



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Communication Protection Capability

Version 1.1.1

Communication Protection is a broad security Capability that is focused on protecting links and routes used for communication and enforcement of related protection policies. The goal is to protect communication channels appropriately for the operating environment.

07/30/2012



CGS Communication Protection Capability

Version 1.1.1



Table of Contents

1	Revisions	2
2	Capability Definition	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions.....	6
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations	7
7	Capability Interrelationships.....	8
7.1	Required Interrelationships	8
7.2	Core Interrelationships	9
7.3	Supporting Interrelationships.....	10
8	Security Controls	11
9	Directives, Policies, and Standards	15
10	Cost Considerations	22
11	Guidance Statements.....	23



CGS Communication Protection Capability



Version 1.1.1

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



CGS Communication Protection Capability



Version 1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Communication Protection is a broad security Capability that is focused on protecting links and routes used for communication and enforcement of related protection policies. The goal is to protect communication channels appropriately for the operating environment. Communication Protection provides enforcement of policies and practices as established in multiple Community Gold Standard (CGS) Capabilities such as Port Security, Network Boundary Protection, Key Management, and Access Management.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Communication Protection Capability is responsible for ensuring the continued confidentiality, availability, integrity, authentication, and non-repudiation of all communications that take place over links and routes, or between sources and destinations. Sources and destinations may include users, processes, or nodes. Communications includes all voice, video, and data being transferred using wires, wireless technologies, or satellite signals. The Communication Protection Capability shall use established Internet standards to allow for interoperability. The Communication Protection Capability covers all communication internal to an Enterprise or that crosses the Enterprise’s network boundaries. Mechanisms are employed across communication channels to protect the communications from unauthorized (accidental or intentional) disclosure and undetected modification and destruction. Communication Protection relies on other Capabilities to safeguard its systems and components (see the System Protection and Physical and Environmental Protection Capabilities).

Communication Protection requirements are driven by the mission needs and threat environment. Together, these shall determine the strength of the mechanism used for



CGS Communication Protection Capability



Version 1.1.1

protection and the required level of assurance (confidence that the mechanism will work).

The Communication Protection Capability shall maintain the confidentiality of transmitted data, when necessary. When confidentiality is ensured through the use of encryption, the strength of the encryption mechanism used shall depend on the classification of the data, the threat environment, and the data's useful life.

The Communication Protection Capability requires keys to use encryption mechanisms. All keys shall be managed through the Key Management Capability.

The Communication Protection Capability shall provide transmission security (i.e., camouflaging), when necessary. Transmission security shall be used when the environment or mission requires that the fact the communication is occurring must be hidden. These messages may still be encrypted so that in those cases where transmission security mechanisms fail the contents of the message remain confidential if necessary.

The Communication Protection Capability shall follow all availability requirements established by the Enterprise for voice, video, and data (see Utilization and Performance Management) and ensure that messages reach their intended destination. This includes the use of anti-jamming solutions that ensure transmissions are not blocked. Precautions shall be taken, such as redundant systems and failover mechanisms (see Contingency Planning), to prevent denial-of-service (DoS) events (i.e., when authorized access to resources is prevented or time-critical operations have been delayed). The Communication Protection Capability shall ensure the use of multiple communication paths over physical separate links and other protection mechanisms to prevent single points of failure. When encryption is employed as part of the Communication Protection Capability, care shall be taken to ensure that its use does not unnecessarily reduce the system's ability to meet its availability or performance requirements.

The Communication Protection Capability shall provide multiple layers of detection for verifying the integrity of communication, when necessary. The types of checks used shall vary based on the threat environment, mission demands, and classification of the data as dictated by Enterprise-established policy. Integrity checking is often accomplished through mechanisms such as cryptographic hash functions. Hashing algorithms and how they are used shall be Community approved.



CGS Communication Protection Capability



Version 1.1.1

The Communication Protection Capability shall ensure that all parties involved in the communication process are authorized to participate. The authentication function is provided by the Access Management Capability.

