV-11 shall be made by the unit commander based on a determination that the official duties of the foreign national require this access.

29.3.1. Foreign Nationals Involved in Combined Exercises and Operations. Foreign nationals may be issued KOV-11s when combined military exercises and operations are initiated, and reclaimed when such operations are concluded. Additional handling restrictions may be levied on foreign national users at the discretion of the issuing CA. The decision to issue cards to Foreign Nationals shall be based upon an operational need determined by the cognizant US military commander. Examples of situations in which foreign nationals may be issued KOV-11s include :

29.3.1.1. Foreign liaison officers granted access to information systems in their extended visit authorization.

29.3.1.2. Foreign exchange officers granted access to information systems in their position authorization.

29.3.1.3. Allies or coalition partners in a co-manned environment and allies or coalition partners in combined exercises or operations .

30. Removing FFC Card from Classified Enclave. Users who have an operational requirement to remove the FFC KOV-11 from a classified high enclave must be authorized by the cognizant DAA and reminded of their responsibility to safeguard the card outside the secure enclave. Users without such a requirement will satisfy paragraph [18.2.1](#). and secure their FFC KOV-11s within the secure enclave. Issue a separate unclassified-only KOV-11 to users who have additional requirements to conduct unclassified transactions outside of an environment approved for classified information processing. In general, do not remove the FFC card from the secure enclave except for administrative purposes (e.g., to transport card from issuing location to user's location).

31. Tampering. Do not attempt to make a copy or tamper with the KOV-11. It is the user's responsibility to report any suspected tampering attempts in accordance with [Section L](#). The user must not attempt any modification to the card's software or hardware .

32. Loaning Cards. KOV-11s programmed and assigned to one individual user will not be loaned to any other individual.

33. Inoperable KOV-11.

33.1. Users must not attempt to repair or reprogram inoperable KOV-11. Return inoperable card to the issuing CA, who will determine if the card can be reused .

33.2. If the KOV-11 cannot be returned in person to the CA, the cards must be returned via controlled methods that provide a continuous chain of accountability, as described in [Section K](#) .

33.3. If the card itself is defective, program a new card, new certificate, and new PIN for the user. Revoke the old certificates from inoperable KOV-11s. The user must notify all CAs who placed certificates on their inoperable KOV-11 so those certificates may be revoked. To allow recovery of existing information (e.g., back traffic, text files, database files) encrypted with the old certificate, reprogram the old certificate onto the new card. This will allow the user to recover and reencrypt

information from the old certificate to the new certificate. The CA must revoke the old certificates 30 days after reissue.

34. Duplicate Cards. Duplicate cards will only be created for infrastructure components (e.g., a Defense Message System Message Transfer Agent).

35. Protecting Workstations. Protect workstation(s) with FORTEZZA-enabled software in a manner sufficient to prevent loss, tampering, or unauthorized use of the system. To prevent possible unauthorized use never leave a terminal unattended after the PIN has been successfully entered into the KOV-11 and the FORTEZZA-enabled software is available for use. An exception is allowed for continuously operating systems protected in accordance with paragraph **18.2.3**.

35.1. Lock screens and screensavers are not acceptable means to protect an unlocked KOV-11 in a workstation.

Section I—Information Systems Security

36. Virus Detection. Install Air Force-approved anti-virus software on workstations, which run FORTEZZA-enabled applications. Operate and update antivirus software according to AFI 33-202, *Network and Computer Security*.

37. Configuration Management. Use the most current version of FORTEZZA-enabled software. If the user receives software and hardware changes contact the local workgroup manager to assist in confirming the authenticity and ensure the installation is approved by the DAA.

38. FFC Architectural Approval. Approve implementation of the FFC card, along with other necessary Information Assurance Solution/FFC components for protecting classified or compartmented information, by the appropriate DAA prior to use.

39. Authorized Computers.

39.1. FORTEZZA Card. A FORTEZZA card and FORTEZZA-enabled software may only be used with a computer authorized to process unclassified or sensitive information.

39.2. FFC Card.

39.2.1. Use FFC cards with certificates for classified information (SECRET, TOP SECRET, etc.) only with a computer, and within an environment, that has been authorized for the processing of comparably classified and below information. An FFC card with certificates for SECRET information must be used on a system authorized to process SECRET and below information within a classified environment. The only exception is the authorized FFC remote user (see **Attachment 5**).

39.2.2. Use FFC cards with both (classified and unclassified) certificates from a classified CAW and unclassified certificates from an unclassified CAW (a “dual-certificate” card) only within a computer and an environment that is authorized to process information at the level of the highest classification asserted by certificates on the card. Do not use an FFC card with dual certificates in an unclassified computer/environment.

40. Classification Labeling. The FORTEZZA-enabled software (e.g., electronic messaging) must provide appropriate security labeling for the data being processed. That is, the FORTEZZA-enabled software must require the user to insert the classification level of the data (message) and it must ensure the correct certificate is used based on the chosen classification and the cryptographic environment of the message recipient .

Section J—Public Key Infrastructure Requirements

41. User Registration. The prospective user must provide at least one official picture identification (e.g., military ID card, driver's license, etc.) to the FRO upon registration for the KOV-11. See [Section H](#) for specific qualifications of a user. The CA promulgates specific user registration procedures .

42. Card and PIN Distribution. Keep the KOV-11 and the associated PIN letter separate from the time they are produced by the CA until the intended user receives them. The CA will issue KOV-11s and PINs to FROs.

