



COVER LETTER
BRAC INPUT

06272005

To: **BASE REALIGNMENT & CLOSURE (BRAC) COMMISSION**

From: Concerned Citizens

Subject: Error in DoD BRAC Recommendations

The Communications Security Logistics Activity (CSLA), based at Fort Huachuca, AZ., is a security focused activity of approximately 300 well trained security and logistics professionals, whose missions include, but are by no means limited to, integrated logistics support for Communications Security (COMSEC) equipment.

We the undersigned individuals submit the attached Information Paper for your consideration. The purpose of this Information Paper is to promote a greater understanding of the diverse security-related missions of CSLA, and to encourage a re-examination of the DOD recommendation.

Unofficial responses or requests for elaboration can be made to:

Susan C. Nichols
1980 Viola Drive
Sierra Vista, AZ. 85635-2152
(520) 439-9396

Kathy Calabrese
6151 S. Calle De La Mente
Hereford, AZ 85615
(520) 803-9457

Requests for official responses for information must be made to the Director,
USACSLA:

ATTN SELCL DIR
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
FORT HUACHUCA AZ 85613-7041
(520) 538-6131

Thank you – Respectfully –

Susan C. Nichols and Kathy Calabrese

INFORMATION PAPER **ERROR IN DOD BRAC ANALYSIS**

ISSUE: The Base Realignment And Closure (BRAC) proposal to realign/relocate the Communications Security Logistics Activity (CSLA) from Fort Huachuca, AZ to Aberdeen Proving Ground, MD is based on incorrect data. Relocation will result in zero increases in efficiency and possible serious threats to National Security. *The following critical points must be considered regarding the relocation of CSLA:*

- Information used by the Department of Defense analysts as the rationale for realignment was based on incomplete and flawed data; specifically, the jobs performed by the vast majority of CSLA personnel do not neatly fit into a supply or even logistics category.
- Of the nearly 300 Department of the Army Civilians, Air Force, Navy and Army Military, and Contract personnel employed by CSLA, only approximately 10-15% are directly engaged in Inventory Control Point (ICP) management.
- Realignment and co-location of the entire Activity with primarily supply-oriented functions will reduce current operational efficiencies, expend critical funds with no payback, and needlessly create security risks during a time of war.
- Due to the nature of its missions (see below), CSLA works closely with many organizations at Fort Huachuca. Examples:
 - When a new COMSEC device is being developed, CSLA collaborates with the Joint Interoperability Test Command (JITC) to ensure the device will operate in the total C4IEW environment.
 - The Information Systems Engineering Command (ISEC) works with the CSLA Cryptographic Modernization Team (see CSLA missions below) on the next generation of Information Assurance (IA) devices to ensure seamless transitions of IA/COMSEC systems to the Warfighter.
 - Finally, the Electronic Proving Ground (EPG) here at Fort Huachuca features the capability to test transmission, reception and other communications functions.

In short, co-location of CSLA with these organizations offers the Department of Defense efficiencies and synergies that will be broken if CSLA is relocated. Below are brief descriptions of some of the CSLA missions other than the ICP.

Electronic Key Management System (EKMS): EKMS is a Joint (multi-service)/National Security Agency (NSA)-mandated system that automates the generation, distribution and management of modern electronic cryptographic key material and equipment to warfighters worldwide. EKMS ensures secure communications essential to protect lives and information on the battlefield. It also supports the White House Communications Agency, military Special Operations, DIA, CIA, FBI, CIA, Department of State and other national agencies and organizations. CSLA manages the portion of EKMS that provides direct support to military and Civil Agency organizations, and operates the Army's EKMS Help Desk to provide worldwide COMSEC problem resolution 24x7. CSLA operates one of two EKMS Tier 1 sites worldwide. The second EKMS Tier 1 site in San Antonio, TX has also been identified for relocation to the eastern seaboard under BRAC. Movement of both sites would create the requirement for a third system to transition, since neither EKMS Tier 1 site can support the entire DoD for an extended

period. The proposed relocation sites create an Operational Security (OPSEC) issue due to the close proximity to the NSA EKMS Tier 0 site in Maryland.

Central Office of Record (COR): The Army COR provides for COMSEC equipment and Cryptographic Key accountability as a Multi-Service mission (Army, Navy and Air Force) and manages automated and manual COMSEC Accounts worldwide. This operation is physically co-located with the EKMS Tier 1 site to allow secure access to the data on a continual basis. The COR tracks items within the account for distribution, destruction and inventory. They are the watchful eye ensuring the warfighter has the tools to communicate, and accounts for and uses those tools properly. Relocation away from the EKMS Tier 1 would require a new secure communications link, not captured in the BRAC costs for relocation.