The Communication Protection Capability works in conjunction with other Capabilities (such as Access Management and Physical and Environmental Protections) to ensure that communication devices are used only in an authorized manner and that a source is authorized to send messages to the specified destination. Depending on the mission, environment, and type of communication, parties may have to reauthenticate periodically during the course of a transmission. Authentication may be required of both parties or just one party, as defined by the mission, the communicating parties, and the communication method. Communication Protection shall determine when to require bidirectional authentication, when unidirectional authentication is sufficient, and what methods to use for that authentication. Factors contributing to this decision include the identity and location of the source/destination, the path between them, and the data being transferred.

The Communication Protection Capability shall use trust relationships to facilitate communications that cross network boundaries. Trust relationships are established and maintained through the Network Boundary Protection Capability.

The Communication Protection Capability shall provide non-repudiation mechanisms for the parties involved in a communication, when necessary. The need for non-repudiation shall be determined based on the mission, threat environment, and classification of the data, as specified by Enterprise policy.

The Communication Protection Capability shall maintain activity logs and be audited regularly. Specific audit requirements and frequency shall be set by Enterprise or Community policy. Auditing shall ensure that users and non-human entities are accountable for communications and their ongoing protection. Audit information shall feed into the Enterprise Audit Management Capability.

The Communication Protection Capability is focused on securing the links used in communication. The data being transferred shall be secured by the Data Protection Capability. The systems involved in communication shall be secured by the System Protection Capability.



CGS Communication Protection Capability



Version 1.1.1

The Communication Protection Capability shall ensure that all personnel involved in a communication process are trained on how to appropriately fulfill their necessary functions. This includes any specialized communication equipment training, as well as procedural training. All other personnel are made aware of information assurance (IA) communication requirements and needs through the IA Awareness Capability.

The Communication Protection Capability mechanisms shall be documented and verified in accordance with any applicable certification and accreditation (C&A) requirements. Tools and equipment used shall be approved by the accrediting authority for the Enterprise.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Unauthorized physical and logical ports and services within the communication devices are blocked.
2. Unauthorized communication protocols are blocked.
3. The infrastructure is in place for communication.
4. The mission needs are defined and documented.
5. Security risk is known and documented.
6. Key management, credential management, and access management are established.
7. Physical and environmental protections are established.
8. Users/administrators are trained in the use and administration of the communication equipment.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability provides both internal and external protected communication mechanisms.
2. The Capability restricts communication routes and communication medium where necessary to enforce the protections that are provided.
3. Encryption techniques are used when necessary.



CGS Communication Protection Capability



Version 1.1.1

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

The Organization will use the Communication Protection Capability to secure and protect all voice, video, and data communication within the Enterprise. Communication methods include circuit switched telephony, voice over Internet Protocol (VoIP), streaming video, and file or message transfers, among others. The Organization will employ communication technologies that follow industry interoperability standards. The Organization will set Communication Protection requirements based on mission needs, the threat environment, and risk tolerance.

The Organization will ensure the confidentiality of communication by using encryption, where appropriate. All encryption keys will be controlled through the Key Management Capability. Communication links will be encrypted using dedicated cryptographic hardware, such as High Assurance Internet Protocol Encryptor (HAiPE) devices, according to Community standards. Individual data transmissions will be protected using end-to-end encryption mechanisms, such as transport layer security (TLS) or secure shell (SSH), as necessary.

The Organization will ensure the continued availability of all communication systems in accordance with Organization policy. This will be accomplished through redundancy, failover measures, and load balancing (see the Contingency Planning Capability). The Organization will conduct regular reviews of its communication infrastructure (see the Architecture Reviews Capability) to make its communication systems as robust and effective as possible.

The Organization will ensure the integrity of all communicated messages, as necessary. Integrity checking methods will be compliant with Organization- and Community-established methods.

The Organization will require authentication by parties involved in communication, where necessary, to prevent unauthorized activity. Specific authentication implementations will be dictated by mission need, threat environment, and data



CGS Communication Protection Capability



Version 1.1.1

classification. The implementation of authentication will be handled through the Access Management Capability.