42.1. In the event of hand-delivery, and if the distribution facility is separate from the FRO's working facility, the FRO may carry both KOV-11 and PIN letter back to the working facility. Provide measures to minimize the risk of the loss or compromise of both card and PIN letter (e.g., don't carry card and PIN letter in the same container). Seal the PIN in an opaque envelope for delivery to the end user with the CA's initials over the seal.

42.2. The KOV-11 and associated PIN letter may be mailed to the user's work address, provided the KOV-11 and PIN letter are mailed at least 3 days apart. Mail cards according to [Section K](#).

43. User Advisory Statement and Receipt. Upon receiving the KOV-11 and PIN, the user must sign and date a User Advisory Statement ([Attachment 4](#)), and return it to the FRO. By signing the receipt, the user acknowledges receipt of both the KOV-11 and PIN, and the user agrees to accept the certificates listed on the documentation provided with the KOV-11. If the user does not sign and return the User Advisory Statement to the FRO within 15 days, the FRO will notify the issuing CA who will revoke all of the user certificates on that KOV-11.

44. KOV-11 Rekey and Certificate Renewal.

44.1. KOV-11 Rekey. Rekey the KOV-11 at least every 3 years. Change the user's PIN when the card is rekeyed. Return the KOV-11 to the issuing CA for rekey using transportation methods specified in [Section K](#).

44.2. Certificate Renewal. Renew and validate the user's certificates at least every 3 years, normally when the card is rekeyed. Also, renew the certificate to reflect any changes in the user's Distinguished Name as they occur.

44.3. Notification. Notification of pending key, PIN, or certificate expiration may occur in one of two ways:

44.3.1. The FORTEZZA-enabled application or User Agent will alert to request rekey and certificate renewal from the issuing CA(s).

44.3.2. The FRO will ensure user cards are rekeyed. The FORTEZZA Receipt, signed by the user, lists the expiration date.

44.4. The FRO will present the KOV-11s to the CA, who will reprogram the KOV-11s to renew all the certificates and key. If the FRO fails to present the KOV-11s to the CA when notified to do so, the certificates will be added to the CRL within 72 hours and further use of the expired certificates will be inhibited.

45. Loss/Compromise Requirements. Report the loss or suspected compromise of a KOV-11 to the CA by the FRO no later than 1 working day after discovery. Information required by the CA is described in **Section L**. Users with KOV-11s programmed with certificates from multiple CAs must report to each CA.

46. Certificate Revocation List (CRL) and Compromised Key List (CKL) Posting. CAs post a new CRL every 14 days, or as necessary due to certificate revocation. Users are responsible to ensure their workstation always contains the most recent CRL or CKL listings.

47. User Departure. Prior to departing an organization, the user must return KOV-11s to the FRO who will give it to the CA. Failure to return the KOV-11 will result in the CA reporting a compromise of user FORTEZZA keys to the Policy Creation Authority (PCA).

47.1. Access to Organizational Cards. Update the access list for the organizational card and remove the user's upon departure or when access to the organization card is no longer needed. Change the PIN number if the user will still have access to the LAN and the card.

48. Digital Signature Verification. Verify the sender's digital signature prepared by the sender's KOV-11 against the CRL listing to validate the authenticity of the transmitted data. If the sender's digital signature certificate has expired or cannot be verified, do not accept the transmission as valid.

Section K—Methods for Transporting Programmed KOV-11s

49. Within the US, Its Territories, and Possessions. To transport KOV-11 within the US, its territories and possessions one of the following is required:

49.1. An authorized user to whom the card is issued.

49.2. A designated US Government courier.

49.3. US Postal Service (USPS) registered mail providing the material does not, at any time, pass out of US control, pass through any foreign postal system, or be subject to any foreign postal inspection.

49.4. A commercial shipping form that meets the following criteria.

49.4.1. Be incorporated in the US and provide door-to-door service.

49.4.2. Guarantee delivery within a reasonable number of days based on the distance to be traveled.

49.4.3. Have a means of tracking individual packages within its system to the extent that, if a package becomes lost, the carrier can, within 24 hours following notification, provide information regarding the package's last known location.

49.4.4. Guarantee the integrity of the transporting vehicle's contents at all times.

49.4.5. Guarantee the package will be afforded a reasonable degree of protection against theft (e.g., use of a security cage, video surveillance, etc.) if it becomes necessary for the carrier to make a prolonged stop at a carrier terminal.

50. Outside the US, Its Territories, and Possessions. Programmed KOV-11 may be transported outside the US, its territories and possessions, according to paragraph 49. above, with the following additional restrictions :

50.1. USPS registered mail may be used to ship FFC cards to/from locations overseas, but only if the location is serviced by a Fleet Post Office (FPO) or Army/Air Force Post Office (APO) that is authorized to process USPS registered mail .

50.2. To the maximum extent possible, material shipped to/from locations outside the US, its territories and possessions must remain under continuous US control. Although some limited handling of the material by foreign nationals may be unavoidable during aircraft loading and unloading operations, the material must be returned to US control upon completion of these operations. If the material subsequently shows evidence of unauthorized access or tampering, report accordance to **Section L** of this document.

Section L—Reportable Events

51. Reportable Events. Report the following events involving KOV-11 use to the FRO. The FRO will report the information to the CA immediately, but no later than 1 working day after the event, for review and possible compromise recovery actions.

51.1. Loss of Card. The temporary or permanent loss of any KOV-11.

51.2. PIN Compromise. Actual or suspected compromise of PIN.

51.3. Card Misuse. Actual or suspected misuse of the KOV-11 and associated software (i.e., unauthorized modification to the FORTEZZA software installed on the host).

