



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS IA Awareness Capability

Version 1.1.1

The Information Assurance (IA) Awareness Capability promotes understanding of IA objectives, threats, risks, and actions, among other IA concerns.

07/30/2012



CGS IA Awareness Capability



Version 1.1.1

Table of Contents

- 1 Revisions2
- 2 Capability Definition3
- 3 Capability Gold Standard Guidance.....3
- 4 Environment Pre-Conditions5
- 5 Capability Post-Conditions.....6
- 6 Organizational Implementation Considerations6
- 7 Capability Interrelationships.....8
 - 7.1 Required Interrelationships8
 - 7.2 Core Interrelationships12
 - 7.3 Supporting Interrelationships.....13
- 8 Security Controls13
- 9 Directives, Policies, and Standards14
- 10 Cost Considerations17
- 11 Guidance Statements18



CGS IA Awareness 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 IA Awareness 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.

The Information Assurance (IA) Awareness Capability promotes understanding of IA objectives, threats, risks, and actions, among other IA concerns. IA Awareness is intended to empower individuals to recognize IA or security concerns and respond accordingly.

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 IA Awareness Capability provides the mechanism to enable awareness and understanding of the various IA concerns that face the Enterprise, such as objectives, threats, and risks, among other concerns. The goal of IA Awareness is to shape the behavior of all personnel to align with what the Enterprise has established in the IA Policies, Procedures, and Standards Capability.

The IA Awareness Capability is a comprehensive program, which focuses on ensuring that all personnel throughout the Enterprise are aware of the role they play in protecting the Enterprise’s assets. IA Awareness involves all personnel, including all outside contractors, who have access to the Enterprise’s internal resources, including technology and facilities.

IA shall be recognized as a shared corporate responsibility within the Enterprise. Leaders shall understand the importance of IA and how it affects current and future missions. IA shall be incorporated with the goals and objectives in the corporate Strategic Plan (see the IA Policies, Procedures, and Standards Capability). IA Awareness helps to achieve those goals. In addition, all personnel shall understand their role and the impact of their decisions on the Enterprise’s security posture and mission. Successful IA Awareness embraces open communication between personnel,



CGS IA Awareness Capability



Version 1.1.1

management, security officers, and system administrators. As there are changes to Enterprise policies, open communication will prevent issues that result from a lack of information sharing.

The IA Awareness Capability is universally focused on communicating information about objectives, threats, risks, and actions. Objectives are IA-related goals the Enterprise wants to accomplish that may or may not be ongoing. Threats and risks are Enterprise concerns that may impact the security posture and mission. Actions are the practices personnel shall employ to help achieve objectives and/or minimize threats and risks. In addition to these topics, IA Awareness shall also communicate information about other IA concerns, which could vary across different Enterprises. Some of the specific issues to be covered by IA Awareness are operations security (OPSEC), physical security, information security, and counterintelligence. IA Awareness information shall span technical, physical, personnel, and environmental concerns. IA Awareness uses different communication media to educate personnel about the importance of these topics and what their role is in relation to each of them.

The IA Awareness Capability is promoted in a number of ways including signage, memos, announcements, and other communications media. In addition, the IA Awareness Capability is tightly coupled with the IA Training Capability. IA Awareness shall use IA Training as a means of promoting awareness and will identify the awareness topics that will feed into IA Training. IA Training will, in turn, develop the necessary curricula and facilitate the instruction of courses that focus on the material identified by IA Awareness. IA Training shall also collect feedback from personnel that will be used to reevaluate awareness topics and training curricula.

The IA Awareness Capability is implemented in the Enterprise through an IA Awareness program. This program determines the when, where, and how for all of the specific implementation details. The program shall also cover the creation and delivery of awareness messages. The IA Awareness Capability shall establish mechanisms by which to acknowledge receipt of awareness messages and evaluate the effectiveness of awareness activities (e.g., surveys, tests). This mechanism shall assess both the level of awareness and understanding among personnel of the various IA topics. Effectiveness shall be measured by the use of Enterprise-determined metrics that will enable the aggregation and trending of results. The IA Awareness program is made up of several components the Enterprise needs to identify or establish. These components include the following:



CGS IA Awareness Capability



Version 1.1.1

- Awareness topics—Topics or issues about which information is communicated to the audience
- Intended audience—Who the awareness messages are supposed to reach
- Communication mechanisms—How the awareness messages will reach their audience
- Goals and objectives—The intended outcome of the awareness messages
- Other potential outcomes—Side effects or unintended outcomes that arise as a result of an awareness message or series of messages
- Enforcement mechanisms—Tactics used to enforce compliance with awareness policies
- Subject matter experts—Individuals able to provide expert advice while producing messages
- Message frequency—How often messages shall reach their audience
- Responsible parties—Individuals who oversee the awareness process for a message or series of messages

Effective IA Awareness is an ongoing process. This requires coordination with other Capabilities (see Capability Interrelationships) to provide information about the state of the Enterprise, which IA Awareness can use to make changes to the program, and enables decision authorities to categorize and prioritize IA Awareness needs. Maintenance and update functions serve to ensure that accurate and updated information is always being delivered to the personnel and that it is achieving the intended goal. Ineffective awareness communications are updated with new messages that are more effective.

The IA Awareness Capability includes a reporting function to keep interested Enterprise stakeholders advised on the status of the various awareness efforts. Reports are issued regularly, according to Enterprise policy. These reports shall include information about updates to the program and trend analysis information about performance and effectiveness.

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. IA Training is available.



CGS IA Awareness Capability



Version 1.1.1

2. The Enterprise has an established security office.
3. The Enterprise is monitoring physical, personnel, and network activity.
4. Risk determinations have already been made.
5. The Enterprise infrastructure supports the various communication mechanisms.
6. Leadership and governance support exists for IA Awareness.

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 ensures awareness among all personnel to help them identify possible incidents and know what actions to take.
2. The Capability provides personnel with an understanding of IA awareness issues.
3. IA Awareness may contribute to the reduction of certain security risks.
4. The Capability assesses effectiveness of the IA Awareness campaign.
5. IA Awareness can use training mechanisms but is not responsible for training.

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 establish an IA Awareness program that it will use to communicate information to its personnel to make sure they are aware of and understand IA issues, events, and best practices. It is imperative that all personnel are exposed to the awareness messages that are relevant to them. This includes personnel internal to the Organization and any contractors or outside personnel with access.

The Organization will identify all of the awareness details that are specific to their needs. This will include which topics to cover, the audience, mechanisms used for communication, awareness objectives, potential side effects, subject matter experts, message frequency, enforcement mechanisms, and individuals who are responsible for each message or set of messages. These details will be used to develop IA Awareness



CGS IA Awareness Capability



Version 1.1.1

messages that will then be delivered to the Organization's personnel through the identified communication mechanisms.

The Organization will focus IA Awareness efforts on whichever topics are determined to be necessary. These topics may vary for each different Organization based on its mission needs and individual risks. Included topics can range from general best practices to specific Organization policies.

Managers within the Organization will consider cybersecurity risk to the Enterprise for every decision they make for the project and their staff. Managers will lead by example, driving IA Awareness from the top down and will be fully aware of their responsibilities for IA. In addition, managers will refrain from influencing subordinates to take risks that have not been properly evaluated or asking them to make IA decisions they are not empowered or qualified to make.

The Organization will use a variety of communication mechanisms at its disposal to spread awareness information to its personnel. Communication mechanisms will be chosen based on the message that needs to be communicated, and the mechanism's effectiveness of message delivery given the environment and personnel that it will reach. For example, signage will be used to promote general best practices, but direct memorandums will be used to alert personnel to a policy change. Each message will be tailored to suit the properties of the chosen communication mechanism. IA Training is one means of communication that can be particularly effective when used by IA Awareness. The Organization will identify awareness topics through IA Awareness and feed that information into IA Training to develop and teach the courses to personnel.

The Organization will determine the criticality of awareness topics based on input from other Capabilities, such as Risk Analysis. Messages will be disseminated to personnel, and enforcement mechanisms will be implemented based on their criticality. For example, highly critical messages may preempt less critical ones. In addition, depending on the defined enforcement mechanism, personnel may be prevented from accessing a system if they do not complete an IA Awareness training course within a specified timeframe.

The Organization will identify and levy specific awareness requirements on external Organizations that provide contractor services. These requirements for the contractor Organization will be in addition to any requirements individual contractors have to complete as personnel of the Organization's internal resources. If this occurs, any



CGS IA Awareness Capability



Version 1.1.1

necessary legal agreements and reporting needs will be defined. Military employees may also be required to complete IA Awareness training through their parent services. As with contractor employees, the military members will be required to complete local IA Awareness training that may be different from their service requirement.

