DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5530.1
N6
15 Sep 2014

CNATRA INSTRUCTION 5530.1

Subj: CHIEF OF NAVAL AIR TRAINING AND NAVAL AIR TRAINING COMMAND DATA COMMUNICATION SPACES LOCK AND KEY CONTROL PROGRAM

Ref: (a) OPNAVINST 5530.14E
(b) SECNAV M-5510.30
(c) SECNAV M-5510.36A
(d) NAVFAC UG-2040-SHR
(e) SECNAV Manual 5210.1

Encl: (1) Controlled Key Inventory
(2) DATACOM Space Custodian Designation Letter
(3) N6 Departmental Key Custodian Letter
(4) Key Issue Record Form
(5) Lost Key Statement/Request for Replacement Locking Device
(6) Data Communication Space Spot Check Form

1. Purpose. To promulgate a Lock Control Program for all controlled locking devices used to meet security and loss prevention objectives per references (a) through (d) for Chief of Naval Air Training (CNATRA) and Naval Air Training Command (NATRACOM) Data Communication (DATACOM) Spaces, to include, server rooms, wiring and telecommunication closets and any space specifically designed or utilized for telecommunications cabling and network infrastructure.

2. Controlled Locking Devices. All keys, locks, padlocks, and locking devices used to meet security and loss prevention objectives. See Controlled Key Inventory form, enclosure (1).

3. Responsibilities

a. CNATRA Chief Information Officer. The CNATRA Chief Information Officer (CIO) manages and supervises the NATRACOM DATACOM Lock Control Program.

b. Primary DATACOM Space Custodian - Lead System Support Specialist (LSSS). The DATACOM Space Custodian will be assigned to the CNATRA N61 Department and is responsible for the security of all data communication closets within CNATRA and NATRACOM Spaces. The Primary DATCOM Space Custodian will be assigned via a designation letter, enclosure (2). Specific duties include:

(1) Ensure adequate locking devices are used for areas requiring greater degree of security per reference (c).

(2) Maintain/manage those personnel authorized to have access to any CNATRA/NATRACOM DATACOM space. Update applicable access lists and visitor logs as well as SF-702 forms on all restricted spaces.

(3) Maintain control of the master cipher lock combination codes and master keys for all locking devices in their purview.

(4) Control access to NATRACOM designated RESTRICTED Spaces.

(5) Change all combinations as directed.

(6) Ensure restricted spaces are protected after-hours.

(7) Ensure all locking devices are functioning correctly.

c. Secondary DATACOM Space Custodian - Information Technology Point of Contact (ITPOC). The ITPOC will be a backup to the LSSS DATACOM Space Custodian. The Secondary DATCOM Space Custodian will be assigned via a designation letter, enclosure (2). Specific duties include:

(1) Act as backup to the Primary DATACOM Space Custodian.

(2) Maintain all logs and cipher combinations in a GSA approved storage container.

(3) Verify combinations are changed as directed.

d. CNATRA N6 Departmental Key Custodian(s). N6 Department Key Custodian(s) will be a CNATRA N6 employee located in Building 10. The Departmental Key Custodian will be assigned via a designation letter, enclosure (3). Specific Duties include:

(1) Conduct quarterly inventory of assigned controlled keys for designated areas of security interest.

(2) Sub-custody controlled keys as requested by department and approved by CIO. Maintain accountability for assigned keys.

(3) Maintain key control log to document issuance of controlled keys.

(4) Maintain and investigate all Lost Key Statements.

e. Program Auditor - Information Assurance Officer (IAO). The Program auditor is responsible for verifying that all physical security protection is implemented correctly and all assets are protected to the highest extent possible. Specific duties include:

(1) Conduct random space walk-through to ensure that all restricted spaces are properly labeled, locked and controlled via access lists and visitor logs.

(2) Ensure all locks are fully operational, all doors are closed when spaces are not occupied and not propped open for any reason.

f. Key User. The key user is anyone that is authorized to have the keys or codes to locks in their organization. They are responsible for protecting their issued key(s) as well as the spaces that the locks are protecting. They must report any issues, upon discovery, to the Primary DATACOM Space Custodian for immediate attention. The Key User must ensure that they prevent others from looking over their shoulders when accessing any of the restricted spaces to prevent theft of the codes. They must report to the DATACOM Space Custodian, immediately, if there are suspicious people loitering around secured spaces.