51.4. Card Tampering. Actual or suspected tampering with the KOV-11.

51.5. Duplicate Cards. Unauthorized use of an authorized duplicate KOV-11 or an unauthorized duplication of a KOV-11.

51.6. Unreported Personal Data Changes. User failure to notify the issuing CA of DN changes.

51.7. User Departure. KOV-11 users leaving an organization without advising the FRO or CA concerning the status of their card.

51.8. Premature Disabling. Detection that a user's card is disabled prior to the user making ten unsuccessful consecutive attempts to unlock their card.

51.9. Incorrect Certificate Use. The use of a sensitive certificate for protecting classified information.

52. Reportable Information. The FRO will provide the following data to the CA to assess the impact of the events detailed in paragraph 51.:

52.1. User's name, distinguished name, card serial number (chip internal serial number), and organization.

- 52.2. All certificates and CAs who programmed certificates on the card.
- 52.3. Complete circumstances of incidents, including physical security situations.
- 52.4. Other personnel involved in the incident.
- 52.5. What was potentially compromised (the card, PIN, or FORTEZZA software).
- 52.6. User's assessment of degree of potential compromise.
- 52.7. Any additional information that may be requested.
- 52.8. Commander's comments and corrective action taken.

Section M—Information Assurance Assessment and Assistance Program (IAAP)

53. Information Assurance Assessment and Assistance Program. Conduct an assessment and audit of KOV-11 user's facilities semiannually at scheduled times. Use AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**, Section 1. Ensures that the KOV-11s are properly received, controlled, handled, safeguarded, stored, and destroyed per this instruction. In addition, the major commands also check these users during the periodic command IAAP. Conduct IAAPs according to AFI 33-230, *Information Protection Assessment and Assistance Program* and AFI 33-211.

Section N—Exceptions

54. Exceptions. Requests for exceptions to any of the provisions of this instruction must be submitted through Air Force Command Information Assurance (IA) channels to HQ AFCA/WFP for analysis and HQ USAF/XICI for approval prior to implementation. All waiver requests for exceptions must be accompanied by complete operational justification.

55. Information Collections, Records, and Forms or Information Management Tools (IMT).

- 55.1. Information Collections: No information collections are created by this publication.
- 55.2. Records: Maintain and dispose of records created by this publication according to AFMAN 37-139, Table 33-28, Rules 1 thru 11.
- 55.3. Forms or IMTs: (Adopted and Prescribed).
 - 55.3.1. Adopted Forms or IMTs: AF Form 847, **Recommendation for Change of Publication**; AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**; SF Form 700, **Security Container Information**; SF Form 701, **Activity Security Checklist**; SF Form 702, **Security Container Check Sheet**; X.509 Certificate Request Form, **FORTEZZA Receipt**; and DD Form 1753, **Master Station Log**.
 - 55.3.2. Prescribed Forms or IMTs: No forms are prescribed by this publication.

WILLIAM HOBBS, Lt Gen, USAF
DCS, Warfighting Integration

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

Public Law 104-13, *The Paperwork Reduction Act of 1995*

Title 5 United States Code (U.S.C.), Section 552a, *The Privacy Act*

Title 10 United States Code (U.S.C.), Section 2224, *Defense Information Assurance Program*

Title 40 United States Code (U.S.C.), *Public Buildings, Property, and Works*, Section 1452

ASD(NII)/Information Assurance Memo, *Defense Message System FORTEZZA Handling Policy Letter*, dated 10 October 2003

NSTISSI 3028, *Operational Security Doctrine for the FORTEZZA User PCMCIA Card*, dated December 2001

AFPD 33-2, *Information Protection* (will become Information Assurance)

AFI 31-401, *Information Security Program Management*

AFI 33-127, *Electronic Messaging Registration and Authority*

AFI 33-202, *Computer Security* (will become *Network and Computer Security*)

AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type 1*

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

AFI 33-230, *Information Protection Assessment and Assistance Program*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFMAN37-123, *Management of Records*

AFMAN37-139, *Records Disposition Schedule*

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

AFSSI 3038, *Operational Security Instruction for the Remote Access Security Program (RASP) Secret Dial-In Solution*

AFSSI 3039, *Operational Security Instruction for the FORTEZZA Card Certification Authority Workstation (CAW)*

Abbreviations and Acronyms

ACL—Access Control List

AFCA—Air Force Communications Agency

AFDIR—Air Force Directory

AFI—Air Force Instruction

AFMAN—Air Force Manual

AO—Approving Official
APO—Army/Air Force Post Office
B-ORA—Base Organizational Registration Authority
CA—Certification Authority
CAW—Certification Authority Workstation
CCI—Controlled Cryptographic Item
CKL—Compromised Key List
CMCS—COMSEC Material Control System
CMI—Certificate Management Infrastructure
COMSEC—Communications Security
COTS—Commercial Off The Shelf
CRL—Certificate Revocation List
CRO—COMSEC Responsible Officer
DAA—Designated Approving Authority
DN—Distinguished Name
DoD—Department of Defense
DSA—Digital Signature Algorithm
FFC—FORTEZZA for Classified
FPO—Fleet Post Office
FRO—FORTEZZA Responsible Officer
FTP—File Transfer Protocol
GS—General Schedule
HAG—High Assurance Guard
IA—Information Assurance
IAAP—Information Assurance Assessment and Assistance Program
IAS—Information Assurance Solution
ISSO—Information System Security Officer
KEA—Key Encryption Algorithm
KMID—Key Material Identifiers
LAN—Local Area Network
NIST—National Institute of Standards and Technology
NSA—National Security Agency