COMSEC Plans and Policy: Develops new and conducts technical review of proposed COMSEC Policy to ensure compliance with all security requirements, conducts reviews of NSA regulatory guidance for applicability to Army COMSEC use, and provides policy clarification and guidance to the Army COMSEC community worldwide.

COMSEC Account Audits and Inspections: The mission is to conduct the mandated inventory of all COMSEC accountable items at Army accounts worldwide. The team also conducts the physical inspection and site approval for COMSEC storage and processing. The Army team interfaces with NSA to report, track, and coordinate corrective actions associated with COMSEC Security incidents to ensure no compromise of COMSEC information. Based on these Incident Reports, this team makes recommendations to the Plans and Policy branch for new policy and required changes.

Cryptographic Modernization Program: This program supports Headquarters Department of Army for replacement planning of all existing COMSEC devices as mandated by The National Security Agency (NSA). CSLA directly supports and coordinates with the Network Enterprise Technology Command's (NETCOM) Enterprise Systems Technology Activity (ESTA), the Army's largest customer for COMSEC equipment, located here at Fort Huachuca. This mission has been significantly accelerated due to technology improvements and evolving security threats

Cryptographic Futures Team: Responsible for analyzing new programs, products and emerging technologies to determine how and if these products and technologies should be integrated into the Army's evolving Information Security (INFOSEC), COMSEC and Information Assurance (IA) missions. The Futures Team plans, programs and implements support agreements that bring these emerging products and technologies under the support management of CSLA.

COMSEC New Equipment Training (NET): As new equipments and systems developed, procured, and fielded, training requirements are met through COMSEC NET. The mission is flexible, and provides either mobile or fixed site training in support of COMSEC fieldings worldwide. To support this NET training, the team uses the preliminary documentation to develop training courses. NET co-location with the Cryptographic Modernization Program and the ICP is critical to orchestrate the development and execution of just in time training for COMSEC equipment fielding and warfighter pre-deployment training.

COMSEC National Maintenance Point (NMP): The COMSEC NMP plans the workloading for the Tobyhanna Army COMSEC Depot. They plan closely with the COMSEC ICP to determine requirements and schedule the maintenance of COMSEC End Items and secondary repairables. COMSEC items are unique due to their classification, and require special training, handling, and safeguarding to protect National Security interests. The COMSEC NMP also plans for all maintenance levels within the Army, provisions for that maintenance, develops the maintenance publications for the Army, and collects the COMSEC maintenance data. The NMP is actively involved in the Global War on Terrorism, supporting warfighter requirements in theater, and executing the Reconstitution program upon their return from deployment.

COMSEC National Inventory Control Point (NICP): More than just the management of existing COMSEC and Controlled Cryptographic items, the ICP is the transition point for new equipment replacements under the Cryptographic Modernization Program. The item managers have technical training and experience in the COMSEC equipment they manage, which is unique to the COMSEC Commodity. The ICP works hand in hand with the COMSEC National Maintenance Point to develop the requirements and workloading for the Army COMSEC Depot facility at Tobyhanna, PA. The NICP actively supports the soldiers deployed in the Global War on Terrorism, the reconstitution of returning forces, and the restructuring of the Army through the Modularity Initiative. The loss of intellectual capital caused by a move would have profound impacts on readiness.

Global Information Security Partnership Conference (GIPC): This annual 3-day conference brings in nearly 350 personnel worldwide to the Sierra Vista/Ft. Huachuca to educate on the latest in the COMSEC and INFOSEC arena. No other conference exists to fulfill this need.

SUMMARY: The true nature of the CSLA mission with regard to Communications Security (COMSEC), Cryptographic Key and Information Assurance (IA) is not widely publicized due to the sensitive and classified nature of the mission performed. This paper has only touched the surface on the contributions to the warfighter and the IA community. While it is not impossible to relocate CSLA, there are no efficiencies to be gained, many security and operational risks that are created, and several unidentified expenses to be funded.

As outlined above, CSLA works closely with many organizations at Fort Huachuca, to include the Joint Interoperability Test Command (JITC), Network Enterprise Technology Command (NETCOM), and the Information Systems Engineering Command (ISEC). CSLA has created a synergistic relationship with these organizations, as well as offering the COMSEC/IA community worldwide a single point of contact for Security expertise.

Co-location of the entire organization with ICP functions sharing only a small overlap of the CSLA mission due to similarities in mission description is not good business and represents a waste of time and funds, while posing operational and Security risks outlined above. We submit this Information Paper to the decision makers in an attempt to rectify what we feel is a mistake for the Warfighter, the country and the American taxpayer.