The Organization will ensure non-repudiation, where appropriate, for communication. Non-repudiation is a critical function whenever any form of accountability is involved, such as when issuing instructions. Organization policy will dictate when and how non-repudiation of communication is achieved because it may vary across different communication channels. One-way non-repudiation can be achieved through the use of digital signature mechanisms, such as Public Key Infrastructure (PKI).

The Organization will perform audits of all Communication Protection functions. The specifics of these audits will be established by Organization policy. The information gathered during these audits will be fed into the Enterprise Audit Management Capability.

The Organization will provide training that ensures that users and administrators are able to perform their job and maintain communication security. For all personnel, mandatory training sessions that cover general communication security best practices will occur annually (see IA Training). For personnel involved in the communication process, the Organization will provide the necessary training for them to be able to fulfill their tasks.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping—The Communication Protection Capability relies on the Network Mapping Capability to provide information about the location of network components that are in the Enterprise in order to provide appropriate protection.
- Network Boundary and Interfaces—The Communication Protection Capability relies on the Network Boundary and Interfaces Capability to provide information



CGS Communication Protection Capability



Version 1.1.1

about network boundaries so that communications that cross network borders can be protected effectively.

- Utilization and Performance Management–The Communication Protection Capability relies on the Utilization and Performance Management Capability to define the utilization baseline that must be followed.
- Understand Mission Flows–The Communication Protection Capability relies on the Understand Mission Flows Capability to provide information about mission needs, which drive protection requirements.
- Understand Data Flows–The Communication Protection Capability relies on the Understand Data Flows Capability to provide information about the data flows that occur within the Enterprise, which drive protection requirements.
- Access Management–The Communication Protection Capability relies on the Access Management Capability to provide authentication functions for communications systems.
- Key Management–The Key Management Capability controls the keys used by the Communication Protection Capability for functions including encryption, digital signatures, and credentials.
- Digital Policy Management–The Communication Protection Capability relies on the Digital Policy Management Capability to manage the digital policies related to secure communications.
- Architecture Reviews–The Communication Protection Capability relies on the Architecture Reviews Capability to assess the security controls of a system to ensure that IA concepts (e.g., confidentiality, integrity, availability, authentication, and non-repudiation) are present in Enterprise architecture requirements.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Communication Protection Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Communication Protection Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Communication Protection Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.



CGS Communication Protection Capability



Version 1.1.1

- IA Training—The Communication Protection Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities—The Communication Protection Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- System Protection—The Communication Protection Capability relies on the System Protection Capability to protect the systems that perform communication functions.
- Physical and Environmental Protections—The Communication Protection Capability relies on the Physical and Environmental Protection Capability to provide physical protection to lines and devices used by communications functions. Physical and Environmental Protections also defines the protection needed during face-to-face communication.
- Metadata Management—The Communication Protection Capability relies on the Metadata Management Capability for metadata used to facilitate the protection of data.
- Threat Assessment—The Communication Protection Capability relies on the Threat Assessment Capability to evaluate the threat environments the Enterprise operates in so protection requirements can be determined.
- Contingency Planning—The Communication Protection Capability relies on the Contingency Planning Capability to ensure protection mechanisms continue to function in the event of a disruptive event, attack, or disaster.
- Risk Analysis—The Communication Protection Capability establishes protection mechanisms that are part of an accredited system and documented as such through a C&A process conducted by the Risk Analysis Capability.
- Risk Mitigation—The Communication Protection Capability relies on the Risk Mitigation Capability to establish the necessary safeguards to ensure the continued security of the Enterprise.