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

OI—Operating Instructions

PAA—Policy Approving Authority

PCMCIA—Personal Computer Memory Card International Association

PCA—Policy Creation Authority

PIN—Personal Identification Number

PKI—Public Key Infrastructure

RA—Registration Authority

RASP—Remote Access Security Program

SA—System Administrator

SAP—Special Access Program

SAR—Special Access Required

SCI—Sensitive Compartmented Information

SF—Standard Form

SHA—Secure Hash Algorithm

SIPRNET—SECRET Internet Protocol Router Network

SRA—Sub-registration Authority

SRO—STU-III Responsible Officer

SSN—Social Security Number

STU-III—Secure Telephone Unit III

TS/SCI—Top Secret/Sensitive Compartmented Information

URL—Uniform Resource Locator

US—United States

USAF—United States Air Force

U.S.C.—United States Code

USPS—United States Postal Service

Terms

Certificate—A record holding security information about an information system user and vouches to the truth and accuracy of the information it contains. A public key certificate contains the name of a user, the public key component of the user, and the identity of the user who vouches that the public key component is bound to the named user. **NOTE:** A public key certificate is normally issued to individuals. When several individuals act in one capacity for an organization, an “organizational certificate” may be issued with the identity of the organization.

Certificate Revocation List (CRL)—A list of invalid certificates that have been revoked by the issuer. It is periodically issued by each certification authority and posted to the directory.

Certification Authority (CA)—A person responsible for issuing and revoking user certificates, and exacting compliance with the PKI policy as defined by the parent Policy Creation Authority. **NOTE:** The term CA refers to both the authoritative office and role, and the incumbent in that office. The CA is the third level in the PKI Certificate Management Infrastructure (CMI).

Certification Authority Workstation (CAW)—Commercial-off-the-shelf (COTS) workstation with a trusted operating system and special-purpose application software. The CAW programs KOV-11s with a user's security personality including certificates and cryptographic key. The CA operates the CAW.

Compromised Key List (CKL)—A list generated by a PCA that contains the Key Material Identifiers (KMID) of keys believed by the PCA to be compromised (i.e., that can no longer be trusted).

CRYPTO—Marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive US Government-derived information .

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority, delegated accrediting authority, and information system security manager.

Directory—An on-line repository of certificates, CRLs, and CKLs.

Distinguished Name (DN) —An identifier, unique to a given PKI CMI that represents an individual's identity.

Enclave—A general computing term used to describe an interconnected collection of some subset of an organization's local computing resources. An enclave is often comprised of heterogeneous platforms that operate in a multi-protocol environment sharing common characteristics. These characteristics may include, but are not limited to common ownership/management, common mission, definable physical boundary, common security policy, controllable access point(s) to the enclave, and heterogeneous levels of trust.

FORTEZZA Card—A personal computer card that uses algorithms and procedures approved by the National Institute of Standards and Technology (NIST) and NSA to provide network related security services. Also identified as the KOV-11. The card, when used in conjunction with the proper applications and network infrastructure, provides data integrity, access control, authentication, nonrepudiation and confidentiality of user information. **NOTE:** When the term KOV-11 is used, it is referring to both the FORTEZZA card (used to protect sensitive information) and the FORTEZZA for Classified (FFC) card.

FORTEZZA-enabled Application—Any software application that has been designed (or enabled) to use FORTEZZA cryptography when providing security services. This can be client software running locally on a user's workstation (e.g., File Transfer Protocol (FTP) clients, electronic mail clients, web browsers) or server software running unattended on a server (e.g., FTP servers, web servers, Directory System Agents).

Information Systems Security Officer (ISSO)—Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal.

Infrastructure Components—Components that provide connectivity to the backbone, provide management, control, security, and message transfer/conversion/expansion services to the site system and are required for the user components to function.

Locked—The KOV-11 is locked when it is not in a computer.

Key Material Identifier (KMID)—The KMID is a unique field contained in an X.509 certificate that identifies a specific set of private key material. The KMID is unique within the Policy Approving Authority (PAA) hierarchy.

Need-to-know—The necessity for access to, or knowledge or possession of, specific information required in performing official duties.

Personal Computer Memory Card International Association (PCMCIA) Card—The FORTEZZA cryptographic card is a peripheral that contains the processor, algorithms, and cryptographic material necessary to support personalized security services .

Personal Identification Number (PIN)—A random character string that unlocks and activates the KOV-11.

Public Key Infrastructure (PKI)—Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software .

Sensitive Information—Any information that the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national security interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy. The responsibility for determining the applicability of the handling caveat or warning notice lies with the originating organization. (Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of Title 10 United States Code (U.S.C), Section 2224 (Defense Information Assurance Program).

System Administrator (SA)—Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

Type 1 Product—Classified or controlled cryptographic item endorsed by NSA for securing classified and sensitive US Government information, when appropriately keyed. The term refers only to products, not to information, key, services, or controls. Type 1 products contain classified NSA algorithms. They are available to US Government users, their contractors, and federally sponsored non-US Government activities subject to export restriction in accordance with International Traffic in Arms Regulation .

Type 2 Product—Unclassified cryptographic equipment, assembly, or component, endorsed by NSA, for use in national security systems as defined in Title 40 U.S.C. Section 1452, *Public Building, Property, and Works*.

Unlocked—The KOV-11 is unlocked when it is in a computer and the PIN entered (activated).