4. Procedures

a. Central Storage. All key codes for N6 cipher locks for CNATRA and NATRACOM DATACOM Spaces will be stored at CNATRA N6 Corpus Christi, Building 10.

b. Key Storage. A site specific SF-700 form will contain the key codes for all cipher protected rooms at each NATRACOM site. A GSA approved safe is maintained at CNATRA N6 Office Spaces for the storage of the SF-700 forms until the codes are changed at their appropriate time. Key code information will be treated in the same manner as classified documents. No unauthorized viewing or copying of code information will be allowed.

All physical keys will be maintained in an approved locking storage box with the appropriate logs associated and managed by the N6 Departmental Key Custodian.

c. Controlled Key Issuance. Key codes for cipher locks and physical keys for doors will be issued to those individuals with a need to know and who have met the approved access requirements. The DATACOM Space Custodian will rigidly control access to all restricted spaces and who will be issued cipher combinations. All physical keys issued will be documented on the Key Issue Form in enclosure (3) and maintained by the N6 Departmental Key Custodian for inventory purposes.

d. Lost, Forgotten or Stolen Keys and Codes. In the event of such occurrences, the DATACOM Space Custodian will be notified immediately. Protection of these keys is vital to the physical security of the devices within the DATACOM spaces. It is the Key Users responsibility to protect keys and codes in every way possible. Cipher codes are not to be written down and shared with others. When unlocking a space, it is the user’s responsibility to position their bodies in such a way as to prevent any issues of “shoulder-surfing” by anyone in the area. If a key or code is stolen a Lost Key Statement/Request for Replacement Locking Device Form, enclosure (4) must be filed with the Primary DATACOM Space Custodian as well as with the N6 Departmental Key Custodian for their records prior to code or key replacement.

e. Procurement of Locks. All locks will meet the minimum military specifications for the level of security use. Personnel requiring locks shall contact N6 CIO. N6 will order all locks and will prepare a list of approved locks from which replacements are ordered.

f. Lockouts. All lockouts involving restricted areas must be investigated by the Primary DATACOM Space Custodian and the Program Auditor to determine if the failure of the locking device occurred because of product failure or as a result of illegal entry attempt. A report of the lockout and the corrective actions shall be reported to the CIO, Site Security Manager, and Commanding Officer.

g. Daily Restricted Space Lock Control. The Primary DATACOM Space Custodian will ensure that all restricted communication spaces are secured after each visit and at the end of the day. A SF-702 form will be posted on the entrance to the restricted space. Any personnel who enter will need to document date and time they entered and left. Personnel must ensure the door is securely locked after they leave.

h. After Hours Entrance. The DATACOM Space Custodian will verify that the individual has a legitimate need to access secured spaces after hours. If the request is legitimate, the DATCOM Space Custodian will ensure the visitors log captures the names of individuals requiring access to locked spaces.

i. Key Code Changes. The Primary DATACOM Space Custodian will be responsible for changing the key codes on all cipher locking devices on a dictated schedule. Key codes will also be changed after an employee that has knowledge of the key codes departs. Code change reports will be submitted via encrypted email to CNATRA N61 for appropriate documentation and GSA storage. All physical keys issued to an N6 employee will be turned over to the N6 Departmental Key Custodian upon employee departure from N6 Department.

j. Auditing. The site IAO will be responsible for making random stops at CNATRA/NATRACOM maintained DATACOM spaces to ensure all security measures are in place. The IAO will verify that the locking mechanism is functioning properly, the door is closed and locked when it is unoccupied and that the door is never propped open for any reason. They will randomly inspect

the access list and the visitor's logs for proper recording of entry and exit. The SF-702 form will also be spot-checked for appropriate documentation.

Auditors will use the Data Communication Space Spot Check form, enclosure (5), for recording inspected spaces. Discrepancies must be reported to the ITPOC and Information Assurance Manager (IAM) immediately for remediation. Both the auditor and ITPOC are required to sign the Data Communication Space Spot Check form. The completed forms will be scanned and emailed to the IAM/A-IAM for records management. The original form will be maintained onsite for a minimum of one year.

5. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of January 2012.

D. M. EDGECOMB
Chief of Staff

Distribution:
CNATRA Website
CNATRA SharePoint

Controlled Key Inventory

Directorate: Date

Key Custodian: Page of

Name of Key Holder (Last, First MI.)	Key Number (Found on key)	Bldg.	Room	Any other locking device on door. (XO9, Cipher, etc.)