CGS Communication Protection Capability



Version 1.1.1

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
AC-4 INFORMATION FLOW ENFORCEMENT	<p>Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.</p> <p>Enhancement/s:</p> <p>(3) The information system enforces dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.</p> <p>(12) The information system, when transferring information between different security domains, identifies information flows by data type specification and usage.</p> <p>(13) The information system, when transferring information between different security domains, decomposes information into policy-relevant subcomponents for submission to policy enforcement mechanisms.</p> <p>(14) The information system, when transferring information between different security domains, implements policy filters that constrain data structure and content to [Assignment: organization-defined information security policy requirements].</p> <p>(15) The information system, when transferring information between different security domains, detects unsanctioned information and prohibits the transfer of such information in accordance with the security policy.</p> <p>(17) The information system:</p> <p>(a) Uniquely identifies and authenticates source and destination domains for information transfer;</p> <p>(b) Binds security attributes to information to facilitate information flow policy enforcement; and</p> <p>(c) Tracks problems associated with the security attribute</p>



CGS Communication Protection Capability



Version 1.1.1

	binding and information transfer.
AC-18 <i>WIRELESS ACCESS</i>	Enhancement/s: (5) The organization confines wireless communications to organization-controlled boundaries.
AU-13 <i>MONITORING FOR INFORMATION DISCLOSURE</i>	Control: The organization monitors open source information for evidence of unauthorized exfiltration or disclosure of organizational information [Assignment: organization-defined frequency]. Enhancement/s: None Specified
SC-3 <i>SECURITY FUNCTION ISOLATION</i>	Control: The information system isolates security functions from non-security functions. Enhancement/s: (2) The information system isolates security functions enforcing access and information flow control from both non-security functions and from other security functions. (3) The organization implements an information system isolation boundary to minimize the number of non-security functions included within the boundary containing security functions. (5) The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.
SC-4 <i>INFORMATION IN SHARED RESOURCES</i>	Control: The information system prevents unauthorized and unintended information transfer via shared system resources. Enhancement/s: (1) The information system does not share resources that are used to interface with systems operating at different security levels.
SC-5 <i>DENIAL OF SERVICE PROTECTION</i>	Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization defined list of types of denial of service attacks or reference to source for current list]. Enhancement/s: (1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks. (2) The information system manages excess capacity,



CGS Communication Protection Capability



Version 1.1.1

	bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.
SC-8 <i>TRANSMISSION INTEGRITY</i>	Control: The information system protects the integrity of transmitted information. Enhancement/s: (1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. (2) The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.
SC-9 <i>TRANSMISSION CONFIDENTIALITY</i>	Control: The information system protects the confidentiality of transmitted information. Enhancement/s: (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. (2) The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.
SC-11 <i>TRUSTED PATH</i>	Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication]. Enhancement/s: None Specified
SC-13 <i>USE OF CRYPTOGRAPHY</i>	Enhancements: (1) The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information. (2) The organization employs NSA-approved cryptography to protect classified information. (3) The organization employs, at a minimum, FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals. (4) The organization employs [Selection: FIPS-validated; NSA-



CGS Communication Protection Capability



Version 1.1.1

	approved] cryptography to implement digital signatures.
SC-14 <i>PUBLIC ACCESS PROTECTIONS</i>	Control: The information system protects the integrity and availability of publicly available information and applications. Enhancement/s: None Specified
SC-19 <i>VOICE OVER INTERNET PROTOCOL</i>	Control: The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system. Enhancement/s: None specified
SC-20 <i>SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)</i>	Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Enhancement/s: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.
SC-21 <i>SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CHACHING RESOLVER)</i>	Control: The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems. Enhancement/s: (1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.
SC-23 <i>SESSION AUTHENTICATION</i>	Control: The information system provides mechanisms to protect the authenticity of communications sessions. Enhancement/s: (1) The information system invalidates session identifiers upon user logout or other session termination. (2) The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.



