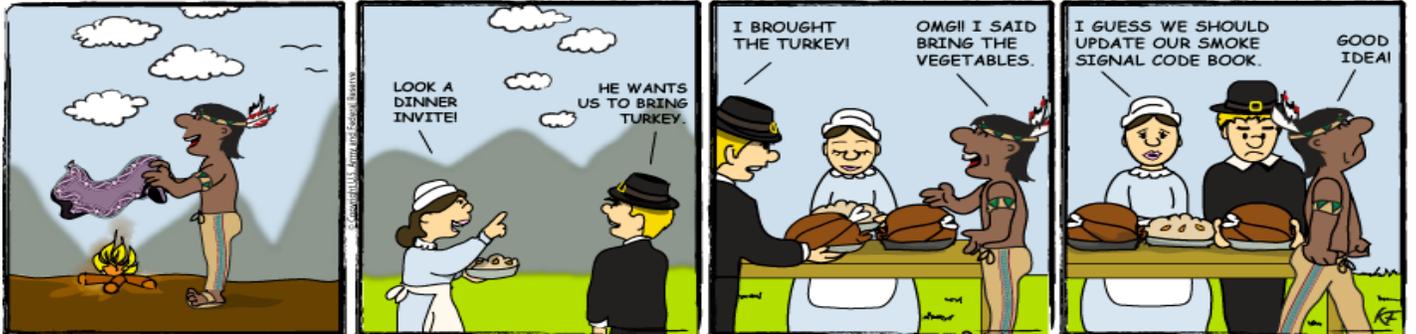


Smoke Signals Key Management

November 2012



ON CYBER PATROL



Yes, it's all about the Network, and this includes ensuring information that travels the Network is secure. This means not just accessing the correct data or getting your message, email, video, or other data from one point to another, but also ensuring the information that was sent is the information that was received.

Communications Security (COMSEC) is an essential component to enabling a secure Network and managing Army information. It is imperative that the confidentiality, integrity, availability, and non-repudiation of Army information be assured, and that users of the data can be properly identified and authenticated. COMSEC is one of the Cybersecurity capabilities that helps make this happen.

So, what is COMSEC really? Many of us think of COMSEC as simply the cryptographic capability in our radios or the cryptographic devices on the Network that we use to encrypt and decrypt Army information. We think of the COMSEC Account Manager who downloads cryptographic keys to our Simple Key Loaders (SKLs) that we then put into our radios or devices so we can communicate. The National Policy defines COMSEC as "measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emission security, and physical security of COMSEC material."

COMSEC is all of those things and more. COMSEC means having the right equipment, the right keys, and the right people to manage, maintain, and use the cryptographic equipment and keys, at the right place, at the right time. COMSEC is used to protect Army information from unauthorized disclosure, to detect unauthorized modification, and to authenticate the identities of people, organizations, devices and processes.

As the Pilgrims and Native American Thanksgiving party organizers found out, they each thought they had the right smoke signal codes to send and receive the Thanksgiving messages, but they did not. Their COMSEC equipment (fire) was out of date, their COMSEC keys (smoke signals) were not synchronized, and they could not even be sure who was sending the signals and who was receiving them. So, they ended up with two turkeys and no vegetables. This is an unfortunate situation for a Thanksgiving dinner, but a disastrous situation in military operations, when the success of the mission and Warfighter lives are dependent on secure and effective communications.

In the 21st Century, under the Network 2020 vision, the Army is providing the Warfighter with the tools they need to be successful, and this includes COMSEC. The Cryptographic Modernization Initiative transforms cryptographic security capabilities for national security systems at all echelons and points of use. The Cryptographic Modernization Initiative is focused on replacing, modernizing and transforming [command and control](#), communications, computer, [intelligence](#), [surveillance](#), [reconnaissance](#), [information technology](#) and [weapons systems](#) that rely on cryptography. If you are using aging or obsolete COMSEC equipment, you need to modernize now! If you do not know if you have obsolete COMSEC equipment, or if you are developing or acquiring a new cryptographic capability, contact the Chief Information Officer (CIO)/G-6 COMSEC Branch and they will assist you. You can have the latest and greatest technology instead of using an outdated smoke signaling system.

In addition to modernizing and transforming COMSEC equipment, the Army is improving its cryptographic key management capabilities as well through the Key Management Infrastructure Program. The National Security Agency (NSA) is developing and fielding a new net-centric infrastructure that supports the ordering, generation, distribution and accountability of keying material and other cryptographic products and services. The smoke signals and flags are gone, the hard copy paper tape is almost gone, and the electronic key is the new standard. The emerging key management

infrastructure is based on electronic keys and certificates. It includes the identification and authentication of personnel and devices to ensure these personnel and devices are trusted to generate and receive the keys and certificates that protect Army information on the Network. The security of national security information, systems and networks are dependent on the strength of the keys, effective protocols and standards associated with keys, and the protection afforded to the keys. If you need to know more about the key or certificates that enable the security in your COMSEC equipment, or about the key management infrastructure itself, contact the CIO/G-6 COMSEC Branch and they will assist you.

Now you have been armed with the latest COMSEC Information. Do not get your signals crossed and end up with a bunch of turkeys. Make sure you have the right ingredients to communicate securely and effectively on the Network. If you want to learn more, contact the CIO/G-6 COMSEC Branch and they will assist you.