CONTENTS

2 GIPC 2010

3 KG Rules Destruction

4 Accountability of Classified COMSEC Equipment

5 Listing Multiple Discrepancies for ONE Short Title on an Incident Report

6 INE Corner

7 Going Secure using the KSV-21

8 Key Order Requests for KSV-21

9 Preparation of COMSEC Incident Reports

10 COMSEC Incident Report Corrective Actions

11 Submitting Incident Reports

12 COMSEC NICP Relocation from Ft. Huachuca, AZ to Aberdeen Proving Ground, MD

13 KSD-64s Destruction and Disposition

14 Fortezza Plus Crypto Card Family End of Life

15-13 CIR DIRECTORY

14 FROM THE EDITOR
There has been a change to the previously released Global INFOSEC Partnership Conference (GIPC) 2010 information in COLT #68 dated November 2009. Due to a change in Army Materiel Command (AMC) conference policy, the 19th annual GIPC and technology expo will now be hosted by the Southern Arizona Chapter of the Armed Forces Communications and Electronics Association (AFCEA) at Fort Huachuca, AZ from 4-6 May 2010.

The theme for GIPC 2010 is “COMSEC: A KEY ELEMENT IN PROTECTING THE GLOBAL NETWORK ENTERPRISE CONSTRUCT.”

Lieutenant General (LTG) Dennis L. Via, Joint Chiefs of Staff, J6, is scheduled as GIPC’s featured Keynote Speaker.

Lectures, workshops, and displays are scheduled to be co-located at Fort Huachuca’s Greely Hall (Bldg #61801), Carter Street Training Facility (Bldg #74912), and at Fitch Auditorium (Alvarado Hall, Bldg #62711).

Because of GIPC’s popularity and space constraints, the number of registered attendees must be limited to 325. It is recommended that all travel and lodging arrangements be made early, and registration completed as soon as website registration is available.

As a courtesy, CSLA will provide a link to the GIPC host website when it becomes operational. The host website is scheduled to become available in March 2010. The site will house all conference information, workshop scheduling, and attendee and exhibitor registration/payment for GIPC 2010. Please continue to check the CSLA website for the host link with your CAC associated to an AKO account at: https://www.csla.army.mil/ or http://csla.army.mil/ for public access.

Arrangements have been made with local hotels to hold GIPC-blocked rooms until mid April; however, some may release the block as early as mid-March. Hotel rates may vary from the list below. Be sure to refer to the room block by name and confirm the room rate when contacting the hotel for reservations. Also, be sure to request the government rate when making reservations at hotels that have no room blocks. The FY10 lodging per diem rate for Fort Huachuca and Sierra Vista is $83.

The following is a list of lodging establishments, phone numbers, room rates and available GIPC-blocked rooms:

**ARMY LODGING**
(520) 533-2222/533-2107
$53 PLUS TAX
40 RMS BLOCKED UNDER THE NAME ‘GIPC’

**BEST WESTERN MISSION INN SIERRA VISTA**
(520) 458-8500
$83 PLUS TAX
20 RMS BLOCKED UNDER THE NAME ‘GIPC’

**BEST WESTERN QUAIL HOLLOW INN**
BENSON, AZ
(APPROXIMATELY 30 MINUTES FROM SIERRA VISTA/FT HUACHUCA)
(520) 586-3646
$83 PLUS TAX
10 RMS BLOCKED UNDER THE NAME ‘GIPC’

**CANDLEWOOD SUITES**
(800) 970-4654/(520) 439-8200
$83 PLUS TAX
40 RMS BLOCKED UNDER THE NAME ‘GIPC’

**FAIRFIELD INN & SUITES BY MARRIOTT**
(520) 439-5900
$83 PLUS TAX
10 RMS BLOCKED UNDER THE NAME ‘GIPC’

**GATEWAY STUDIO SUITES**
(877) 443-6200/(520) 458-5555
$83 PLUS TAX
10 RMS BLOCKED UNDER THE NAME ‘GIPC’

**GARDEN PLACE SUITES**
(520) 439-3300
$83 PLUS TAX
10 RMS BLOCKED UNDER THE NAME ‘GIPC’

**HAMPTON INN**
(520) 439-5400
$83 PLUS TAX
20 RMS BLOCKED UNDER THE NAME ‘GIPC’

**HOLIDAY INN EXPRESS SIERRA VISTA**
(888) 465-4329/(520) 439-8800
$83 PLUS TAX
40 RMS BLOCKED UNDER THE NAME ‘GIPC’

(Continued on page 3)
(Continued from page 2)

