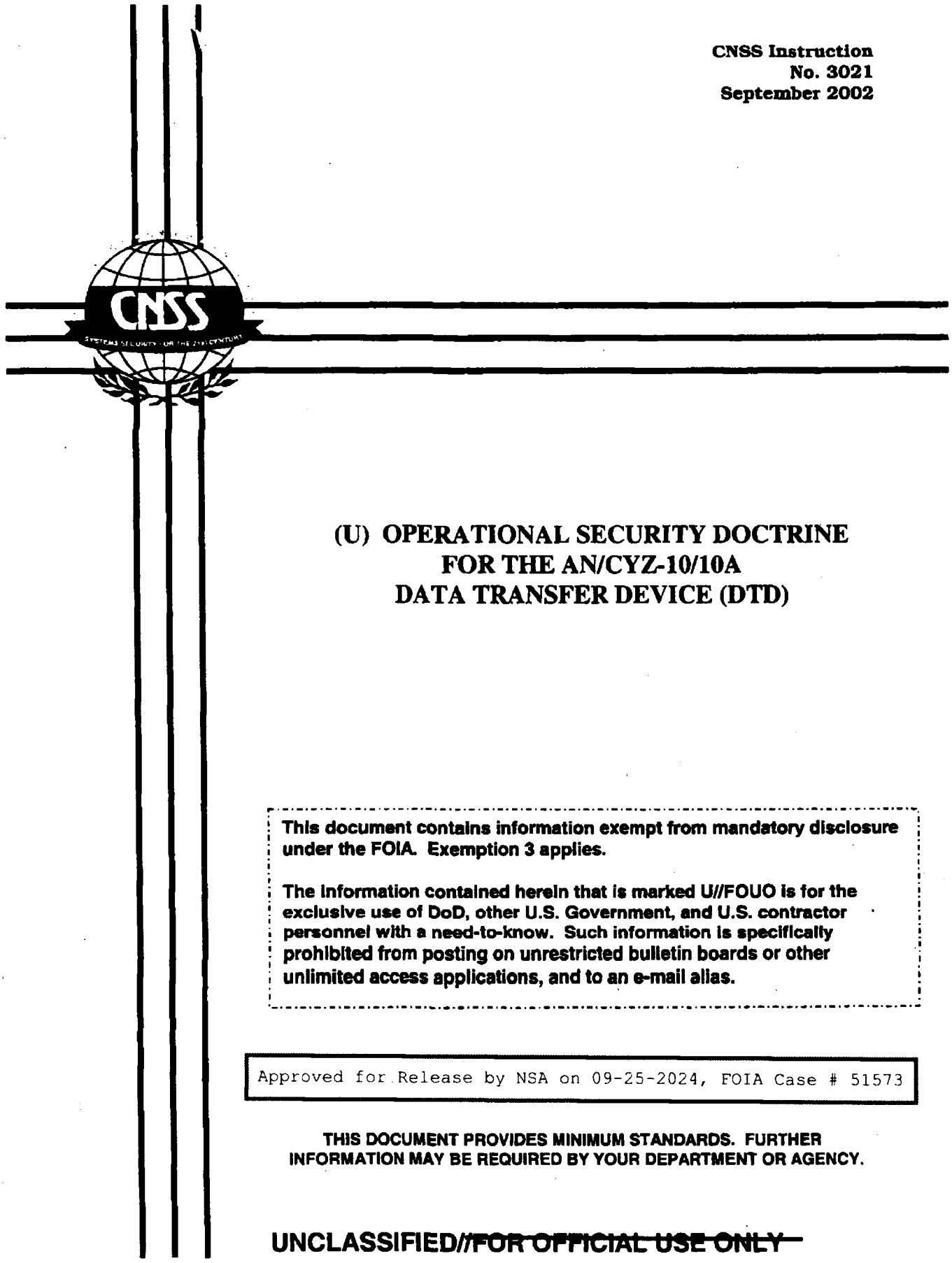


CNSS Instruction
No. 3021
September 2002

(U) OPERATIONAL SECURITY DOCTRINE FOR THE AN/CYZ-10/10A DATA TRANSFER DEVICE (DTD)

CNSS INSTRUCTION
No. 3021

Committee on National Security Systems

National Manager

FOREWORD

1. (U) This Instruction provides minimum security standards for the protection and use of the AN/CYZ-10/10A Data Transfer Device (DTD) and associated Communications Security (COMSEC) material. Please check with your department or agency for applicable implementing documents.