Enclosure (1)

CNATRAINST 5530.1
15 Sep 2014

Date

From: CIO, Chief Naval Air Training
To: _____

Subj: DESIGNATION AS CHIEF OF NAVAL AIR TRAINING DATA COMMUNICATIONS SPACE CUSTODIAN

Ref: (a) CNATRAINST 5530.1

1. Per reference (a), you are hereby designated as the **PRIMARY/ALTERNATE** CNATRA Data Communications Space Custodian.

2. In the performance of this duty, you shall become thoroughly familiar with reference (a) and other security directives which pertain to this appointment.

3. Specific duties of the Primary CNATRA Data Communications Space Custodian include:

a. Ensure adequate locking devices are used for areas requiring greater degree of security.

b. Maintain/manage those personnel authorized to have access to any CNATRA/NATRACOM Data communication space; Updating applicable access lists and visitor logs as well as SF-702 forms on all restricted spaces.

c. Maintain control of the master cipher lock combination codes for all locking devices in their purview.

d. Control access to NATRACOM designated RESTRICTED Spaces.

e. Change all combinations as directed.

f. Ensure restricted spaces are protected after-hours.

g. Ensure all locking devices are functioning correctly.

CNATRA CIO

Enclosure (2)

Date

From: CIO, Chief Naval Air Training
To: _____

Subj: DESIGNATION AS N6 DEPARTMENTAL KEY CUSTODIAN

Ref: (a) CNATRAINST 5530.1

1. Per Reference (a), you are hereby designated as the N6 Departmental Key Custodian.

2. In the performance of this duty, you shall become thoroughly familiar with Reference (a) and other security directives which pertain to this appointment.

3. Specific duties of the N6 Departmental Key Custodian include:

a. Conduct quarterly inventory of assigned controlled keys for designated areas of security interest.

b. Sub-custody controlled keys as requested by department and approved by CIO. Maintain accountability for assigned keys.

c. Maintain key control log to document issuance of controlled keys.

d. Maintain and investigate all Lost Key Statements.

CNATRA CIO

KEY ISSUE RECORD		
From:	To: N6 Department Key Custodian	Date:
Request that:		
NAME	GRADE	Employee/Military Number
Be issued _____ key(s) to the following area(s): (Identify building number, floor and room number, container, cage, or section, as applicable		
From	To: N6 Department Key Custodian	Date:

STATEMENT OF ACKNOWLEDGEMENT OF RECEIPT OF KEY

I understand that keys issued to me provide access to the space listed above. Additionally, I have read and am familiar with the CNATRA and NATRACOM Data Communications Spaces Lock and Key Control Program and understand that the following provisions apply:

a. Duplication of keys is not approved unless express written consent from the CIO.

b. Keys must remain in my possession at all times and may not be loaned

c. Upon my transfer or reassignment, the keys must be turned into the department Key Custodian

d. Loss of keys must be reported to the key custodian immediately.

e. It is my responsibility to ensure that all spaces to which I have keys are locked at the end of the day.

f. Keys are the property of the U.S. Government.

g. A key code is not to be shared with anyone, every effort must be taken to prevent "shoulder surfing"

Signature: _____

Lost Key Statement/Request
for Replacement Locking Device

Date: _____

Directorate: _____

Name of Key Holder: _____

Date and Time Key(s) Last Seen: _____

Date and Time Key(s) Realized Missing: _____

Last Known Place Key(s) Last Seen: _____

Space(s) affected By Loss of Key(s) (Bldg., Room): _____

Brief description of what you were doing between the times the key(s) was last seen and when the key was noticed missing:

_____

_____

_____

_____

_____

_____

_____ _____
Signature Date

_____ _____
Key Custodian Date

_____ _____
Primary DATACOM Custodian Date

* Note: All requests for issuance of keys must first be approved by the CIO.

Data Communication Space Spot Check

Command:	Date:
Building:	
Room:	

YES ☐	NO ☐	Is locking device operational?
YES ☐	NO ☐	Is door closed securely?
YES ☐	NO ☐	Is visitors log filled out correctly?
YES ☐	NO ☐	SF-702 updated as required?

Comments:

Auditors Signature	Date
ITPOC Signature	Date