CGS Communication Protection Capability



Version 1.1.1

	<p>(3) The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated,</p> <p>(4) The information system generates unique session identifiers with [Assignment: organization-defined randomness requirements].</p>
--	---

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Communication Protection Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Intelligence Community Public Key Infrastructure (PKI) Overarching Policy for the SCI Fabric, 25 October 1999, Classified	Summary: It is the policy of the Intelligence Community (IC) that a single-root, hierarchical Public Key Infrastructure (PKI) be established for use on Sensitive Compartmented Information (SCI) networks between members of the Community. The IC PKI will provide IC member Organizations, for those applications that require them, strong identification and authentication, data integrity, digital signature, non-repudiation, and encryption services for all information system-based communications and services traversing Community SCI networks. These services shall be used for communications and services between IC member Organizations and those Organizations and their customers.
Intelligence Community Certificate Policy, Version 4.3.3, 25 September 2008, Classified	Summary: This policy provides uniform policy guidance and requirements for ensuring interoperability between Certification Authorities (CAs) within the IC PKI. It establishes standard operating policies and procedures to be used by IC agencies/components for services between members of the U.S. IC, IC customers, and others as approved by the Information and Technology Governance Board (ITGB) and the Intelligence Community Chief Information Officer (IC CIO). IC PKI public certificates and



CGS Communication Protection Capability



Version 1.1.1

	associated private keys have applicability to areas such as, but not limited to, confidentiality of information, digital signatures, and identification and authentication of individuals, as well as information system infrastructure components.
ICPM 2007-500-3 Intelligence Information Sharing, 22 December 2007, Unclassified	Summary: Policy: To maximize the dissemination of intelligence information to IC customers relevant to their missions, while balancing the obligation to protect intelligence sources and methods, the IC elements shall: ... b. Implement DNI approved information technology, personnel/physical security standards, and procedures for providing and protecting intelligence information. . . .
ICD 503 IC Information Technology Systems Security Risk Management, Certification and Accreditation, Effective 15 September 2008, Unclassified	Summary: This directive addresses interconnection of accredited information technology (IT) systems and the standards for interconnections.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoD 5200.1-R, Information Security Program, 14 January 1997, Unclassified	Summary: The Department of Defense (DoD) Information Security Program promotes proper and effective classification, protection, and downgrading of official information requiring protection in the interest of the national security. It provides guidance and references addressing protection of automated information systems and networks.
DoDD 8000.01, Management of DoD	Summary: It is DoD policy that: a. Information shall be considered a strategic asset to the



CGS Communication Protection Capability



Version 1.1.1

<p>Information Enterprise, 10 February 2009, Unclassified</p>	<p>Department of Defense; it shall be appropriately secured, shared, and made available throughout the information life cycle to any DoD user or mission partner to the maximum extent allowed by law and DoD policy.</p> <p>d. Information solutions shall provide reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents.</p>
<p>DoDD 8500.01E, Information Assurance, 23 April 2007, Unclassified</p>	<p>Summary: All DoD information systems shall maintain an appropriate level of confidentiality, availability, integrity, authentication, and non-repudiation that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost-effectiveness. The directive's stated scope includes applicability to the following: (2.1.2.2) Platform IT interconnections, e.g., weapons systems, sensors, medical technologies, or utility distribution systems, to external networks.</p>
<p>DoDI 8500.2, Information Assurance (IA) Implementation, 6 February 2003, Unclassified</p>	<p>Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks.</p>
<p>DoDI 8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 1 April 2004, Unclassified</p>	<p>Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a department-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption. It aligns DoD PKI and PK-enabling activities with DoD Directive 8500.1, as implemented by DoD Instruction 8500.2, and the DoD Common Access Card (CAC) program, as specified by DoD Directive 8190.3.</p>
<p>DoDI 8523.01, Communications Security</p>	<p>Summary: The ability to maintain the confidentiality, integrity, and availability, during transmission, of DoD</p>



