For copies of the additional NSA reference materials mentioned in this brief, Please send email requests to:  Heather.Dunn@lmco.com
CRYPTOGRAPHY (Cryptology)

- κρυπτός “Hidden, Secret”
- Graphein “Writing” Or
- -logia “Study”
COMSEC

- Protection of electronically transmitted classified and sensitive information
- Ensures authenticity of US National Security electronic information transmission
- NSA (National Security Agency) primary US Government Agency responsible for COMSEC
COMSEC

- May be classified or unclassified

- May be applied to:
  - Documents
  - Information
  - Hardware (equipment)
COMSEC

- Governed by the NSA 3-16
  - Newly Issued NSA 3-16 in January 2015
    - References Appendixes in place of..... Everything
    - Pro’s: Smaller NSA 3-16 and access to elusive doctrine
    - Con’s: Now we HAVE to follow elusive doctrine
COMSEC

INFOSEC Policy and Doctrine Division of NSA

- CNSS(I) stands for Committee on National Security Systems (Issuance)

- NSTISS(I) stands for National Security Telecommunications and Information Systems Security (Issuance)
COMSEC

- General Components of the program
  - Transmission Security
  - Emission Security
  - Cryptographic Security
  - Physical Security
COMSEC ACCESS

- CCI - Controlled Cryptographic Item aka Hardware
  - Unkeyed CCI required safeguarding equal to “Sensitive material”
  - Security clearance not required for unkeyed CCI

- CRYPTO - Cryptographic aka KEY
What’s What of COMSEC

- COMSEC vs CCI vs CRYPTOGRAPHIC
What’s What of COMSEC

- COMSEC vs CCI vs CRYPTOGRAPHIC
Cryptographic ACCESS

- UNCLASSIFIED COMSEC and CCI Access requirements
  - Brief + Need to Know + U.S. Citizenship

- CLASSIFIED COMSEC Access requirements.
  - Brief + Need to Know + U.S. Citizenship + Final Clearance
    - US Government granted security clearance to the appropriate level and Need to Know
COMSEC ACCESS

- Cryptographic aka KEY
  - CRYPTO Brief + Need to Know + U.S. Citizenship + Final Clearance
    - A separate/additional Cryptographic brief is required
    - US Government granted security clearance to the appropriate level and Need to Know
COMSEC

Simple Key Loader or SKL
(AN/PYQ-10)

Electronic Transfer Device or KYK-13
(KYK-13)

Hand Held Paper Tape Reader
(KOI-18)

Data Transfer Device or CYZ-10
(AN/CYZ-10)

TACLANE-Micro
(KG-175D)
KG-175G

Left: PLGR
(Right: DAGR)
The briefing must, at a minimum, include the parts of the contractor's Standard Operating Procedure (SOP) addressing the sensitivity of the material; the rules for safeguarding such material; the laws pertaining to espionage; the procedures for reporting COMSEC incidents; and the rules pertaining to foreign contacts, visits, and travel.

**NEW! NSA 3-16 SECTION III 14.a.c.1**

The SOP must include a preparation/creation date and must be reviewed and updated annually thereafter.
NEW! NSA 3-16 SECTION IV 24.b.1.b

24. (U) COMSEC Material Control System: Forms, Files, and Reports. 1) (U) Accounting Files:

b) (U) All COMSEC correspondence that includes but is not limited to: COMSEC Account Manager, Alternate COMSEC Account Manager, and FSO appointment confirmation letters; memoranda; messages; disposition records; emails; and other documentation related to COMSEC accounting.
NEW! NSA 3-16 SECTION IV.29.b

(U) COMSEC Account Managers of contractor accounts are required to submit to their NSA/CSS COR Account Managers with their semiannual inventories all contract specifications (DD Form 254 and if appropriate, an MOU/MOA/Framework Agreement) held by the account that require access to COMSEC information, and their associated expiration or contract review dates.

VS old: Where applicable (contractors), have access to a copy of the DD Form 254, and ensure compliance with the specification.