Attachment 2**EXAMPLE OF APPOINTMENT LETTER FOR
FORTEZZA RESPONSIBLE OFFICER (FRO) AND ALTERNATES**

(Letterhead)

Date

MEMORANDUM FOR (Wing COMSEC Account)

FROM: (Office and Address)

SUBJECT: Appointment of FORTEZZA Responsible Officer (FRO) and Alternate(s)

1. The following persons are assigned as Primary FRO and Alternate FRO(s) for (unit/office symbol). They may receipt for KOV-11s up to and including (clearance) from (COMSEC Account Number).

PRIMARY FRO

NAME:

RANK:

SSN

CLEARANCE:

PHONE:

E-MAIL ADDRESS:

ALTERNATE FRO(s) *(repeat this information for all alternates)*

NAME:

RANK:

SSN

CLEARANCE:

PHONE:

E-MAIL ADDRESS:

2. Request you train the appointed FRO and alternate FRO(s) on the handling and safeguarding of KOV-11s according to AFI 33-277, *FORTEZZA Operational Security*.

3. This letter contains personal information protected by the Privacy Act of 1974.

4. This letter supersedes all previous letters from this office on this subject (or provide dates if specific letters are affected) .

NOTE: Letter must be marked FOUO when completed.

(Commander's Signature Block)

Attachment 3

FORTEZZA USER TRAINING

NOTES:

When the term KOV-11 is used, it is referring to both the FORTEZZA card (used to protect sensitive information) and the FFC card (used to protect SECRET information).

1. A locked KOV-11 (*i.e., a card that is not in use*) is considered unclassified. When the KOV-11 is in the terminal in the unlocked mode (*KOV-11 in the terminal and PIN activated*), afford protection commensurate with the highest level of the key it contains and ensure use only by the authorized individual.
2. When unauthorized personnel are in the area, discontinue the processing of sensitive or classified information on the terminal. Pay strict attention to the authorized classification level of the KOV-11 and ensure transmission does not exceed the highest authorized classification. To prevent possible unauthorized use never leave a terminal unattended after the PIN has been successfully entered into the KOV-11 and the FORTEZZA-enabled software available for use. Lockscreens and screensavers are not acceptable means to protect an unlocked KOV-11. Do not leave a FFC card in a terminal unattended. Remove KOV-11s from their card readers when they are not actively in use for message origination or reception.
3. When not in use, protect KOV-11s in a manner similar to a credit card or high value item to limit the possibility of loss, unauthorized use, substitution, tampering, or breakage. The KOV-11 must be in the user's possession at all times. When sleeping, protect the KOV-11 as you would your money, credit cards, and other valuables.
4. Memorize the PIN. Do not write the PIN on the KOV-11 card or record it in any manner in the vicinity of the host system for any reason. Do not share the PIN for individual cards. The PIN for a KOV-11 is unclassified. For FORTEZZA cards, securely store the PIN or PIN letter separate from the card to prevent loss or unauthorized access. For FFC cards, record the PIN on a SF 700, **Security Container Information**, and store in a GSA-approved container. Destroy the PIN letter as classified waste. An alternative to the SF 700 would be to store the PIN in a sealed opaque envelope with initials over the envelope's seal in such a way that tampering will be obvious.
5. Maintain an access list of authorized users of the organizational card. A custody log for the KOV-11 will be maintained when sharing the PIN for organizational cards and duplicate cards for infrastructure components.
6. Users are responsible for the proper safekeeping and immediate reporting of its loss, destruction, theft, or tampering. Notify the FRO immediately if an FFC card is left in an unattended terminal or a KOV-11 or its PIN is compromised.
7. In the event of fire, natural disaster, or covert threat, remove the KOV-11 from the terminal and secure it or keep it in the possession of the authorized user.

(Printed/Typed Name of User)

(Signature of User)

(Printed/Typed Name of Trainer)

(Signature of Trainer)

(Modify this training list for your location)

Attachment 4**FORTEZZA USER ADVISORY STATEMENT AND RECEIPT**

The KOV-11, FORTEZZA/FFC cryptographic card, is a self-contained security device which provides you, the user, with a digital certificate--a unique electronic "personality"--and all the cryptographic support functions you need to perform electronic digital signature, encryption, and decryption of your information, all in a flexible and compact package.

Because of its compact size, the cryptographic card can be carried readily in a pocket or purse. Used properly, your KOV-11 will provide you with a high degree of security. Be aware that loss of your KOV-11 may place the information you have protected at risk. A hostile entity that has unauthorized access to your card could attempt to use the card to decrypt information protected by that card. Furthermore, it could enable an unauthorized person to electronically masquerade as you.

While the KOV-11 does employ a Personal Identification Number (PIN) to prevent use of the card by unauthorized parties, no PIN-based system is absolutely foolproof. You must, therefore, take precautions to protect your KOV-11 and PIN from loss or theft .

Immediately report loss, attempted theft, destruction, tampering, or any similar possible compromise of your KOV-11 to your FORTEZZA Responsible Officer (FRO) at _____ or Certification Authority (CA) at _____.