2. (U) This Instruction supersedes NSTISSI No. 3021, Operational Security Doctrine for the AN/CYZ-10/10A DTD, dated September 1998.

3. (U) Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this Instruction from the address listed below.

4. (U) U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

5. (U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

MICHAEL V. HAYDEN
Lieutenant General, USAF

CNSS Secretariat [redacted]. National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716

CNSS INSTRUCTION
No. 3021

(U) OPERATIONAL SECURITY DOCTRINE FOR THE AN/CYZ-10/10A DATA TRANSFER DEVICE (DTD)

(U) SECTION I - PURPOSE AND SCOPE

1. (U) Purpose - This Instruction contains minimum security standards for the protection and use of the AN/CYZ-10/10A DTD, and its associated components and Communications Security (COMSEC) material.

2. (U) Application - The provisions of this doctrine apply to all departments and agencies of the U.S. Government and their contractors who handle, distribute, account for, store, use, or dispose of the DTD and associated COMSEC material.

3. (U) Doctrinal Conflicts - Any conflicts between the requirements contained in this doctrine and any other national-level publication should be identified and submitted for resolution to the Director, National Security Agency (DIRNSA), Information Assurance Policy, Procedures and Insecurities Division. However, this does not preclude any department or agency of the U.S. Government from applying more stringent security measures to their equipment than this doctrine requires.

(U) SECTION II – REFERENCES

4. (U) This doctrine makes reference to a number of other national-level documents. A listing of these documents is contained in ANNEX A.

(U) SECTION III – DEFINITIONS

5. (U) Definitions and acronyms contained in Reference a apply to this doctrine. Additional definitions of specialized terms that are unique to this doctrine are contained in ANNEX B.

(U) SECTION IV – EQUIPMENT/SYSTEM DESCRIPTION/LEVEL OF USE

6. (U//~~FOUO~~)

7. (U//~~FOUO~~)

8. (U//~~FOUO~~)

9. (U//~~FOUO~~)

(U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

10. (U//~~FOUO~~)

(U) SECTION V – KEYING INFORMATION

11. (U) Controlling Authority – Reference b describes the responsibilities of organizations that serve as Controlling Authorities for COMSEC keying material and provides guidance for fulfilling those responsibilities.

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

12. (U) Local Key Encryption Key (LKEK)

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

13. (U) CIK

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

(1) (U//~~FOUO~~)

(2) (U//~~FOUO~~)

d. (U//~~FOUO~~)

e. (U//~~FOUO~~)

(U//~~FOUO~~)

14. (U) Transfer Key Encryption Key (TrKEK)

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

d. (U) Cryptoperiod

(1) (U//~~FOUO~~)

(2) (U//~~FOUO~~)

(U//~~FOUO~~)

15. (U//~~FOUO~~)

(U) SECTION VI - CLASSIFICATION

16. (U//~~FOUO~~)

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

c. (U) Data Transfer Classification

(1) (U//~~FOUO~~)

(2) (U//~~FOUO~~)

d. (U//~~FOUO~~)

17. (U//~~FOUO~~)

18. (U//~~FOUO~~)

19. (U) Audit Data – After review by supervisory personnel, audit data uploaded to an information system (IS) may be declassified.

20. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(U) SECTION VII - CONTROL REQUIREMENTS

21. (U) DTD

a. (U) Physical Security – Each user shall regularly verify the serial number on the DTD case for correctness. Also, the physical integrity of the DTD housing shall be regularly checked for any security breaches.

b. (U//~~FOUO~~)

(1) (U) Single segment loading of the key, per short title, with the unused segments remaining in the canister until they become effective.

(2) (U) Full canister (edition) per short title of keying material, to be loaded into the DTD at one time.

(U) NOTE: This is permitted with the understanding that the Controlling Authority accepts the risk of having to supersede an entire edition of keying material if a compromise occurs.