CGS Communication Protection Capability



Version 1.1.1

(COMSEC), 22 April 2008, Unclassified	classified information and unclassified information that has not been approved for public release is of paramount importance for an effective DoD security posture. Therefore, it is DoD policy that “Transmission of DoD information shall be protected through the (use of) COMSEC measures and procedures ...”
DoDI 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense, 8 June 2010, Unclassified	Summary: This instruction establishes that all DoD-owned or controlled space systems, regardless of their mission assurance category or confidentiality level, must comply with the specified procedures that cover communication processes, use of cryptography, and other IA considerations.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction provides joint policy and guidance for information assurance (IA) and Computer Network Defense (CND) operations. The policy includes the following: Communications Security (COMSEC) material and techniques will be used to safeguard communication and communication systems.
DISA Network Infrastructure Security Technical Implementation Guide (STIG), version 7.1, 25 October 2007, Unclassified	Summary: This guide provides security considerations at the network level needed to achieve an acceptable level of risk for information as it is transmitted through an enclave. It was developed to enhance the confidentiality, integrity, and availability of sensitive DoD automated information systems.
DISA enclave Security Technical Implementation Guide (STIG), version 2.4, 10 March 2008, Unclassified	Summary: This guide provides Organizations an overview of the applicable policy and additional Security Technical Implementation Guide (STIG) documents required to implement secure information systems and networks while ensuring interoperability.
Committee for National Security Systems (CNSS)	
CNSSP-12, National Information Assurance Policy for Space Systems Used to Support National Security Missions, 20 March 2007, Unclassified	Summary: Applicable space systems shall all comply with the specified set of IA requirements including considerations for IA throughout the lifecycle of a product, compliance with the Federal Information Security Management Act (FISMA), and use of National Security Agency (NSA) approved cryptographic methods.
CNSSP-21 National	Summary: Federal department and agency Enterprise



CGS Communication Protection Capability



Version 1.1.1

Information Assurance Policy on Enterprise Architectures for National Security Systems, March 2007, Unclassified	Architectures (EA) shall integrate IA capabilities to mitigate risks associated with national security information. Security controls shall be incorporated at the component, system, service, and application levels of EAs, including plans to manage risk, protect privacy, and provide confidentiality, availability, integrity, authentication, and non-repudiation as part of an integrated IA approach.
CNSSI-1253 Security Categorization and Control Selection for National Security Systems, October 2009, Unclassified	Summary: This instruction provides all federal government departments, agencies, bureaus, and offices with a process for security categorization of National Security Systems (NSS) that collect, generate, process, store, display, transmit, or receive national security information.
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
National Communications System (NCS) Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, 25 July 2007, Unclassified	Summary: This directive establishes policy, explains legal and regulatory basis, assigns responsibilities, and prescribes minimum requirements for continuity communication capabilities.
Legislative	
Public Law 107-347, E-Government Act, 17 December 2002, Unclassified	Summary: This Public Law was enacted to enhance the management and promotion of electronic government services and processes. It requires the development of EAs within and across the Federal Government, and the provision of information security protections commensurate with the risk and magnitude of the harm resulting from information systems' corruption. It is divided into five titles. The Federal Information Security Management Act of 2002 (FISMA) was enacted as Title III of the E-Government Act. The act recognized the importance of information security



CGS Communication Protection Capability



Version 1.1.1

	<p>to the economic and national security interests of the United States and requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Further recognizing the highly networked nature of the current federal computing environment, the act provides for effective government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities.</p>

Communication Protection Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Intelligence Community Public Key Infrastructure (PKI) Interface Specification (Draft), version 2.9.4, September 2009, Classified	Summary: This specification describes the interfaces to the IC PKI, defines the interface requirements for creating X.509 Version 3 (V3) certificates and X.509 Version 2 (V2) Certificate Revocation Lists (CRLs), provides a baseline for IC PKI certificate profiles (largely mirroring those of the DoD's PKI certificate profiles), and establishes the content for PKI certificates.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Joint DoD IIS /Cryptologic SCI Information Systems Security Standards, Revision 4, 1 January 2006, Unclassified	Summary: This standard provides procedural guidance for the protection, use, management, and dissemination of SCI. The combination of security safeguards and procedures used for information systems shall achieve U.S. government policy that all classified information must be appropriately safeguarded to assure the confidentiality, integrity, and availability of that information.