HOLIDAY INN EXPRESS TOMBSTONE  
(APPROXIMATELY 30 MINUTES FROM SIERRA VISTA/FT HUACHUCA)  
(520) 457-9507  
$83 PLUS TAX  
10 RMS BLOCKED UNDER THE NAME ‘GIPC’

QUALITY INN AND CONFERENCE CENTER  
(800) 458-0982/(520) 458-7900  
$83 PLUS TAX  
80 RMS BLOCKED UNDER THE NAME ‘GIPC’

SIERRA SUITES  
(520) 459-4221  
$83 PLUS TAX  
50 RMS BLOCKED UNDER THE NAME ‘GIPC’

SUBURBAN EXTENDED STAY  
(520) 458-0540  
$83 PLUS TAX  
40 RMS BLOCKED UNDER THE NAME ‘GIPC’

SUN CANYON INN  
(800) 822-6966/(520) 459-0610  
$83 PLUS TAX  
25 RMS BLOCKED UNDER THE NAME ‘GIPC’

WINDEMERE HOTEL AND CONFERENCE CENTER  
(800) 825-4656/(520) 459-5900  
$83 PLUS TAX  
40 RMS BLOCKED UNDER THE NAME ‘GIPC’

---------------------------------------------------------------------

Other area hotels with no room blocks:

AMERICA’S BEST VALUE INN  
(888) 315-2378/(520) 459-5380

BELLA VISTA  
(520) 458-6737

BUDGET INN / SIERRA VISTA EXTENDED STAY  
(520) 458-6711

COMFORT INN  
(800) 221-2222/(520) 459-0515

HOLIDAY INN EXPRESS BENSON, AZ  
(APPROXIMATELY 30 MINUTES FROM SIERRA VISTA/FT HUACHUCA)  
(520) 586-8800

TOWNEPLACE SUITES BY MARRIOTT  
(520) 515-9900

(U) For administrative questions regarding GIPC 2010, feel free to contact the CSLA POCs:

Ms. Alicia DeCarlo,  
DSN 879-7583/CML (520) 538-7583

Ms. Karen Molet,  
DSN 821-1853/CML (520) 533-1853

Ms. Ronda Harmon,  
DSN 879-6469/CML (520) 538-6469

CSLA-GIPC@conus.army.mil

(KG-RULES Destruction (U))

By Claire Clark, AMSEL-LCA-KEY  
DSN: 879-6532/CML: (520) 538-6532  
email: claire.clark@us.army.mil

(U) CSLA Tier 1 has recently noticed some COMSEC accounts are holding both Edition I (9) and Edition J (10) of the KG-Rules, USKAD BU71260 880091. Edition I is superseded therefore the only edition a COMSEC Account may currently hold is Edition J. If your COMSEC Account contains Edition I, you are required to destroy it.

(U) Keep in mind, no matter what supersession date appears on an old edition of KG-Rules, as soon as a new edition is received, COMSEC Account Managers are required to destroy the old edition.

(U) If you do not have Edition J, you may request it electronically by contacting the Army Electronic Key Management System (EKMS) Help Desk at: DSN: 879-9900/CML: (520) 538-9900, or toll free 1-877-896-8094.
Today there are approximately 1,200 classified COMSEC items of equipment incorrectly accounted for in the Property Book Unit Supply Enhanced (PBUSE) Automated System. COMSEC equipment items identified with a Controlled Inventory Item Code (CIIC) of "D", "E" or "F", are classified as CONFIDENTIAL, SECRET, AND TOP SECRET; therefore they MUST be accounted for exclusively within the COMSEC Material Control System (CMCS), and ONLY by a duly appointed COMSEC Account Manager. This is outlined in AR 710-2, paragraph 1.18.d (1). Property Book Accounts are required to maintain property records for such classified COMSEC items authorized under TAADS, but those records are only allowed to reflect Authorization Data and Identification Data as described in paragraph 2-5k AR 710-2. See also DA Pamphlet 710-2-1, paragraph 4-7b. Property transactions, on hand balances, serial number data, and location information for classified COMSEC equipment must not be posted to PBUSE accounting records. This is a security violation. Property Book Officers (PBOs) should transfer all classified COMSEC equipment currently accounted for on property book accounts to the local designated supporting COMSEC account using a DA Form 3161 Lateral Transfer Voucher Document. The COMSEC Account Manager will use this Transfer Document to support the preparation of a COMSEC Material Possession Report and establish CMCS Accountability. PBOs can then utilize the Asset Description Update (ADU) to drop those classified COMSEC items from the property book.