(3) (U) No more than one canister of keying material (per short title), not to exceed twelve months and one spare month of keying material, shall be held in a DTD at any given time.

(4) (U) The only exception to the "one canister" rule per DTD is that the follow-on canister of keying material can be loaded into the DTD at any time during the final month prior to the current edition being superseded.

(5) (U) Canisters containing key and segments extracted from the canister shall be secured to the level of classification of the key until the segment or canister is superseded, at which time they shall be destroyed. Retaining the segments outside of the canister is not recommended.

(6) (U) Physical keying material loaded into a DTD may be transferred from the DTD to the LMD/KP and stored there until supersession, to be reissued to the DTD if necessary. For accounts without reasonable access to an LMD/KP, a backup canister may be stored but should be avoided if possible.

(U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

c. (U) Loading Electronic Key – Refer to Section IX – Transferring COMSEC Key, for guidance on loading electronic key into the DTD.

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

d. (U) Audit Data

(1) (U//~~FOUO~~) [redacted]

(a) (U) Mandatory Minimum DTD Auditable Events that shall be reviewed:

- (U) Alarm event entry
- (U) Audit trail full
- (U) Audit trail initialization
- (U) Audit upload
- (U) CIK initialized
- (U) Connection to a device
- (U) Date change
- (U) Time change
- (U) DTD zeroized
- (U) Key file received
- (U) Key file transferred
- (U) Key received
- (U) Key transmitted

- (U) Key zeroized (destroyed)
- (U) DTD serial number change

(b) (U) Recommended DTD Auditable Events:

- (U) CIKs properly secured when not in use
- (U) Proper accounting procedures for the DTD

(2) (U//~~FOUO~~)

(3) (U//~~FOUO~~)

e. (U) Key Accounting and Inventory

(1) (U//~~FOUO~~)

(2) (U//~~FOUO~~)

f. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

22. (U) CIK

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

d. (U//~~FOUO~~)

e. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(U) SECTION VIII – RISK FACTORS/SECURITY MEASURES

23. (U) DTD Risk – The risk to the DTD, the keys and information contained in the DTD, and to the information these keys secure can vary drastically. When the risk is higher, additional restrictions on the DTD must be implemented beyond the minimum security requirements stated below.

24. (U//~~FOUO~~)

- (U)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)

25. (U) Additional Security Measures – Depending on the level of risk, the following additional security measures are added to the minimum security requirements. The measures are cumulative (i.e., each successive group includes those listed previously).

a. (U) LOW RISK – Follow minimum security requirements.

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

d. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

26. (U) Risk Minimization – To minimize the necessity for applying additional security restrictions, user organizations should consider the following recommendations to reduce the level of risk:

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

(U) SECTION IX - TRANSFERRING COMSEC KEY

27. (U//~~FOUO~~)

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

CAUTION: (U//~~FOUO~~)

28. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

29. (U//~~FOUO~~)

(U) SECTION X - MAINTENANCE

30. (U//~~FOUO~~)

31. (U//~~FOUO~~)

(U) SECTION XI – DISPOSITION/DESTRUCTION

32. (U//~~FOUO~~)

33. (U//~~FOUO~~)

34. (U//~~FOUO~~)

35. (U//~~FOUO~~)

36. (U//~~FOUO~~)

(U) SECTION XII – REPORTABLE COMSEC INCIDENTS/ INSECURE PRACTICES

37. (U) DTD

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

38. (U//~~FOUO~~)

39. (U//~~FOUO~~)

a. (U)

b. (U)

c. (U//~~FOUO~~)

d. (U)

e. (U//~~FOUO~~)

f. (U)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

g. (U)

h. (U)

i. (U)

(U//~~FOUO~~)

40. (U//~~FOUO~~)

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

(U) SECTION XIII – EXCEPTIONS

41. (U) Waivers - Requests for exceptions to the provisions of this doctrine must be approved, on a case-by-case basis, prior to implementation. Each request must include a complete operational justification and shall be submitted through command channels to DIRNSA, Information Assurance Policy, Procedures and Insecurities Division for review. Accounting related issues concerning the DTD shall be resolved within department/agency channels.

