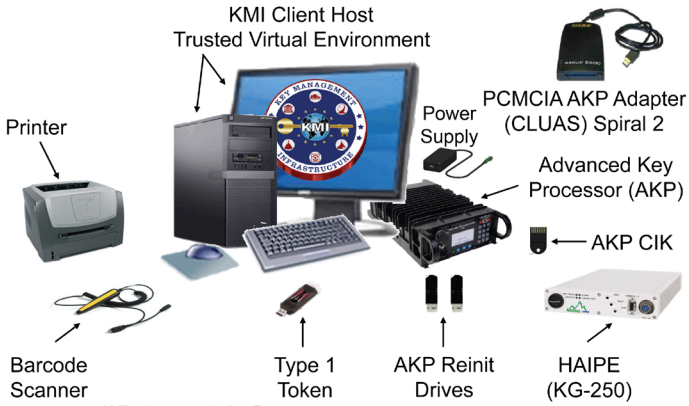
Key Management Infrastructure (KMI)

Executive Summary
- The National Security Agency (NSA) Senior Acquisition Executive (SAE) authorized full deployment for the Key Management Infrastructure (KMI) Increment 2 in November 2019.
- DOT&E approved the KMI Increment 3 Test and Evaluation Master Plan (TEMP) in August 2020.
- The NSA SAE approved KMI Increment 3 Milestone B in November 2020.

System
- KMI will replace the legacy Electronic Key Management System (EKMS) to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products (e.g., encryption keys, cryptographic applications, and account management tools).
- KMI consists of core nodes that provide web operations at sites operated by the NSA, as well as individual client nodes distributed globally, to enable secure key and software provisioning services for the DOD, the Intelligence Community, and other Federal agencies.
- KMI combines substantial custom software and hardware development with commercial off-the-shelf (COTS) computer components. The custom hardware includes an Advanced Key Processor for autonomous cryptographic key generation and a Type 1 user token for role-based user authentication. The COTS components include a client host computer with monitor and peripherals, printer, and barcode scanner.
- The NSA delivered KMI Increment 2 capabilities in two spirals.
- The NSA is delivering KMI Increment 3 in eight planned Agile releases that will enhance existing capabilities and subsume EKMS Tier 0 and Tier 1 cryptographic product delivery into the infrastructure.

Mission
- Combatant Commands, Services, DOD agencies, other Federal agencies, coalition partners, and allies will use KMI to provide secure and interoperable cryptographic key generation, distribution, and management capabilities to support mission-critical systems, the DOD Information Network, and initiatives, such as Cryptographic Modernization.
- Service members will use KMI cryptographic products and services to enable security services (confidentiality, non-repudiation, authentication, and source authentication) for diverse systems, such as Identification Friend or Foe, GPS, and the Advanced Extremely High Frequency Satellite System.



Major Contractors
- Leidos – Columbia, Maryland (Prime for Increment 2, Spiral 2)
- General Dynamics Information Technology – Dedham, Massachusetts
- SafeNet – Belcamp, Maryland

Activity
- The NSA SAE authorized full deployment for the KMI Increment 2 in November 2019.
- The Joint Interoperability Test Command did not conduct any KMI operational tests in FY20.
- DOT&E approved the KMI Increment 3 TEMP in August 2020.
- The NSA SAE approved KMI Increment 3 Milestone B in November 2020.

Assessment
- DOT&E determined KMI to be operationally effective, suitable, and secure for continued operations in 2019, and the current KMI Increment 2 deployed software baseline remained stable in 2020.
- The NSA continues to monitor and resolve problems based on recommendations from previous operational test reports.
  - NSA KMI Operations has recurring staffing shortages that affect long-term system sustainment.

  - The NSA KMI help desk, which supports DOD agency and external (non-DOD) users, lacks adequate knowledge of the system and is subject to high staff turnover rates.
  - Long-standing KMI configuration management problems remain that require experienced system and database administration, rigid process adherence, adequate staffing, and monitoring to sustain configuration.
- The KMI Test Infrastructure (TI) provides a safe laboratory for evaluating KMI software builds; however, the KMI TI is not maintained in the same configuration as the operational KMI. This limits the KMI TI users' ability to accurately identify problems prior to deploying a new KMI version to the operational system.

Recommendations

- The KMI Program Management Office should:
  1. Continue to resolve system defects and sustainment problems.
  2. Maintain the KMI TI to the same degree as the operational environment.
- The NSA KMI Operations should:
  1. Improve KMI configuration management and long-term sustainment.
  2. Reassess KMI Operations and help desk staffing to ensure that it can support all existing and planned new capabilities, networks, sites, and users.