Questions should be directed to the CECOM CSLA Point of Contacts:
Mr. Ricky Ward
DSN 879-2332 CML (520) 538-2332
ricky.ward@us.army.mil
Mr. Peter Michaud
DSN 879-6431/CML (520) 538-6431
pete.michaud@us.army.mil
The HQDA POC
CW5 Alexander Brown
CML (703) 692-9485
alexander.brown@us.army.mil
(U//FOUO) FASTLANE ATM/SONET ENCRYPTOR (KG-75A)

Non-Standard Line Item Number: To Be Announced
National Stock Number: 5810-01-582-2276

(U) The General Dynamics C4 Systems FASTLANE Asynchronous Transfer Mode (ATM)/Synchronous Optical Network (SONET) Encryptor (KG-75A) provides high-speed, end-to-end, low-latency security for local and wide area ATM and SONET networks. The National Security Agency (NSA) certified the FASTLANE ATM/SONET (KG-75A) as a Type I encryptor on 30 Mar 08. The device is approved for all levels of information from Top Secret Codeword and below.

(U) FASTLANE eliminates the leased lines between two dedicated points that traditional Type I ATM bulk encryptors require. It provides both authentication and end-to-end protection of user information as well as supports up to 1,022 simultaneous, cryptographically isolated ATM connections. For each connection, FASTLANE dynamically generates traffic keys. This approach of isolating the connections and using different keys for each connection provides greater security than a bulk encryptor’s single key for all connections. A Personal Computer card containing a Crypto Ignition Key (CIK) protects the key material in a FASTLANE when not in use. FASTLANE incorporates recognized standards and is interoperable with commercial ATM switches and routers. FASTLANE is also interoperable with NSA certified TACLANE Classic (KG-175), operating on an ATM network, and managed by the GEM encryptor management software while in the ATM mode.

ATM/SONET Input/Output Interfaces:
- OC-3c (155 Mb/s) multi-mode
- OC-3c (155 Mb/s) single mode
- OC-12c (622 Mb/s) single mode
- OC-48c (2.5 Gb/s) single mode
- OC-192c (10 Gb/s) single mode (ATM only)

Physical Specifications:
- Height: 7.25 inches
- Width: 17.50 inches
- Depth: 21.50 inches
- Weight: 35 pounds

(U) FASTLANE is not on the NSA Indefinite Delivery Indefinite Quantity contract and is purchased directly from the vendor upon approval of the requirement in the Information Systems Security Program (ISSP) Application.

(U) FASTLANE is currently being evaluated by the Cryptographic Modernization Program Management Office (CM PMO), Ft. Monmouth, New Jersey. We anticipate receiving test results from the CM PMO. For information on Crypto Modernization, equipment, and or test results, visit: https://cryptomod.kc.us.army.mil/cryptomod.nsf

(Continued on page 6)
operations or performance along with combining highly secure, NSA-approved algorithms with the flexibility to integrate into SONET/SDH-based networks at virtually any rate.

(U) The encryptor’s integrated front panel features an interactive keypad and RS-232 CLI serial interface providing full local encryptor management access, and a Universal Serial Bus (USB) port to supporting firmware upgrades. Operational status displays through front panel Light Emitting Diodes (LEDs) as well as a two-line, 20-character Liquid Crystal Display (LCD). Status of local and network interfaces, Zeroized Power, temperature, battery, system operation, security, and interface transmission and reception are displayed via LEDs. The Crypto Ignition Key (CIK) features the Serial CIK Interface that supports Data-Key’s KSD 4000 device. The Key Fill is MIL-CON MC283 six-pin audio connector with an RS-232 fill interface.

Physical Specifications:
Width: 19.0 inches
Depth (without handles): 23.0 inches
Depth (with handles): 24.5 inches
Height: 3.5 inches
Weight: 25 pounds

(U) The KG-340 was certified by the National Security Agency (NSA) on 8 Aug 08 to provide Top Secret and below data confidentiality and user authentication and is currently under evaluation by the Crypto Modernization Program Management Office, Ft. Monmouth, New Jersey. We look forward to receiving test results from the CM PMO soon. For information on the Crypto Modernization, equipment, and or test results, visit: https://cryptomod.kc.us.army.mil/cryptomod.nsf

(U) CSLA Information Assurance – National Inventory Control Point INE Team Members:
General Dynamics TACLANE Products: KG-75/KG-75A/KG-175/KG-175A/KG-175D
L-3 Communication Systems Products: TALON KOV-26

Project Lead: Art Chavira
DSN: 879-7477/CML: (520) 538-7477
art.e.chavira@us.army.mil

Logistics Management Specialist: Mary Jo Schneiders
DSN: 879-6922/CML: (520) 538-6922
mary.jo.schneiders@us.army.mil

Contractor SRA: Lewis Hyde
DSN: 879-8265/CML: (520) 538-8265
lewis.hyde@us.army.mil