The Organization will evaluate its IA Awareness program to determine its effectiveness. The Organization will define a series of metrics that it will use to measure effectiveness. Personnel will complete surveys and tests to measure their awareness and understanding of IA topics. This information will be aggregated and analyzed to determine trends.

The Organization will update the IA Awareness program as necessary to improve its effectiveness and to incorporate the most current information into the messages. Feedback collected from personnel and trend analysis created through the use of metrics will be used to update IA Awareness Programs. Updated awareness content on the state of the Enterprise will come from other Capabilities such as those in the Know the Enterprise and Protect the Enterprise groups. This new content will be incorporated into awareness messages where appropriate.

The Organization will identify a point of contact (POC) for IA concerns within each office and provide this information to the central Organization. This POC will be responsible for ensuring compliance with IA Awareness policies as a supplement to any technical awareness monitoring that may be in place. In addition, this individual will collect feedback from personnel that will be incorporated into future IA Awareness updates.

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 IA Awareness Capability relies on the Network Mapping Capability to provide information about the state of the Enterprise, which will be



CGS IA Awareness Capability



Version 1.1.1

considered when constructing awareness messages. Personnel must understand this information and how it impacts their daily operations.

- Network Boundary and Interfaces—The IA Awareness Capability relies on the Network Boundary and Interfaces Capability to provide information about the state of the Enterprise, which will be considered when constructing awareness messages. Personnel must understand this information and how it impacts their daily operations.
- Utilization and Performance Management—The IA Awareness Capability relies on the Utilization and Performance Management Capability to provide information about the state of the Enterprise, which will be considered when constructing awareness messages. Personnel must understand this information and how it impacts their daily operations.
- Understand Mission Flows—The IA Awareness Capability relies on the Understand Mission Flows Capability to provide information about the state of the Enterprise, which will be considered when constructing awareness messages. Personnel must understand this information and how it impacts their daily operations.
- Understand Data Flow—The IA Awareness Capability relies on the Understand Data Flows Capability to provide information about the state of the Enterprise, which will be considered when constructing awareness messages. Personnel must understand this information and how it impacts their daily operations.
- Hardware Device Inventory—The IA Awareness Capability relies on the Hardware Device Inventory Capability to provide information about the state of the Enterprise, which will be considered when constructing awareness messages. Personnel must understand this information and how it impacts their daily operations.
- Software Inventory—The IA Awareness Capability relies on the Software Inventory Capability to provide information about the state of the Enterprise, which will be considered when constructing awareness messages. Personnel must understand this information and how it impacts their daily operations.
- Understand the Physical Environment—The IA Awareness Capability relies on the Understand the Physical Environment Capability to provide information about the state of the Enterprise, which will be considered when constructing awareness messages. Personnel must understand this information and how it impacts their daily operations.
- System Protection—The IA Awareness Capability relies on the System Protection Capability to provide information about protections applied within the Enterprise.



CGS IA Awareness Capability



Version 1.1.1

Personnel must understand this information and how it impacts their daily operations.

- Communication Protection–The IA Awareness Capability relies on the Communication Protection Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Physical and Environmental Protection–The IA Awareness Capability relies on the Physical and Environmental Protection Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Personnel Security–The IA Awareness Capability relies on the Personnel Security Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Network Access Control–The IA Awareness Capability relies on the Network Access Control Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Configuration Management–The IA Awareness Capability relies on the Configuration Management Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Port Security–The IA Awareness Capability relies on the Port Security Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Network Boundary Protection–The IA Awareness Capability relies on the Network Boundary Protection Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Identity Management–The IA Awareness Capability relies on the Identity Management Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Access Management–The IA Awareness Capability relies on the Access Management Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.