By signing and returning this statement to your FRO, you agree to the following terms:

"I have read this statement and acknowledge receipt of the KOV-11 identified by serial number below, the associated PIN, and certificate noted on the PIN letter. I also agree to follow AFI 33-277, *FORTEZZA Operational Security*, pertaining to the policy for the KOV-11s. "

Card Type**Individual or Organizational**

Card Serial Number: _____

Expiration Date: _____

Unit/Office Symbol: _____

Duty Phone Number: _____

Name of User: _____

Signature: _____

Date of Receipt: _____

Attachment 5

USE OF THE FFC CARD TO SEPARATE COMPARTMENTED DATA

A5.1. Top Secret/Sensitive Compartmented Information (TS/SCI) Network. The FFC card may be used to separate SCI (including various releasability caveats), and Special Access Program/Special Access Required (SAP/SAR) information on a TS/SCI approved system or network. The application of FFC to protect SCI or SAP/SAR on a TS/SCI system must be approved by the DAA for the TS/SCI system. A central Access Control List (ACL) for the compartment is established and maintained by the compartment or program's Control Officer. The FORTEZZA provides Identification and Authentication of the individual users who are authorized access to the compartmented program. This technique employs the unique electronic "personality" (i.e., certificate) of the user stored in the FORTEZZA card as a positive method of identification. Access to SCI or SAP/SAR is enforced by either :

A5.1.1. Using FORTEZZA identification and authentication to verify a user against the ACL prior to allowing the user access to SCI or SAP/SAR information, or ;

A5.1.2. Having the sender and receiver of SCI or SAP/SAR information verify each other's identity against the ACL prior to exchanging the information.

A5.2. SECRET Network. The FFC card may be used to enforce releasability caveats and need-to-know within a SECRET approved system or network (e.g., SIPRNET). This application of FFC must be approved by the DAA for the system. As with the TS/SCI compartmented scenario, a central ACL for the caveat or need to know control is established and maintained by the cognizant authority. The FORTEZZA provides Identification and Authentication of the individual users who are authorized access to the information. Access to the need-to-know information is enforced by either:

A5.2.1. Using FORTEZZA identification and authentication to verify a user against the ACL prior to allowing the user access to the information, or ;

A5.2.2. Having the sender and receiver of compartmented information verify each other's identity against the ACL prior to exchanging the need-to-know information.

Attachment 6

INTERIM CHANGE 2004-1 TO AFI 33-277, FORTEZZA OPERATIONAL SECURITY

18 MARCH 2004

SUMMARY OF REVISIONS

Adds the requirements from ASD/NII memo on removing FORTEZZA cards when not actively in use for message origination or reception and adds the memo as a reference. Added the AFMAN reference concerning records management. Adds the function of the Base Organizational Registration Authority (B-ORA) to the function of the Certification Authority (CA) for Certification Authority Workstations (CAW) that have been regionalized. Changes the PIN for the KOV-11 to unclassified. Changes retention of the custody log from 90 days to 20.5 years. Updates publication titles and terms. Changes the security check function from an FORTEZZA Responsible Officer (FRO) duty to a User responsibility.

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*) and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3028, *Operational Security Doctrine for the FORTEZZA User Personal Computer Memory Card International Association (PCM CIA) Card*, dated December 2001, and Assistant Secretary of Defense (NII)/Information Assurance Memo, *Defense Message System FORTEZZA Handling Policy Letter*, dated 10 October 2003. It provides guidance for the FORTEZZA Responsible Officers (FRO) and FORTEZZA users. This instruction contains minimum security standards for the protection and use of the FORTEZZA User PCM CIA card. This instruction applies to all Air Force military and civilian personnel, including civilians under contract by the Department of Defense (DoD), who handle, distribute, account for, or use the FORTEZZA card and associated Public Key Infrastructure (PKI) certificates. The users of this Air Force instruction (AFI) may extract information as deemed necessary to perform their duties. Additional security instructions and manuals are listed on the Air Force website at Uniform Resource Locator (URL): <http://www.e-publishing.af.mil> under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct any questions or comments concerning the contents of this instruction through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**. Provide an information copy to Headquarters United States Air Force (HQ USAF/XICI), 1800 Air Force Pentagon, Washington DC 20330-1800. Send supplements to this publication to HQ AFCA/WFP for review, coordination, and approval prior to publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with AFMAN 37-139, *Records Disposition Schedule*. Public Law 104-13, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Content Management Program--Information Management Tool (CMP-IMT)*, affect this publication. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See [Attachment 1](#) for a glossary of references and supporting information.

6.6. For MAJCOMs who have regionalized CAWs, the CA acts as the Base Organizational Registration Authority (B-OTA).

8.9. DELETED.

9.4. Remove KOV-11s from their card readers when they are not actively in use for message origination or reception and safeguard according to paragraph 18.

9.5. Ensure security checks are performed according to paragraph 15.

11.3. Retain the custody log for KOV-11s at the using organization for three years from the date of the last entry, after which the logs will be forwarded to the cognizant CA for archiving, which will be kept for 20.5 years, See Table 2.

20.3. The PIN for a KOV-11 is unclassified.

20.3.2. At the discretion of the implementing organization the following steps are provided to further mitigate risk to operational information. For FFC cards, record the PIN on an SF 700 and store in a GSA-approved container at the level of the certificate in the FFC. Destroy the PIN letter as classified waste. An alternative to the SF 700 would be to store the PIN in a sealed opaque envelope with initials over the envelope's seal in such a way that tampering will be obvious.

24.1.2. PIN Letters. Destroy the PIN letter as you would classified waste for FFC cards. Destroy the PIN letters for FORTEZZA cards by tearing them up and throwing them into two separate trash containers.

27.3. The FRO, who signs for the shared organizational certificates, must ensure control of these certificates, including accounting for which individual had control of the keys at all times.