(U) CSLA New Equipment Training Team Members for INE Equipment:
Tony Brimm
CML: (520) 538-8373
tony.brimm@us.army.mil

Vince Naputi
CML: (520) 538-2725
vicente.naputi@us.army.mil

William Jensen
CML: (520) 538-7524
william.c.jensen@us.army.mil

Tony May
CML: (520) 538-8343
anthony.may@us.army.mil

Going Secure Using the KSV-21 (U)

By Dan McGarry, AMSEL-LCA-NET
DSN: 879-9019/CML: (520) 538-9019
daniel.mcgarry@us.army.mil

(U) The CSLA New Equipment Training team (NET) is aware that some customers have reported problems going secure after transitioning to the KSV-21 Enhanced Crypto Card. Specifically, the details of the problem reported is that after pressing the SECURE VOICE soft key the STE will display SECURE REQUESTED SECURE CAPABILITIES DISABLED. This seems to only occur when one or both of the STEs are installed on a PSTN (Analog) network. STEs installed on ISDN networks do not suffer this issue.

(U) KSV-21s do not have STU-III key, but the STE still has the hardware (Modem) to go secure with a
Recently, CSLA personnel have been noticing COMSEC Account Managers (CAMs) periodically ordering KSV-21s for use with the Local COMSEC Management Software Workstation (LCMS) without the EKMS ID.

When ordering the KSV-21 keys, CAMs need to fill out CF Form 1032, EKMS Key Order Request and insure the following items are filled out on the form:

- Block 8 – Be sure to check STE KSV-21
- Block 9 – Be sure EKMS ID is entered
- Block 11 – Be sure LMP/KP account is checked YES

Instructions on filling out CF form 1032 and complete instructions are available at website www.keysupport.net.

If you need further assistance in ordering KSV-21 keys contact the Central Facility Help Desk, toll free at 1-800-635-5689. Once you get through on this telephone number hit 4 twice and your call will be transferred to the CF Help Desk Personnel.

(U) Recently, CSLA personnel have been noticing COMSEC Account Managers (CAMs) periodically ordering KSV-21s for use with the Local COMSEC Management Software Workstation (LCMS) without the EKMS ID.

(U) When ordering the KSV-21 keys, CAMs need to fill out CF Form 1032, EKMS Key Order Request and insure the following items are filled out on the form:

- Block 8 – Be sure to check STE KSV-21
- Block 9 – Be sure EKMS ID is entered
- Block 11 – Be sure LMP/KP account is checked YES

Instructions on filling out CF form 1032 and complete instructions are available at website www.keysupport.net.

(U) If you need further assistance in ordering KSV-21 keys, contact the Army EKMS Help Desk DSN 879-9900/CML (520)-538-9900 or toll free at 1-877-896-8094

(U) To prevent this from happening, configure the STE to use SCIP protocol exclusively. Instructions are as follows:

- Press the Blue MODE button – the display will show AUTOSIG.
- Press the CHANGE soft key until the display shows STE/SCIP (on ISDN) or just SCIP (on PSTN).
- Press the BACK soft key until the display is clear.

(U) Recently, CSLA personnel have been noticing COMSEC Account Managers (CAMs) periodically ordering KSV-21s for use with the Local COMSEC Management Software Workstation (LCMS) without the EKMS ID.

(U) When ordering the KSV-21 keys, CAMs need to fill out CF Form 1032, EKMS Key Order Request and insure the following items are filled out on the form:

- Block 8 – Be sure to check STE KSV-21
- Block 9 – Be sure EKMS ID is entered
- Block 11 – Be sure LMP/KP account is checked YES

(U) Instructions on filling out CF form 1032 and complete instructions are available at website www.keysupport.net.

(U) If you need further assistance in ordering KSV-21 keys, contact the Central Facility Help Desk, toll free at 1-800-635-5689. Once you get through on this telephone number hit 4 twice and your call will be transferred to the CF Help Desk Personnel.

(U) Recently, the COMSEC Incident Monitoring Activity (CIMA) has noticed a variety of common errors on Incident Reports submitted by COMSEC Account Managers (CAMs). In order to process incident reports in a timely manner, the CIMA would like to remind CAMs of the following:

1. Ensure all account information provided in the Initial Report is accurate and up to date. It is essential to submit a new CARP every time account information changes. Account information available to the Incident Team on the TIER-1 CAD is not always current; therefore, the CIMA depends on CAMs to submit the most current account information as changes occur.

2. Be aware of incomplete short titles. For example, USFAU 32795 is not a complete short title. Some short titles require leading zeros followed by the COMSEC Account number. The correct short title would be: USFAU 000032795 888888.

3. Ensure edition numbers are complete. A six-digit entry is required.
   Note: This does not apply to keymat with alpha characters as the edition.