CGS IA Awareness Capability



Version 1.1.1

- Key Management–The IA Awareness Capability relies on the Key Management Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Digital Policy Management–The IA Awareness Capability relies on the Digital Policy Management Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Metadata Management–The IA Awareness Capability relies on the Metadata Management Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Credential Management–The IA Awareness Capability relies on the Credential Management Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Attribute Management–The IA Awareness Capability relies on the Attribute Management Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Data Protection–The IA Awareness Capability relies on the Data Protection Capability to provide information about protections applied within the Enterprise. Personnel must understand this information and how it impacts their daily operations.
- Network Enterprise Monitoring–The IA Awareness Capability relies on the Network Enterprise Monitoring Capability to monitor activity occurring in the Enterprise and feed that information into IA Awareness so it can be communicated
- Physical Enterprise Monitoring–The IA Awareness Capability relies on the Physical Enterprise Monitoring Capability to monitor activity occurring in the Enterprise and feed that information into IA Awareness so it can be communicated to personnel, as necessary.
- Personnel Enterprise Monitoring–The IA Awareness Capability relies on the Personnel Enterprise Monitoring Capability to monitor activity occurring in the Enterprise and feed that information into IA Awareness so it can be communicated to personnel, as necessary.
- Network Intrusion Detection–The IA Awareness Capability relies on the Network Intrusion Detection Capability to monitor activity occurring in the Enterprise and



CGS IA Awareness Capability



Version 1.1.1

feed that information into IA Awareness so it can be communicated to personnel, as necessary.

- Host Intrusion Detection—The IA Awareness Capability relies on the Host Intrusion Detection Capability to monitor activity occurring in the Enterprise and feed that information into IA Awareness so it can be communicated to personnel, as necessary.
- Network Hunting—The IA Awareness Capability relies on the Network Hunting Capability to monitor activity occurring in the Enterprise and feed that information into IA Awareness so it can be communicated to personnel, as necessary.
- Physical Hunting—The IA Awareness Capability relies on the Physical Hunting Capability to monitor activity occurring in the Enterprise and feed that information into IA Awareness so it can be communicated to personnel, as necessary.
- Enterprise Audit Management—The IA Awareness Capability relies on the Enterprise Audit Management Capability to monitor activity occurring in the Enterprise and feed that information into IA Awareness so it can be communicated to personnel, as necessary.
- Risk Analysis—The IA Awareness Capability relies on the Risk Analysis Capability to provide information used to prioritize awareness needs.
- Risk Mitigation—The IA Awareness Capability relies on the Risk Mitigation Capability to identify training needs as a form of mitigation for specific risks.
- IA Training—The IA Awareness Capability relies on the IA Training Capability to provide one of the mechanisms used to disseminate awareness information. The IA Awareness Capability also relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.

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 IA Awareness 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 IA Awareness 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.
- Organizations and Authorities—The IA Awareness Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.



CGS IA Awareness Capability



Version 1.1.1

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.

- Risk Monitoring–The IA Awareness Capability relies on the Risk Monitoring Capability to measure the effectiveness of IA awareness activities, in terms of Enterprise risk.

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-8 SYSTEM USE NOTIFICATION	Control: The information system: <ol style="list-style-type: none"> Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.



CGS IA Awareness Capability



Version 1.1.1

	Enhancements: None Specified
CT-2 SECURITY AWARENESS	Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [Assignment: organization-defined frequency] thereafter. Enhancement/s: (1) The organization includes practical exercises in security awareness training that simulate actual cyber attacks.
AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATION	Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community: - To facilitate ongoing security education and training for organizational personnel; - To stay up to date with the latest recommended security practices, techniques, and technologies; and - To share current security-related information including threats, vulnerabilities, and incidents. Enhancement/s: None Specified

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.

IA Awareness Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
The United States Government-Wide Cyber Counterintelligence Plan, 2008, Classified	Summary: The plan includes the establishment/expansion of Cyber Counterintelligence (CI) education and awareness programs.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National



CGS IA Awareness Capability



Version 1.1.1

National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 8570.01 Information Assurance Training, Certification and Workplace Management, certified current 23 April 2007, Unclassified	Summary: This directive sets policy and requirements for Information Assurance (IA) Awareness, IA training, and certification. It established responsibilities from the Department of Defense (DoD) Chief Information Officer (CIO) down to the heads of DoD components.
DoD 8570.01-M Information Assurance Workplace Improvement Program, incorporating change 2 on 20 April 2010, Unclassified	Summary: This manual provides guidance for the identification and categorization of positions and certification of personnel conducting IA functions within the DoD workforce supporting the DoD Global Information Grid. It also provides information on IA Awareness training.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction identifies policy and assigns responsibilities for IA training and IA Awareness training in addition to the requirement for refresher training annually.
Committee for National Security Systems (CNSS)	
CNSSD-500 Information Assurance (IA) Education, Training, and Awareness, August 2006, Unclassified	Summary: This directive establishes the requirements for federal departments and agencies to establish and implement IA education, training, and awareness programs for personnel with responsibilities in relation to National Security Systems.
CNSSI-4012, National Information Assurance Training Standard for Senior System Managers, June 2004, Unclassified	Summary: This instruction establishes the minimum standard for development and implementation of IA training for Senior System Managers, CIOs, Designated Approval Authorities (DAAs), and Chief Technology Officers (CTO). It encompasses both IA training and awareness.
CNSSI-4013 National Information Assurance Training Standard for System Administrators,	Summary: This instruction establishes the minimum standards for development and implementation of IA training for system administrators. It encompasses both IA training and awareness.