NSA 3-16 SECTION IV.26

Hand receipting COMSEC material between COMSEC Accounts is prohibited.
The COMSEC Account Manager will notify the mail and receiving departments that a COMSEC Account has been established and provide them with specific internal address instructions so that COMSEC mail or COMSEC material received for the COMSEC Account will be \textit{forwarded unopened} to the COMSEC Account Manager.

\begin{itemize}
  \item See Template provided
\end{itemize}

\textbf{NEW! NSA 3-16 SECTION IV 34.a}

Shipping COMSEC material to an individual and not a COMSEC or DoDAAC Account is not authorized and \textit{is reportable as an incident} in accordance with Section XI of this manual.
NEW! NSA 3-16 SECTION VII 46.b

a. (U) Protective Packaging of Lock Combinations. Lock combinations should be packaged and sealed in special commercially-available tamper-indicating envelopes. The protective packaging should be inspected at least monthly.

b. (U) Protective Packaging Techniques. Guidance for one method (other methods may be equally acceptable) for protective packaging is as follows:

1) (U) Lock combination record cards may be protectively packaged by covering the record card front and back with aluminum foil. Place the lock combination record card into an opaque envelope. On the face of the envelope, mark the highest classification of the information protected by the combination, the number of containers to which the combination applies, the identification number of the safe, and the date the combination was changed. These entries must be made in ink to lessen the possibility of alteration.

2) (U) Place the envelope in a tamper-proof plastic bag and seal according to instructions. The tamper-proof plastic bags are available from the NSA/CSS Physical Assurance Engineering Division ((301) 688-5861).
NEW! NSA 3-16 SECTION VII 46.b

a. (U) Protective Packaging of Lock Combinations. Lock combinations should be packaged and sealed in special commercially-available tamper-indicating envelopes. The protective packaging should be inspected at least monthly.

b. (U) Protective Packaging Techniques. Guidance for one method (other methods may be equally acceptable) for protective packaging is as follows:

1) (U) Lock combination record cards may be protectively packaged by covering the record card front and back with aluminum foil. Place the lock combination record card into an opaque envelope. On the face of the envelope, mark the highest classification of the information protected by the combination, the number of containers to which the combination applies, the identification number of the safe, and the date the combination was changed. These entries must be made in ink to lessen the possibility of alteration.

2) (U) Place the envelope in a tamper-proof plastic bag and seal according to instructions. The tamper-proof plastic bags are available from the NSA/CSS Physical Assurance Engineering Division ((301) 688-5861).

VS old: NOTE: (U) In those instances where only the COMSEC Custodian, Alternate COMSEC Custodian, and FSO (if applicable) have access to the central container, only the records for TOP SECRET keying material require protective packaging.
CNSSI 4005 bits and bobs

- CNSSI 4005 SECTION VII.50.d
  - 50. (U) Record of Combinations
d. (U) It is specifically prohibited for individuals to record and carry, or store insecurely for personal convenience, the combinations to facilities or containers where COMSEC material is stored. Records of such combinations may not be stored in electronic form in a computer without the written approval of the cognizant security officer or stored at unattended or contingency facilities.
76. (U) Duties and Responsibilities - The duties and responsibilities of a COMSEC Account Manager include, but are not limited to, the following:

l. (U) Ensuring Standard Operating Procedures (SOPs), emergency protection or destruction plans are prepared in accordance with the requirements of CNSSI No. 4004.1 (Reference y), are provided to all hand receipt holders, and are present at all COMSEC facilities served by the COMSEC account;
a. (U) Keying material, including key used to protect COMSEC software, shall not be transferred between COMSEC accounts without written Controlling Authority approval (or Command Authority approval for modern key), since Controlling Authorities must be able to identify and verify the secure communications requirement for their cryptonet for all users of their key. If Controlling Authority approval cannot be obtained in time to meet operational requirements, or if a Controlling Authority cannot be identified, the local commander may authorize the transfer. The Controlling Authority must then be notified at the earliest opportunity and always within three days.
CNSSI 4005 bits and bobs

- CNSSI 4005 SECTION XII.106.c
- 106. (U) Issuing Keying Material for Use Within Fixed Facilities
  - c. (U) The KYK-13 and KYX-15 Common Fill Devices store key only in unencrypted form and do not provide an audit trail. They must not be used to hold key for longer than 12 hours from the time the key is loaded into the end-equipment or 12 hours after the end of the applicable cryptographic period (cryptoperiod) whichever is longer, except in cases of operational necessity. *Continues on...*
a. (U) It is expressly forbidden to apply any type of label to protective packaging such as canisters, marbleized wrapping, and logo tape, as it will divert attention from actual or attempted penetration of the material. Grease pencil and non-permanent markers may be used if it is absolutely necessary to mark a surface.