CGS Communication Protection Capability



Version 1.1.1

Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems, September 1996, Unclassified	Summary: This special publication (SP) presents generally accepted system security principles and common practices that are used in securing IT systems. IT includes hardware, software, firmware, information data, and telecommunications.
NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002, Unclassified	Summary: This SP provides guidance for planning, establishing, maintaining, and terminating interconnections between IT systems that are owned and operated by different Organizations. It identifies the basic components of an interconnection, describes methods and levels of interconnectivity, and discusses potential security risks associated with an interconnection.
FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, Unclassified	Summary: Federal Information Processing Standard (FIPS) 199 developed standards for categorizing information and information systems that promote: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
ISO/IEC 7498-1, Open Systems Interconnection–	Summary: This document provides a common basis for the coordination of standards development for the purpose of



CGS Communication Protection Capability



Version 1.1.1

The Basic Model, 15 June 1996, Unclassified	systems interconnection, while allowing existing standards to be placed into perspective within the overall Reference Model.
ISO/IEC 7498-2, Open Systems Interconnection–Security Architecture, 1989, Unclassified	Summary: This document defines the security-related architectural elements that are appropriate for application when security protection is required in an open systems environment.

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Solution used for implementation–The strength of the protection mechanism that is implemented in hardware and software products used will need to reflect Enterprise or Community policies and standards.
2. Assurance requirements–The Enterprise assurance requirements may add additional cost to the implementation of this Capability by forcing functions to change the way they operate.
3. Inconvenience of communication restrictions–The communication restrictions may make some types of communication difficult or impossible. This could lead to complications fulfilling mission objectives.



CGS Communication Protection Capability



Version 1.1.1

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Communication Protection Capability.

- The Enterprise shall protect links and routes used for communications and enforcement of related protection policies and ensure communications channels are appropriately protected for the operating environment.
- The Enterprise shall ensure the continued confidentiality of all communications that take place over links and routes, or between sources and destinations.
- The Enterprise shall ensure the continued integrity of all communications that take place over links and routes, or between sources and destinations.
- The Enterprise shall ensure the continued availability of all communications that take place over links and routes, or between sources and destinations.
- The Enterprise shall ensure the continued authentication of all communications that take place over links and routes, or between sources and destinations.
- The Enterprise shall ensure the continued non-repudiation of all communications that take place over links and routes, or between sources and destinations, when necessary.
- Communications mechanisms shall use established Internet standards to allow for interoperability.
- Communication protection requirements are driven by the mission needs and threat environment, which together determine the strength of the mechanism used for protection and the required level of assurance (confidence that the mechanism will work).
- The use of encryption technologies to ensure the confidentiality of transmitted data shall depend on the classification of the data, the threat environment, and the data's useful life.
- All keys and key products used to protect communications shall be managed through a centralized key management system.
- The Enterprise shall provide transmission security (i.e., camouflaging), when necessary.
- Enterprise availability requirements shall be met to ensure that messages reach their intended destination.
- Precautions shall be in place to prevent denial-of-service events.



CGS Communication Protection Capability



Version 1.1.1

- The Enterprise shall ensure the use of multiple paths over physical separate communications links and other protection mechanisms to prevent single points of failure.
- Multiple layers of detection shall be used for verifying the integrity of communications, when necessary.
- The Enterprise shall ensure that all parties involved in the communications process are adequately authenticated and authorized to participate.
- Protection mechanisms shall be in place to ensure that communications devices and systems are used only in an authorized manner and that a source is authorized to send messages to the specified destination.
- The Enterprise shall use trust relationships to facilitate communications that cross network boundaries.
- The Enterprise shall maintain activity logs and be audited at a frequency to be set by Enterprise or Community policy.
- Auditing shall ensure that users and non-human entities are accountable for communications and their ongoing protection.
- All personnel using communications equipment or participating in communications functions shall receive appropriate training in the proper policies and equipment usage.
- Communications mechanisms and policies shall be documented and verified in accordance with any applicable C&A requirements.
- Tools and equipment used for communications shall be approved by the accrediting authority for the Enterprise.