4. Ensure all Accounting Legend Codes are correct.
   Reminder: Not all keymat is ALC 6.

5. Ensure the correct Controlling Authority is included on the Incident Report.

6. Ensure your Army Command, ASCC, or DRU is listed on the Incident Report. It is essential the most current Army Command, ASCC, or DRU information is included in the report.

(U) Help us process your Incident Report quicker by taking the time to ensure all information is complete, accurate, and current.

Should you have questions or need additional information, please contact:
Ms. Brenda Stacy, DSN 879-7068/CML (520) 538-7068
Mr. Joe Oslund, DSN 879-6439/CML (520) 538-6439
Mr. Glen Winkley DSN 879-1816/CML (520) 538-1816
csla-incident@conus.army.smil.mil
(U) The COMSEC Incident Monitoring Activity (CIMA) has noticed that incident reports frequently do not adequately address corrective actions. Commanders and COMSEC Account Managers (CAMs) should periodically assess the account’s Standard Operating Procedures (SOP), especially when an incident has occurred. Corrective actions allow the CAM to implement procedures that will prevent the incident from recurring. Administrative incidents also require corrective actions.

(U) All final reports must include the corrective actions the COMSEC account took, or plans to take, to minimize the possibility of recurrence (see AR 380-40 para 7-4c). Sometimes the corrective actions cited in the incident report simply recount the CAMs response to the incident (e.g. destroyed superseded key, returned found key to COMSEC vault, re-certified key processor, etc.). While it is necessary to tie up loose ends, these types of actions usually do not put procedures in place to prevent a recurrence.

(U) The CIMA has also noticed that some accounts have submitted multiple incident reports throughout the year citing the same corrective actions on every report. In these cases, the corrective actions are most likely not effective, and the CAM needs to implement new corrective measures to prevent recurrence. Some incident reports have failed to cite corrective actions altogether.

(U) In the corrective actions paragraph, the CAM can briefly explain how their SOP was updated; if personnel required refresher training; if a briefing statement was signed (IAW TB 380-41 para 4.13.3c (3)); or any other measures the account initiated to prevent recurrence of the incident.

(U) The CIMA will continue to review incident reports to ensure Commanders address measures the account is taking to prevent recurrence. If the account does not provide sufficient corrective actions, the CIMA will either suggest corrective actions or request the CAM update the report with adequate corrective measures.

(U) Corrective actions empower the CAM to improve the account’s procedures, prevent future COMSEC incidents, and ensure secure communications within the Army.

For further assistance regarding COMSEC Incident Reporting, please contact the CIMA:

Mr. Joe Oslund
DSN: 879-6439/CML: (520)538-6439
joep.oslund@us.army.mil

Ms. Brenda Stacy
DSN: 879-7068/CML: (520)538-7068
brenda.stacy@us.army.mil

Mr. Glen E. Winkley
DSN: 879-1816/CML: (520)538-1816
glen.e.winkley@us.army.mil
csla-incident@conus.army.smil.mil

(U) In recent months, the CSLA COMSEC Incident Monitoring Activity (CIMA) has received many reports with important information missing causing delays in processing time. As a result, CIMA must contact the COMSEC Account Manager (CAM) or Property Book Officer to request the missing information. Please refer to the Incident Report examples in TB 380-41 page 7-20 through 7-22 to ensure your report contains the appropriate and complete information.

(U) Additionally, IAW AR 380-40 and TB 380-41 there are four types of incident reports submitted: An Initial Report, Amplifying Report, Final Report, and an Abbreviated Report. The CIMA has noticed a lack of amplifying reports submitted. This is a friendly reminder that amplifying reports are required when there is new or additional information, and every 30 days until a final report is submitted.

*CAMs are requested to ensure a copy of this COLT article is provided to your supporting PBO.

(U) Should you need additional information or have questions, please contact
the Army Service Authority POC,
Ms. Denita Dezelan,
DSN 879-8006/CML 520-538-8006.
denita.a.dezelan@us.army.mil
COMSEC National Inventory Control Point (NICP) Relocation from Ft. Huachuca, AZ to Aberdeen Proving Ground (APG), MD (U//FOUO)

By Nancy Calderon, AMSEL-LCA-DMT
DSN: 879-6408/CML: (520) 538-6408
email: nancy.calderon@us.army.mil

(U) Since first addressed in COLT #67, August 2009, COMSEC unclassified equipment inventory management has begun the transition from CSLA Ft. Huachuca, AZ to CSLA East, Aberdeen Proving Ground (APG), MD, as mandated by the 2005 Base Realign-ment and Closure (BRAC) decision. Listed below are the equipments that are now managed at APG, MD, with current Item Manager point of contact information:

**Fill Devices:** DTD (AN/CYZ-10(V3)), SDS (KIK-20), KYK-13, KOI-18, KYX-15A, and KIK-30 (RaSKL). The SKL (AN/PYQ-10) inventory management for Secondary Parts only is also being performed by APG, MD. The Item Manager is Natasha Henderson, DSN 867-0492/CML (410) 417-0492, natasha.henderson@us.army.mil

**NOTE:** For questions regarding the SKL End Item, Inventory management remains at Ft Huachuca, AZ. Point of contact Kim Dorman, DSN 879-8342/CML (520) 538-8342, kim.dorman@us.army.mil

**Secure Voice:** All STE models, Secure Wireline Terminal (SWT), OMNI, OMNIxi, and GSM. The Item Manager is Eyvette Preston, DSN 867-0493/CML (410) 417-0493, eyvette.preston@us.army.mil

**NOTE:** KSV 21 Key Order Requests (KOR) will continue to be managed at Ft Huachuca, AZ. POC for all STE KOR is Judy Elmquist, DSN 879-7536/CML (520) 538-7536, judy.elmquist@us.army.mil

**VINSON:** KY-57, KY-58, and all ancillaries. The Item Manager is Eyvette Preston, DSN 867-0493/CML (410) 417-0493, eyvette.preston@us.army.mil

(U) The CSLA COMSEC NICP move will meet BRAC milestones set for September 2011. CSLA will continue to function in a split-based operation during this transition period, continuing to provide the COMSEC community with the level of customer support you have come to expect from the CSLA.

(U) Some important points to remember:

- Requisitions for all COMSEC consumables and repair parts will continue to be input into the standard supply system as they are today. All requisitions will route automatically to the appropriate Inventory Manager, regardless of location.
- Army requirements are still posted in the web based Information Security Systems Program (ISSP). The ISSP Team will remain at Ft. Huachuca, AZ.
- Upon ISSP approval for purchasing COMSEC equipment, Army customers will continue to be referred to the CSLA Electronic Commerce (ECOM) Team for guidance on how to prepare their Military Inter-departmental Purchase Requests. The CSLA ECOM Team will remain at Ft. Huachuca, AZ.
- The COMSEC National Maintenance Point will also remain at Ft. Huachuca, AZ. All processes related to COMSEC Maintenance, COMSEC RESET and Forward Repair Activities remain unchanged.

For questions regarding the CSLA BRAC transition to APG, MD please contact:

Nancy Calderon, CSLA West
DSN: 879-6408
CML: (520) 538-6408

CSLA East contacts:
Tom Muffer, DSN: 867-0495
CML: (410) 417-0495
Shirley Hayden, DSN: 867-0494
CML: (410) 417-0494
FOR OFFICIAL USE ONLY

FORTEZZA Plus Crypto Card Family End of Life (U/FOUO)

By Judy Elmquist, AMSEL-LCA-ICW
DSN: 879-7536/CML: (520) 538-7536
email: judy.elmquist@us.army.mil

(U/FOUO) Attention COMSEC Account Managers (CAMs):

Effective 31 DEC 2009, the FORTEZZA Plus Crypto Card (FPCC) (KOV-14, KOV-14E, KOV-15, and KOV-16) are no longer authorized for use. This complies with DIRNSA Ft. George G. Meade, MD, EKMS Notice #215, P261303Z AUG 09, Subject: Reminder, STU-III and STE FORTEZZA FPC Card End-of-Life Info, paragraph 2B, which states “The use of STU III and STE FPC Cards in a secure mode after 1 January 2010, will be considered a reportable COMSEC incident.”

(U/FOUO) CAMs are directed to turn-in their FPCCs IAW below guidance:

1. KSD-64s must be zeroized and returned to Tobyhanna Army Depot (TYAD) COMSEC account 5B1099 with a SF-153 to the following address:

   Tobyhanna Army Depot
   11 Hap Arnold Rd, BLDG 73
   ATTN: SIOTY.MC-d
   (M/F: Pat Mirabelle, 570-895-5698)
   COMSEC Account 5B1099
   Tobyhanna Army Depot, PA 18466-5110

   If shipping DCS:
   5B1099 MG04
   Tobyhanna Army Depot

   (U) Should you have questions please contact:
   Ms. Judy Elmquist,
   DSN: 879-7536/CML: (520) 538-7536
   judy.elmquist@us.army.mil

   Ms. Nettie McCarroll,
   DSN: 879-8749/CML: (520) 538-8749
   nettie.mccarroll@us.army.mil

Commanders and Security Officers Take Note:

Recommend that all units conduct a 100% search of offices and work sites in which a Secure Telephone Unit (STU-III) had previously been installed for KSD-64 CIKs that may be laying around in desk drawers, safes, etc.

