

New Army streamlined COMSEC processes do more without more

By Josh Davidson

Program Executive Office Command, Control and Communications-Tactical and Project Director Communications Security is partnering with platform and system integrators across the U.S. Army to more efficiently secure networked mission command solutions whose future enhancements will require greater protection.

“We can really bring to the table a focus and an in depth knowledge-base as programs try to integrate COMSEC into their systems,” said Chris Manning, project director for COMSEC.

PD COMSEC procures, sustains and fields capabilities that secure and encrypt data on the Army’s tactical network. It is also a central point for the Army’s system integrators who seek COMSEC expertise as they integrate network and software

capabilities.

PD COMSEC will synchronize system integrators from separate project management offices through semi-annual COMSEC Integration Integrated Process Team forums. Representatives from the PD will travel to various Army acquisitions hubs to discuss COMSEC integration-related challenges and lessons-learned. Industry will also use the forum to present the future objectives in their roadmaps.

Government representatives will pose issues to multiple corporations who will offer potential solutions. Representatives from separate government entities and industry will converge, examine the pros and cons of various solutions and determine which approach might be best suited for their respective needs, Manning said. Previously, individual

(Continued on page 48)



Photo by U.S. Air Force TSG Johnny L. Saldívar

BAGHDAD, Iraq - Prior to the start of a mission, Army Sgt. Justin Green (left) and Pfc. Michael Moore (right) program a simple key loader to allow their radios to communicate securely between vehicles during a detail in Iraq. Their personal security detail team provides constant individual security. Both are deployed from the 2nd Brigade Heavy Combat Team, 1st Infantry Division, Fort Riley, Kan.

(Continued from page 47)

approaches to these solutions may have prevented the COMSEC community from efficiently reaching its overall objectives, he said.

At the forums, PD COMSEC will also articulate innovative, cost-effective communications security approaches to Army platform integrators. The integrators will determine the most effective ways to build COMSEC features into their future capabilities.

PD COMSEC has collaborated with the Assistant Secretary of the Army for Acquisition, Logistics and Technology ASA(ALT) Systems of Systems Engineering

Office to institute the most effective communications security and key management approaches and analysis across ASA(ALT)'s programs of record.

"We will assist project managers throughout ASA(ALT) in making informed program decisions regarding COMSEC integration into their platforms," Manning said.

For example, many systems engineers deem Type 1 encryption necessary on capabilities that require less than the top secret protection it can provide, Manning said. Excess expenses are incurred when programs procure greater COMSEC protection than the operational level they need. PD COMSEC guides these

individuals to alternatives to Type 1, when lesser security levels are appropriate.

"By consolidating and establishing PD COMSEC, those program offices have a place to go with acquisitions professionals that understand the business they are working in and understand that what you need in a program office are choices," Manning said.

Aside from the cost efficiencies yielded by its efforts, PD COMSEC is also bringing efficiency to the field. To lessen the logistics burden on Soldiers, PD COMSEC is leading the Army effort, in conjunction with the National Security Agency, to deploy Over The Network Keying capability to the Army to reduce the need



Components of the Project Director Communications Security portfolio. PD COMSEC procures, sustains and fields capabilities that secure and encrypt data on the Army's tactical network.

to receive COMSEC key from a physical workstation. The goal is to leverage the Key Management Infrastructure based solution in the next iteration of the Simple Key Loader. SKL is used to load cryptographic keys to encryption devices used to make data indiscernible to the enemy.

With this solution, the user will connect to the Secure Internet Protocol Router network from any location, register his or her brigade's devices and use the SKL to download key for each of their systems. This will eliminate the burden of carrying transit cases that contain large key distribution systems or searching for a COMSEC custodian.

"The user will be able to update key from garrison, all the way to the tactical edge," Manning said.

The solution will be usable with many of the 1.5 million end cryptographic units that are currently fielded, but some legacy systems will be replaced to support this application.

"We see this as the bridge until the Army can modernize its entire crypto fleet, that 1.5 million devices, so that they have the hooks to be able to get the key directly through the KMI infrastructure," Manning said.

PD COMSEC interfaces with both the Army and National Security Agency to find the most suitable key management and cryptographic materiel solutions for both entities. It is also collaborating with the NSA to resolve the challenge of distributing commercial key through military standard key distribution chains.

PD COMSEC manages the overall Army budget of the NSA-led KMI Program. This includes coordination, cost, schedule, performance and management. It also leads the training, fielding, sustainment and other logistics efforts for Army communications security.

Many Army developers approach industry to solve COMSEC challenges where viable solutions already exist. Some systems engineers may make their initial approach their sole solution to an issue. They do so without determining if the algorithms in the device can still function for the life of the host platform and must replace the capability within a few years. PD COMSEC's knowledge-set covers the broad scope of the Army's COMSEC products. The project management office offers viable options and specific timeframes on when key will become outdated, Manning said.

PD COMSEC was chartered to the Army's Program Executive Office for Command, Control and Communications-Tactical (PEO C3T) in September 2010. It was created as a result of an April 2008 memorandum when then CECOM Commanding General, LTG Dennis Via, recommended that ASA(ALT) establish an O6-level project management office within PEO C3T to centrally manage programs of record for the cryptographic modernization, key management and overall life-cycle management of Army COMSEC. PD COMSEC was established to synchronize a multitude of capabilities and program offices which require COMSEC, the many joint agencies which coordinate their delivery and centrally manage the more than 380 separate cryptographic and ancillary models in the field.

"The scope of COMSEC across the Army results in a high level of complexity of program of record and policy requirements and information assurance architecture modernization," Manning said.

The organization which simultaneously supports cryptographic modernization and key management objectives, is participating in a joint Lean Six Sigma project with CECOM to make Army wide COMSEC help desks more efficient. The project

will streamline help desk support for users who now access separate help desks throughout the United States.

The organization was established within PEO C3T's existing force structure, which eliminated the need for additional personnel authorizations. It also used the funding lines already allocated for the Army's key management and cryptographic modernization efforts, so additional budget requests were unnecessary.

"We did 'more without more' as we stood up the organization within the existing funding lines, without requesting additional money or affecting the amount of equipment purchased," Manning said.

Josh Davidson is a graduate of The College of New Jersey (formerly Trenton State College), in Ewing, N.J. Prior to becoming a government civilian strategic communications representative with PEO C3T, he was an investigative, music, sports and municipal journalist with numerous publications including Gannett Newspapers. He has interviewed GEN David Petraeus, GEN (Ret) Kevin Chilton, and GEN Ann Dunwoody. He has covered numerous tests, exercises and events related to Army satellite communications systems and applications.

ACRONYM QuickScan

ASA(ALT) - Army for Acquisition, Logistics and Technology

IPT - Integrated Process Team

KMI - Key Management Infrastructure

NSA - National Security Agency

OTNK - Over The Network Keying

PD COMSEC - Project Director Communications Security

PEO C3T - Program Executive Office for Command, Control and Communications-Tactical

SKL - Simple Key Loader