Cryptographic Systems

INVESTMENT COMPONENT

- **Modernization**
- Recapitalization
- Maintenance

MISSION

Provides Army users strategic and tactical advantages through communication security (COMSEC) superiority by modernizing and fielding cryptographic equipment and systems that protect against cyber threats, increase battlefield survivability/lethality, and enable critical mission command activities.

DESCRIPTION

Cryptographic Systems procures and fields solutions to secure the National Network Enterprise. New and emerging architectures are driving the need to replace current inventory of stove pipe systems with technologically advanced [network centric/Global Information Grid (GIG) compliant)] devices that incorporate Chairman of the Joint Chiefs of Staff and Joint Requirements Oversight Council directed cryptographic modernization, advanced key management and network centric performance capabilities. This program enables DoD to equip the force with critical cryptographic solutions and services during peacetime, wartime, and contingency operations.

The In-Line Network Encryptor (INE) family of network encryption devices provides network communications security in support of the movement to Everything over Internet Protocol (EoIP). These systems are used in both tactical and strategic networks and support multiple bandwidth configurations.

The Link & Trunk Encryptor Family (LEF) is used to multiplex and encrypt numerous signals into wideband data streams to be transmitted over fiber, cable, or satellites. The wide-band circuits require systems with rapid encryption capabilities.

Finally, the Secure Voice (SV) family uses security tokens and/or public key encryption to provide secure voice communication. There is a drive towards substitution in preference from wide-bandwidth to narrow-bandwidth communication channels.

Cryptographic Systems is modernizing legacy devices in order to accomplish cryptographic standardization of the Network for the Army, effectively countering the emerging cyber threat while supporting decisive full spectrum operations.

The Army-wide Cryptographic Network Standardization (ACNS) project, a multi-year effort which commenced in May 2012, ensures that legacy items with NSA mandated cease-key dates are replaced with fully modernized COMSEC equipment in support of the Army Modernization Strategy and Plan.

SYSTEM INTERDEPENDENCIES

In this Publication

None

Other Major Interdependencies

Cryptographic Systems are considered enabling systems which provide required COMSEC capabilities.

PROGRAM STATUS

- **1QFY12:** Started depot balancing efforts providing operational cost avoidance to PMs/Units
- **2QFY12:** Accelerated process of obtaining Standard Line Item Numbers (LINs)
- **3QFY12:** Decreased time in depot receiving process from 57 to 20 days
- **3QFY12:** Commencement of ACNS effort

PROJECTED ACTIVITIES

- **FY13-FY14:** Pursue and execute upon the Army Airborne Secure Voice requirement
- **FY13-FY15:** Continue modernization of INE, LEF and Secure Voice devices
- **FY13-FY15:** Continue the ACNS effort

ACQUISITION PHASE

Technology Development	Engineering & Manufacturing Development	Production & Deployment	Operations & Support

Cryptographic Systems

FOREIGN MILITARY SALES
None

CONTRACTORS
General Dynamics Communication Systems (Needham, MA)
Harris Corp. (Palm Bay, FL)
L3 Communications (Camden, NJ)
SafeNet (Columbia, MD)
ViaSat (Carlsbad, CA)