



# United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, DC 20240

OCIO DIRECTIVE 2012-005

To: Assistant Directors for Information Resources

From: Bernard J. Mazer  
Chief Information Officer

Subject: Enterprise Secure Communications Program Management

## **Purpose:**

This document establishes policy and responsibility for Enterprise Secure Communications Program Management within the Department of the Interior (DOI). This includes the control of communications security (COMSEC) material and equipment and other secure communications methods and systems.

Secure Communications is defined as:

*The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC, communications security includes: cryptographic security, transmission security, emission security, and physical security of communications security materials and information.*

- a. Cryptographic security--The component of communications security that results from the provision of technically sound cryptosystems and their proper use.
- b. Transmission security--The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.
- c. Emission security--The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.
- d. Physical security--The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons<sup>1</sup>

---

<sup>1</sup> <http://www.thefreedictionary.com/Secure+communications>

**Scope:**

This policy's scope is within the National Security Framework as prescribed by National Security Directives (NSD), National Security Agency (NSA) guidelines, and the Committee on National Security Systems (CNSS) directives, issuances and policy.

The scope of this policy applies to Departmental Secure Communications Information Technology Management and Bureau/Office Secure Communications Information Technology Operational Management.

**Authorities:**

The Office of the Chief Information Officer shall retain authority for Information Technology and records management functions including telecommunications and infrastructure management covering secure communications.

The Office of Law Enforcement and Security (OLES) shall retain authority for the physical certification, accreditation and access management associated with the location and storage of Controlled Cryptographic Item (CCI).

The Office of Emergency Management (OEM) shall retain authority for coordinating secure continuity communications capabilities requirements.

**Timeframe:**

This directive is effective immediately upon date of signature.

**Policy:**

The Office of the Chief Information Officer (OCIO) shall provide enterprise management of the Department's secure communications program to include: secure communication systems policy development, architecture, relationship management with internal and external organizations, acquisition standards, capital planning to include budget and forecasting, and secure communications equipment life cycle management including systems replacement and asset management.

The Office of the Chief Information Officer, Service Delivery, Infrastructure Services Division, (OCIO-SD-ISD) shall serve as the Department's Central Office of Record (COR) for all secure communications CCI processing and management, Department-wide. The Departmental COR shall be responsible for ensuring that CCI material is received, controlled, distributed and accounted for all Departmental, Bureau and Office uses.

Bureaus/Offices are responsible for the operational control and safeguarding of such equipment and CCI material in accordance with National Security Agency (NSA) directives and must be aligned as a subcomponent with the Department's COR.

**Contact:**

For further information concerning the Enterprise Secure Communications Program, please contact Robert E. Lewis, Enterprise Secure Communications Program Manager at [robert\\_e\\_lewis@ios.doi.gov](mailto:robert_e_lewis@ios.doi.gov) or via telephone at (703) 648-5576.