REMINDER: It is not permissible to ship undeleted KP CIKs or active STU-III CIKs containing key with the zeroized KSD-64s sent to TYAD for further disposition. Doing so is a Reportable COMSEC Incident per the Army-adopted national-level LMD/KP Operational Doctrine (IDOC-026-06), and TB 380-41.

KSD-64s Destruction and Disposition (FOUO)

By Larry Bryson, AMSEL-LCA-CPT
DSN: 879-6433/CML: (520) 538-6433
email: larry.j.bryson@us.army.mil

(FOUO) Now that STU-IIIIs are no longer authorized to be on hand in Army organizations, many of you have contacted us about what to do with quantities of KSD-64 Crypto Ignition Keys (CIKs) being discovered in your organizations. There are a couple options available to you, discussed in the paragraphs below.

(FOUO) If your organization no longer has a STU-III retained for CIK deletion purposes, and a KOK-22A (KP) is not available for use, you may smash the CIKs with a hammer or mallet beyond reuse/recognition or possible reconstruction, (especially the internal circuit card), and dispose of the remains as you would with like materials (plastics/metal) following your organization’s local directives. It is strongly suggested that a plastic bag be used for safety purposes to control the scattering of the broken plastic chips, and to contain the residue of the destroyed KSD-64s.

a. KSD-64s previously associated to a STU-III (i.e., User CIKs) do not require the presence of a witness, nor is recording/reporting destruction of these KSD-64s required.

b. KSD-64s containing Crypto Key (seed or operational), or KSD-64s used for other than STU-III operations (i.e., KP Reinit 1 or 2 keys) being accounted for in the COMSEC account’s assets, must be destroyed with a properly cleared witness using standard COMSEC accounting procedures IAW TB 380-41, and reported to the Tier-1/COR.

c. KSD-64s that can be confirmed as having been previously zeroized, but are still on hand may be destroyed IAW the above guidance, or may be boxed in bulk and shipped to Tobyhanna Army Depot (TYAD) COMSEC account 5B1099 for further disposition. In the event the zeroized KSD-64s are sent to TYAD, the shipment will be handled as “Unclassified residue.” There are no COMSEC accounting and control requirements for these items.

CAUTION: DO NOT ASSUME A KSD-64 HAS BEEN ZEROIZED. IF YOU DON’T KNOW FOR SURE, DESTROY THE KSD-64 LOCALLY.
CSLA’s INFOSEC Representatives

FEDORE, FRANK
FORT LEWIS, WA
DSN: 347-3781/CML (253) 966-3781
FAX DSN: 347-8861/FAX CML: (253) 966-8861
Cell: (253) 335-9671
email: frank.fedore2@us.army.mil
Mail: 404th AFSB-PAC/ESSC-CIR FL
Mail Stop 25, Box 339500,
Bldg 9503, Rainer Ave
Logistics Center, Fort Lewis, WA 98433-9500

GETTIS, DARRYL
FORT CARSON, CO
DSN: 691-9015/CML (719) 526-9015
Cell: (520) 331-9876
darryl.gettis@us.army.mil
Mail: USCCLA
ATTN: CSLA CIR Darryl Gettis
1/407 AFSBn
2530 O’Connell Blvd Bldg 8100, Room 111
Fort Carson, CO 80913-2527

RICKER, LARRY
TEAM LEADER
CSLA Customer Support Center, Fort Huachuca
DSN 879-8009/CML (520) 538-8009
e-mail: larry.ricker@us.army.mil
Mail: DIRUSACSLA,
ATTN: SELCL-ID,
2133 CUSHING ST STE 3600
Fort Huachuca, AZ 85613-7041

GIRDNER, BOB
FORT HUACHUCA, AZ (including Ft Bliss, TX)
DSN: 879-5043/CML: (520) 538-5043
FAX DSN: 879-8091/FAX CML: (520) 538-8091
Cell: (520) 891-4804
e-mail: robert-girdner@us.army.mil
Mail: ATTN SELCL IAD CIR
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
Fort Huachuca, AZ 85613-7090

MARK, GODFREY*
FORT HOOD, TX (Including Puerto Rico)
DSN: 737-8532/CML: (254) 287-8532
FAX DSN: 738-5686/FAX CML: (254) 287-5686
Cell: (254) 462-3341
godfrey.mark@us.army.mil
Mail: ATTN SELCL IAD CIR
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
Fort Huachuca, AZ 85613-7090

*Mr. Mark is deployed until 15 Apr 10. Support provided by CIR Ken Thurman at:
kenneth.thurman1@us.army.mil
DSN: 879-0686/CML: (520) 538-0686
CSLA’s INFOSEC Representatives (con’t)