(U) NOTE: The outside surface of COMSEC equipment is considered protective packaging. No company/program/contractor labels period. Toe Tags are your BFF.
143. (U) Reproduction - COMSEC material is considered reproduced (copied) when it is duplicated in like form (e.g., DTD/SKL to DTD/SKL or LMD/KP to DTD/SKL, or creating a back-up copy of a disk containing unencrypted key). It is also considered reproduction of key when physical key is converted to electronic form for the purpose of being loaded into an electronic fill device (DTD/SKL) and subsequently filling into an ECU, or extracting a key file from a disk and storing it on an electronic key fill device. Reproduced material must be documented and controlled in the same manner as the original material. (To be Continued)
e. (U) Traditional Key - COMSEC accounts are normally provided only one copy of traditional (symmetric) key in electronic form (called Reg 0 key). Additional electronic copies may be made locally (e.g., in multiple fill devices) as long as records are kept by the local COMSEC Account Manager detailing all transactions for each copy of the key, including when each copy is destroyed. Only after all hand receipted copies of a key are destroyed is the original key itself capable of being destroyed in LCMS. Only then, may the COMSEC Account Manager report destruction of the key, as required. See Paragraph 92.b on Accounting for Reg 0 Key.

f. (U) Modern Key - Modern (asymmetric) key may not be copied since each key is unique and may only be used in one piece of equipment (end cryptographic unit or ECU). (U) NOTE: Unlike traditional key, modern (asymmetric) key is unique to the one ECU. Although modern key may be copied for transmission purposes (e.g., from a local SKL to a remote SKL), the same key may not be used in more than one operational ECU.
14. (U) Access by Non-U.S. Citizens:
   a. (U) Employed by the U.S. Government. 
   b. (U) Employed by a U.S. Government Contractor, Vendor, or a Federally Sponsored Activity. Permanently admitted resident aliens, and any other non-U.S. citizens employed by a U.S. Government contractor, vendor, or federally sponsored activity, may only be granted access to unkeyed CCIs with the prior written approval of the cognizant NSA or Department or Agency program office. Requests for granting such access must be fully justified and based on operational need.
17. (U) Transportation of Unkeyed CCIs: Regardless of the mode of transportation selected, prepare unkeyed CCIs for shipment as set forth in paragraph 16, above. In addition:

c) U.S. Postal Service (USPS) registered mail or express mail provided the material does not at any time pass out of U.S. control. When using express mail, the shipper must obtain assurance from USPS authorities that ITV is provided to the point of delivery. A recipient’s signature must be obtained when using either registered or express mail. Material must be introduced into the postal system across-the-counter at a USPS facility; postal drop boxes must not be used.
NOTE: (U) An Electronic Key Management System (EKMS) Disposition Record Form must be maintained for all electronic keying material loaded into a Common Fill Device (CFD) (e.g., RASKL (Really Simple Key Loader), SDS (Secure Data Transfer Device 2000 System), SKL (Simple Key Loader)) so that personal responsibility can be traced in the event of a compromise. Disposition forms used for CFDs that contain only UNCLASSIFIED keying material will be marked as UNCLASSIFIED//FOR OFFICIAL USE ONLY. Disposition forms used for CFDs containing keying material classified as CONFIDENTIAL or higher are classified as CONFIDENTIAL. Accounts must complete the form in its entirety in order to ensure all information is provided and is classified properly.
NOTE: (U) The NSA/CSS COR prohibits the use of “property book/asset management” databases or any similar database(s) to account for or track any COMSEC material that is accountable in the COMSEC Account’s approved CMCS COMSEC Register. It is poor operational security practice to make available COMSEC information to personnel who are not performing or supporting official COMSEC Account Manager duties/responsibilities. The intent is to prevent drawing attention to COMSEC areas or COMSEC material from individuals who would not have access to COMSEC material or a need-to know.
2) (U) The following personally owned electronic devices are prohibited in COMSEC facilities:

a) Personally owned photographic, video, or audio recording equipment;

b) Personally owned Personal Electronic Devices (PEDs). These include but are not limited to: Personal Digital Assistants (PDAs), palm tops, hand-held and laptop computers, workstations and associated media, cell phones, web based phones, two-way pagers, wireless e-mail devices, and portable music players/devices with memory (e.g., iPods but not CD players)

How do you classify FitBit, Jawbone, etc?

How do you classify Bluetooth enabled?
b. (U) Personal or Government-owned or leased (or Company owned or leased) Equipment -

The following items are prohibited in COMSEC facilities unless approved by the cognizant security officer for the conduct of official duties:

1) (U) Two-way transmitters (including cell phones);
2) (U) Audio, video, or optical recorders; and
3) (U) Test, measurement, and diagnostic equipment.
Protective Technologies

- Free standard product in small amounts
  - Tamper Evident Bags
  - Indicative Locks
  - Loop Seals
  - Security Labels
  - Security Tape
- Government Off-The-Shelf or program specific customized products
Questions?

- Cards
  - Somewhat correct

- Hardware doctrine

- Looking for something new(ish)?