27.3.3. DELETED.

30. Removing FFC Card from Classified Enclave. Users who have an operational requirement to remove the FFC KOV-11 from a classified high enclave must be authorized by the cognizant DAA and reminded of their responsibility to safeguard the card outside the secure enclave. Users without such a requirement will satisfy paragraph 18.2.1. and secure their FFC KOV-11s within the secure enclave. Issue a separate unclassified-only KOV-11 to users who have additional requirements to conduct unclassified transactions outside of an environment approved for classified information processing. In general, do not remove the FFC card from the secure enclave except for administrative purposes (e.g., to transport card from issuing location to user's location).

36. Virus Detection. Install Air Force-approved anti-virus software on workstations, which run FORTEZZA-enabled applications. Operate and update antivirus software according to AFI 33-202, *Network and Computer Security*.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 104-13, *The Paperwork Reduction Act of 1995*

Title 5 United States Code (U.S.C.), Section 552a, *The Privacy Act*

Title 10 United States Code (U.S.C.), Section 2224, *Defense Information Assurance Program*)

Title 40 United States Code (U.S.C.), *Public Buildings, Property, and Works*, Section 1452

ASD(NII)/Information Assurance Memo, *Defense Message System FORTEZZA Handling Policy Letter*, dated 10 October 2003

NSTISSI 3028, *Operational Security Doctrine for the FORTEZZA User PCMCIA Card*, dated December 2001

AFPD 33-2, *Information Protection* (will become Information Assurance)

AFI 31-401, *Information Security Program Management*

AFI 33-127, *Electronic Messaging Registration and Authority*

AFI 33-202, *Network and Computer Security*

AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type 1*

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

AFI 33-230, *Information Protection Assessment and Assistance Program*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFMAN 37-123, *Management of Records*

AFMAN 37-139, *Records Disposition Schedule*

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

AFSSI 3038, *Operational Security Instruction for the Remote Access Security Program (RASP) Secret Dial-In Solution*

AFSSI 3039, *Operational Security Instruction for the FORTEZZA Card Certification Authority Workstation (CAW)*

Abbreviations and Acronyms

ACL Access Control List

AFCA Air Force Communications Agency

AFDIR Air Force Directory

AFI Air Force Instruction

AFMAN Air Force Manual

AO Approving Official

APO Army/Air Force Post Office

B-OTAB Base Organizational Registration Authority

CA Certification Authority

CAW Certification Authority Workstation

CCI Controlled Cryptographic Item

CKL Compromised Key List

CMCS COMSEC Material Control System

CMI Certificate Management Infrastructure

COMSEC Communications Security

COTS Commercial Off The Shelf
CRL Certificate Revocation List
CRO COMSEC Responsible Officer
DAA Designated Approving Authority
DN Distinguished Name
DoD Department of Defense
DSA Digital Signature Algorithm
FFC FORTEZZA for Classified
FPO Fleet Post Office
FRO FORTEZZA Responsible Officer
FTP File Transfer Protocol
GS General Schedule
HAG High Assurance Guard
IA Information Assurance
IAAP Information Assurance Assessment and Assistance Program
IAS Information Assurance Solution
ISSO Information System Security Officer
KEA Key Encryption Algorithm
KMID Key Material Identifiers
LAN Local Area Network
NIST National Institute of Standards and Technology
NSA National Security Agency
NSTISSI National Security Telecommunications and Information Systems Security Instruction
OI Operating Instructions
PAA Policy Approving Authority
PCMCIA Personal Computer Memory Card International Association
PCA Policy Creation Authority
PIN Personal Identification Number
PKI Public Key Infrastructure
RA Registration Authority
RASP Remote Access Security Program
SA System Administrator

SAP Special Access Program
SAR Special Access Required
SCI Sensitive Compartmented Information
SF Standard Form
SHA Secure Hash Algorithm
SIPRNETSECRET Internet Protocol Router Network
SRA Sub-registration Authority
SRO STU-III Responsible Officer
SSN Social Security Number
STU-III Secure Telephone Unit III
TS/SCI Top Secret/Sensitive Compartmented Information
URL Uniform Resource Locator
US United States
USAF United States Air Force
U.S.C. United States Code
USPS United States Postal Service

Terms

Certificate A record holding security information about an information system user and vouches to the truth and accuracy of the information it contains. A public key certificate contains the name of a user, the public key component of the user, and the identity of the user who vouches that the public key component is bound to the named user. **NOTE:** A public key certificate is normally issued to individuals. When several individuals act in one capacity for an organization, an “organizational certificate” may be issued with the identity of the organization.

Certificate Revocation List (CRL) A list of invalid certificates that have been revoked by the issuer. It is periodically issued by each certification authority and posted to the directory.

Certification Authority (CA) A person responsible for issuing and revoking user certificates, and exacting compliance with the PKI policy as defined by the parent Policy Creation Authority. **NOTE:** The term CA refers to both the authoritative office and role, and the incumbent in that office. The CA is the third level in the PKI Certificate Management Infrastructure (CMI).

Certification Authority Workstation (CAW) Commercial-off-the-shelf (COTS) workstation with a trusted operating system and special-purpose application software. The CAW programs KOV-11s with a user's security personality including certificates and cryptographic key. The CA operates the CAW.

Compromised Key List (CKL) A list generated by a PCA that contains the Key Material Identifiers (KMID) of keys believed by the PCA to be compromised (i.e., that can no longer be trusted).

CRYPTO Marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive US Government-derived information.

Designated Approving Authority (DAA) Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

Directory An on-line repository of certificates, CRLs, and CKLs.

Distinguished Name (DN) An identifier, unique to a given PKI CMI that represents an individual's identity.