3 Encls:

ANNEX A - References
ANNEX B – Definitions and Acronyms
ANNEX C – DTD Routine Demilitarization/Destruction

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

ANNEX A

(U) REFERENCES

(U) The following national-level documents are referenced in this doctrine or are otherwise applicable for U.S. Government departments and agencies:

a. (U) NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated September 2000.

b. (U) NSTISSI No. 4006, Controlling Authorities for COMSEC Material, dated 2 December 1991.

c. (U) NSTISSI No. 4005, Safeguarding COMSEC Facilities and Material, dated August 1997.

d. (U) NSTISSI No. 4001, Controlled Cryptographic Items, dated July 1996.

e. (U) NSTISSI No. 4000, Communications Security Equipment Maintenance and Maintenance Training, dated January 1998.

f. (U) NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987.

g. (U) NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991.

(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

ANNEX B

(U) DEFINITIONS AND ACRONYMS

1. (U) Definitions - The following definitions apply to this doctrine:

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

d. (U//~~FOUO~~)

e. (U//~~FOUO~~)

f. (U//~~FOUO~~)

g. (U//~~FOUO~~)

h. (U//~~FOUO~~)

i. (U//~~FOUO~~)

j. (U//~~FOUO~~)

k. (U//~~FOUO~~)

l. (U//~~FOUO~~)

m. (U//~~FOUO~~)

n. (U//~~FOUO~~)

o. (U//~~FOUO~~)

p. (U//~~FOUO~~)

q. (U//~~FOUO~~)

2. (U) Acronyms – The following acronymns are used in this document:

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Acronym	Expansion
CCI	Controlled Cryptographic Item
CIK	Crypto-Ignition Key
COMSEC	Communications Security
COR	Central Office of Record
DIRNSA	Director, National Security Agency
DTD	Data Transfer Device
EKMS	Electronic Key Management System
INFOSEC	Information Systems Security
KEK	Key Encryption Key
LKEK	Local Key Encryption Key
LMD/KP	Local Management Device/Key Processor
NATO	North Atlantic Treaty Organization
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
STE	Secure Terminal Equipment
STU	Secure Telephone Unit
TrKEK	Transfer Key Encryption Key
UAS	User Application Software

ANNEX C

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(U) DTD Routine Demilitarization/Destruction

1. (U) Who May Perform Routine Demilitarization/Destruction?

a. (U) MILITARY – Demilitarization/destruction generally is performed by the Service element, e.g., Tobyhanna Army Depot.

b. (U) CONTRACTORS – If the DTD is Government Furnished Equipment (GFE), return it per your contract or to the activity from which it was acquired. If contractor-owned, go to 2.b. below.

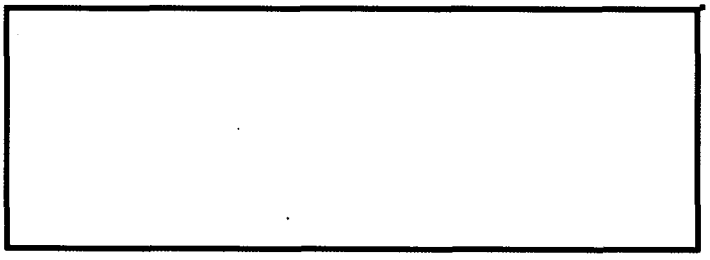
2. (U) Demilitarization

a. (U) Determine if equipment can be re-used. Check with the local Asset Recovery Office. If no local or Service use is found for the equipment, contact the National Reserve Program on 410-854-6154, to see if they need to acquire the equipment.

b. (U) Demilitarize the equipment:

(U//~~FOUO~~)

c. (U//~~FOUO~~)



(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

d. (U) Dispose of equipment hulk:

(1) (U) Military: Return equipment hulk to a Defense Reutilization Marketing Office (DRMO). If DRMO does not want the hulk, destroy locally (according to local trash disposal ordinances).

(2) (U) Contractor: locally destroy in a proper manner.

(U) NOTE: While not required, it is recommended that the remaining hulk be smashed prior to disposal.

(U//~~FOUO~~)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DISTRIBUTION:

[redacted]

(b)(3)-P.L. 86-36