EDWARDS, NORMAN*
FORT RILEY, KS
DSN: 520-0406/CML: (785) 240-0406
Cell: (520) 220-1538
email: darryl.gettis@us.army.mil
3/407th AFSB
CECOM LCMC CSLA CIR (Norman Edwards)
406 Pershing Court, Building 406
Ft. Riley, KS 66442
*Mr. Edwards is currently deployed to Iraq. Support provided by Fort Carson CIR, Darryl Gettis

BURCHETTE, BENNIE
FORT GORDON, GA
(Including Honduras and the Virgin Islands)
CML Cell: (520) 220-1113
email: bennie.burchettejr@us.army.mil
Mail: Fort Gordon LAO
Attn: Bennie Burchette, Jr.
Bldg 994 10th Street
Fort Gordon, GA 30905

RAIMONDI, DANIEL*
FORT DRUM, NY
DSN: 774-0623/CML (315) 774-0623
Cell: (520) 331-9879
email: john.calvin.knight@us.army.mil
Mail: Bldg T-126, Room 201
Conway/1st Street West
Fort Drum, NY 13602
*Mr. Raimondi is currently deployed to Afghanistan. Support provided by Fort Bragg CIR, John Knight

KNIGHT, JOHN
FORT BRAGG, NC
DSN: 337-2775/CML: (910) 907-2775
Cell: (202) 299-4050
FAX DSN: 236-2162/FAX CML: (910) 396-2162
email: john.calvin.knight@us.army.mil
Mail: USA CECOM LCMC CSLA
ATTN: John Knight
AMC ESSC Bldg AT 5225 Off of DeGlopper St
Fort Bragg, NC 28310
CSLA’s INFOSEC Representatives

**JOHNSON, LORENZO**

Yongsan, Korea  
DSN: 315-723-6237  
CML Cell: 011-82-10-6335-8343  
email-NIPR: lorenzo.johnson@korea.army.mil  
email-SIPR: lorenzo.johnson@korea.army.mil  
CECOM-FE 403rd AFSB-Korea (P)  
ATTN: CSLA-FE (Lorenzo Johnson)  
Unit 15599 Box 304  
APO AP 96205-5599

**SIMMS, ABDUS-SHAHEED**

Heidelberg, Germany  
DSN: 879-5043/CML: (520) 538-5043  
FAX DSN: 879-8091/FAX CML: (520) 538-8091  
Cell: (520) 891-4804  
email: abdusshaheed.simms@eur.army.mil  
Mail: HQ USAREUR (USACSLA)  
CMR 420, Box 129  
APO AE 09063-0129

**EDWARDS, NORMAN**

Balad, Iraq  
DSN: 312-987-5130  
(automated switch press 1) ext 4470#  
CML: 732-427-5130  
(automated switch press 1) ext 4470#  
email: csla-cir-balad@mmcs.army.mil  
Mail: 402nd AFSB, CECOM FRA 1-CSLA  
APO AE 09391

**GASKINS, CLARA**

Kuwait  
DSN: 318-430-2270  
Cell: 011-965-6613-8469  
email: clara.gaskins@kuwait.swa.army.mil  
Email: clara.gaskins@kuwait.swa.army.mil  
Mail: 401st AFSB-SWA  
Box 526  
Camp Arifjan  
APO AE 09366

**RAIMONDI, DANIEL**

Afghanistan  
DSN: 312-987-5130, option 1, ext 8094  
CML: (732) 427-5130, option 1, ext 8094  
email: csla-cir-kaf@mmcs.army.mil  
AKO email: daniel.raimondi@us.army.mil  
Mail: 4/401st AFSB  
AMC LSE FWD  
APO AE 09355
The COLT is a periodic publication of the U.S. Army CECOM LCMC Communications Security Logistics Activity. This publication is unofficial and does not supersede or take precedence over regulations or other official directives. If there is a conflict between information in the COLT, and what regulations dictate, follow the regulation.

Articles are enthusiastically accepted from any sector of the COMSEC community, as are any constructive comments, questions, corrections, or suggestions.

The COLT is a periodical publication made available electronically on the CSLA website. Please visit: https://csla.army.mil for copies of past issues of the COLT.

Our primary readers are COMSEC Account Managers (CAM), Property Book Officers (PBO), Signal/Communications Officers, Maintenance Personnel, and Controlled Cryptographic Item Serialization Officers (CCISO) however, many of our readers are not identifiable to us, so we ask that our COMSEC Account Managers also make the COLT available to our other customers. Contact the COLT Editor for copies of individual articles.

Thank You, The Editor