CGS IA Awareness Capability



Version 1.1.1

March 2004, Unclassified	
CNSSI-4014 National Information Assurance Training Standard for System Security Officers, March 2004, Unclassified	Summary: This instruction establishes the minimum standard for the development and implementation of IA training for system security officers. It encompasses both IA training and awareness.
CNSSI-4016 National Information Assurance Training Standard for Risk Analysts, November 2005, Unclassified	Summary: This instruction establishes the minimum training standard for the development and implementation of IA training for Risk Analysts (RA). It encompasses both IA training and awareness.
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

IA Awareness Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	



CGS IA Awareness Capability



Version 1.1.1

Other Federal (OMB, NIST, ...)	
NIST SP 800-16 Rev 1, DRAFT Information Security Training Requirements: A Role- and Performance-Based Model, 20 March 2009, Unclassified	Summary: This document is intended to be used by federal information security professionals and instructional design specialists to accomplish two major tasks: 1) design role-based training courses or modules, 2) design a basics and literacy course for all users of information systems. It encompasses both IA training and awareness.
NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003, Unclassified	Summary: This document provides the guidelines for building and maintaining a comprehensive awareness and training program, as a part of an Organization's IT security program. The guidance is presented in a lifecycle approach. It encompasses both IA training and awareness.
NIST SP 800-100, Information Security Handbook: A Guide for Managers, October 2006, Unclassified	Summary: This publication is to inform members of the information security management team (agency heads; CIOs; senior agency information security officers; chief information security officers; and security managers) about the various aspects of information security they will be expected to implement and oversee in their respective Organizations. It encompasses both IA training and awareness.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	

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:



CGS IA Awareness Capability



Version 1.1.1

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 Capability makes use of awareness materials to fulfill its functions.
2. Communication mediums—Awareness processes need communication mediums to be available and usable. Communications may need to be secured.

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 IA Awareness Capability.

- The Enterprise shall operate a comprehensive IA awareness program that focuses on ensuring all personnel are aware of the role they play in protecting the Organization's assets.
- The IA awareness program shall involve all personnel, including all outside contractors, who have access to the Enterprise's internal resources, including technology and facilities.
- The IA awareness program shall ensure that IA is recognized as a shared corporate responsibility within the Enterprise and understand how it affects current and future missions.
- The IA awareness program shall ensure that IA is incorporated with the goals and objectives in the corporate strategic plan.
- The IA awareness program shall ensure all personnel understand their role and the impact of their decisions on the Enterprise's security posture and mission.



CGS IA Awareness Capability



Version 1.1.1

- The IA awareness program shall embrace open communication between personnel, management, security officers, and system administrators such that as there are changes to Enterprise policies, all relevant parties become aware of those changes in a reasonable amount of time.
- The IA awareness program shall focus on communicating information about objectives, threats/risks, and actions as well as other IA concerns that may vary across Enterprises, such as OPSEC, physical security, information security, and counterintelligence.
- The IA awareness program shall span technical, physical, personnel, and environmental concerns.
- The IA awareness program shall use a variety of communications media including signage, memos, announcements, and other communications media to educate personnel.
- The IA awareness program shall leverage the Enterprise's training capabilities as a means to communicate awareness messages with personnel.
- The IA awareness program shall establish mechanisms by which to acknowledge receipt of awareness messages and evaluate the effectiveness of awareness activities using Enterprise-determined metrics that will enable the aggregation and trending of results.
- The IA awareness program shall periodically update its material and reevaluate its communication mechanisms to ensure the most up-to-date information is being communicated in the most effective manner.
- The IA awareness program shall provide reports to relevant Enterprise stakeholders on the status of the various awareness efforts including information about updates to the program and trend analysis information about performance and effectiveness.