Enclave A general computing term used to describe an interconnected collection of some subset of an organization's local computing resources. An enclave is often comprised of heterogeneous platforms that operate in a multi-protocol environment sharing common characteristics. These characteristics may include, but are not limited to common ownership/management, common mission, definable physical boundary, common security policy, controllable access point(s) to the enclave, and heterogeneous levels of trust.

FORTEZZA Card A personal computer card that uses algorithms and procedures approved by the National Institute of Standards and Technology (NIST) and NSA to provide network related security services. Also identified as the KOV-11. The card, when used in conjunction with the proper applications and network infrastructure, provides data integrity, access control, authentication, nonrepudiation and confidentiality of user information. **NOTE:** When the term KOV-11 is used, it is referring to both the FORTEZZA card (used to protect sensitive information) and the FORTEZZA for Classified (FFC) card.

FORTEZZA-enabled Application Any software application that has been designed (or enabled) to use FORTEZZA cryptography when providing security services. This can be client software running locally on a user's workstation (e.g., File Transfer Protocol (FTP) clients, electronic mail clients, web browsers) or server software running unattended on a server (e.g., FTP servers, web servers, Directory System Agents).

Information Systems Security Officer (ISSO) Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal.

Infrastructure Components Components that provide connectivity to the backbone, provide management, control, security, and message transfer/conversion/expansion services to the site system and are required for the user components to function.

Locked The KOV-11 is locked when it is not in a computer.

Key Material Identifier (KMID) The KMID is a unique field contained in an X.509 certificate that identifies a specific set of private key material. The KMID is unique within the Policy Approving Authority (PAA) hierarchy.

Need-to-know The necessity for access to, or knowledge or possession of, specific information required in performing official duties.

Personal Computer Memory Card International Association (PCMCIA) Card The FORTEZZA cryptographic card is a peripheral that contains the processor, algorithms, and cryptographic material necessary to support personalized security services.

Personal Identification Number (PIN) A random character string that unlocks and activates the KOV-11.

Public Key Infrastructure (PKI) Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.

Sensitive Information Any information that the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national security interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy. The responsibility for determining the applicability of the handling caveat or warning notice lies with the originating organization. (Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of Title 10 United States Code (U.S.C), Section 2224 (Defense Information Assurance Program).

System Administrator (SA) Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

Type 1 Product Classified or controlled cryptographic item endorsed by NSA for securing classified and sensitive US Government information, when appropriately keyed. The term refers only to products, not to information, key, services, or controls. Type 1 products contain classified NSA algorithms. They are available to US Government users, their contractors, and federally sponsored non-US Government activities subject to export restriction in accordance with International Traffic in Arms Regulation.

Type 2 Product Unclassified cryptographic equipment, assembly, or component, endorsed by NSA, for use in national security systems as defined in Title 40 U.S.C. Section 1452, *Public Building, Property, and Works*.

Unlocked The KOV-11 is unlocked when it is in a computer and the PIN entered (activated).

Attachment 3

FORTEZZA USER TRAINING

NOTE: When the term KOV-11 is used, it is referring to both the FORTEZZA card (used to protect sensitive information) and the FFC card (used to protect SECRET information).

1. A locked KOV-11 (*i.e., a card that is not in use*) is considered unclassified. When the KOV-11 is in the terminal in the unlocked mode (*KOV-11 in the terminal and PIN activated*), afford protection commensurate with the highest level of the key it contains and ensure use only by the authorized individual.
2. When unauthorized personnel are in the area, discontinue the processing of sensitive or classified information on the terminal. Pay strict attention to the authorized classification level of the KOV-11 and ensure transmission does not exceed the highest authorized classification. To prevent possible unauthorized use never leave a terminal unattended after the PIN has been successfully entered into the KOV-11 and the FORTEZZA-enabled software available for use. Lockscreens and screensavers are not acceptable means to protect an unlocked KOV-11. Do not leave a FFC card in a terminal unattended. Remove KOV-11s from their card readers when they are not actively in use for message origination or reception.
3. When not in use, protect KOV-11s in a manner similar to a credit card or high value item to limit the possibility of loss, unauthorized use, substitution, tampering, or breakage. The KOV-11 must be in the user's possession at all times. When sleeping, protect the KOV-11 as you would your money, credit cards, and other valuables.

4. Memorize the PIN. Do not write the PIN on the KOV-11 card or record it in any manner in the vicinity of the host system for any reason. Do not share the PIN for individual cards. The PIN for a KOV-11 is unclassified. For FORTEZZA cards, securely store the PIN or PIN letter separate from the card to prevent loss or unauthorized access. For FFC cards, record the PIN on a SF 700, **Security Container Information**, and store in a GSA-approved container. Destroy the PIN letter as classified waste. An alternative to the SF 700 would be to store the PIN in a sealed opaque envelope with initials over the envelope's seal in such a way that tampering will be obvious.

5. Maintain an access list of authorized users of the organizational card. A custody log for the KOV-11 will be maintained when sharing the PIN for organizational cards and duplicate cards for infrastructure components.

6. Users are responsible for the proper safekeeping and immediate reporting of its loss, destruction, theft, or tampering. Notify the FRO immediately if an FFC card is left in an unattended terminal or a KOV-11 or its PIN is compromised.

7. In the event of fire, natural disaster, or covert threat, remove the KOV-11 from the terminal and secure it or keep it in the possession of the authorized user.

(Printed/Typed Name of User)

(Signature of User)

(Printed/Typed Name of Trainer)

(Signature of Trainer)

(Modify this training list for your location)