



National Security Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS IA Training Capability

Version 1.1.1

Information Assurance (IA) Training is the training of users and IA practitioners on IA policies, requirements, processes, and procedures.

07/30/2012



# CGS IA Training 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 .....	6
7	Capability Interrelationships.....	8
7.1	Required Interrelationships .....	8
7.2	Core Interrelationships .....	9
7.3	Supporting Interrelationships.....	10
8	Security Controls .....	10
9	Directives, Policies, and Standards .....	12
10	Cost Considerations .....	16
11	Guidance Statements.....	16



# CGS IA Training 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 Training 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.

Information Assurance (IA) Training is the training of users and IA practitioners on IA policies, requirements, processes, and procedures. It also includes technical and operational IA Training to all personnel based on user and/or role. Within this Capability, an IA Training program is established, which includes identification, administration, maintenance, and evaluation of the training activities and materials.

## 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.

An Enterprise has multiple, dynamic IA Training needs; therefore, its IA Training needs shall be determined for a department or agency. These needs shall be defined within the Enterprise’s various departments to achieve the overall IA Training Capability. The IA Training Capability shall define a sustainable training program, including funding requirements, instructors, and training tools; training methods; equipment; and courses. The IA Training Capability shall identify training needs and implement, maintain, and evaluate the IA Training program.

### Identify

The IA Training Capability shall identify training needs and establish the necessary curricula throughout the Enterprise. To identify needs, the IA Training Capability shall rely on the IA Awareness Capability, as well as the Detect Events and Respond to Incidents Capabilities. The IA Training Capability shall use the IA Awareness Capability to reach out across the Enterprise to raise awareness and work with personnel to find gaps to ensure security training needs are identified and training is made available. The identification of training needs shall include universally accepted courses, which are technical and non-technical, and span the range of basic, intermediate, and advanced training requirements.



# CGS IA Training Capability



Version 1.1.1

IA Training shall be defined and designated based on a person's role, including identification of training needs for specialized areas. For example, every person shall be responsible for taking IA Awareness training, whereas personnel operating in a security or technical role may require specialized training. In addition, the method of training (e.g., on the job training [OJT], classroom, web-based virtual, computer-based training [CBT]) shall be determined based on training goals. The different methodologies for providing IA Training shall be used to align with identified training and student needs to provide training to the widest audience. During identification of training needs, in addition to internal curricula development, the Enterprise shall identify vendors or universities for external IA Training needs and establish the necessary partnerships and agreements.

All new training courses shall include the necessary IA relationships or explanations as part of the course. For example, business processes need to agree with IA policies and procedures, and technology courses need to incorporate security needs. Whereas, incorporating IA into a time management course may not be necessary. In addition, the Enterprise shall review the current curriculum to determine where IA aspects were overlooked and should be incorporated, what aspects should be updated, and what aspects can be consolidated or eliminated.

## Administer or Implement

The IA Training Capability shall administer or implement training needs to personnel, including contractors, who have access to the Enterprise's internal resources (e.g., technology, facilities). Senior officials within the Enterprise shall provide top-down guidance to direct and support the importance of training. Training shall be administered and implemented in accordance with applicable policies (as defined in the IA Policies, Procedures, and Standards Capability). Specific Enterprise policies may choose to incorporate a consequence should training not occur. Personnel shall be accountable for the direction provided in the policies during implementation.

The departments within the Enterprise shall determine the training needs of the roles within their departments. If needed, management shall consider training important enough to stop the execution of the mission and provide OJT to ensure that personnel are provided the time to maintain and expand their knowledge and skills in accordance with changes in operations and technology. The Enterprise shall establish a threshold of training needed to fulfill the person's job based on his or her role and ensure that personnel are adequately trained to perform their functions. The frequency in training shall be available on demand or on a defined schedule, according to the training course,



# CGS IA Training Capability

Version 1.1.1



student needs, environment, and roles. The IA Training Capability shall consider prior training when determining whether personnel meet the training needs of their role(s), including degrees and external courses.

All personnel affiliated with the Enterprise hold some level of responsibility for the overall security and IA for that Enterprise. The IA Training Capability is responsible for overseeing the user IA Training programs' policies related to them. IA Training based on role is mandatory for all personnel.

## Maintain

The IA Training Capability shall maintain IA Training courses, materials, and personnel training requirements. IA courses shall be kept current and updated according to technology or operational changes in the Enterprise. In addition, courses shall be reviewed for relevance according to mission needs and updated when necessary. The mechanisms for training delivery also shall be reviewed to determine courses if the delivery methods need to be changed. Modifications to an IA Training course may be needed because of changes in delivery technology, additional delivery environments, or changes of the mission pace. The Enterprise shall gain IA knowledge from the subject matter experts for the IA Training curriculum. Then, a curriculum manager shall determine modifications that are needed for an IA course, which shall be based on the input from the experts.

Tracking of personnel training requirements and fulfilled requirements shall be provided in a central repository, such that the information is searchable. A centralized system shall provide the ability to report on personnel who have or have not taken training based on the reporting needs. This information shall be accessible across the Enterprise in a standard format and be reportable to external (authority or peer) Organizations, when necessary. Reporting shall be sensitive to personnel security and identification anonymity requirements.

## Evaluate

The IA Training Capability shall evaluate the overall IA Training curriculum for relevance. In addition, the Capability shall assess individual IA courses, the instructors, and the effectiveness of training. To effectively evaluate a course, the requirements and the objectives of that course shall be understood before the course is provided to the intended audience. Based on these objectives, a course shall be measured against a defined standard. For example, if a standard for evaluation exists within the Community, the Enterprise shall either use that standard or establish Enterprise standards based on



# CGS IA Training Capability



Version 1.1.1

the Community standards (see IA Policies, Procedures, and Standards). IA courses shall be evaluated based on performance or knowledge. In either case, there shall be an evaluation of the effectiveness of the training. This evaluation shall feed back into the process to improve the training and determine where training has impacted performance or the Enterprise knowledge base; therefore, feedback mechanisms shall be implemented (e.g., course surveys). The Enterprise shall define metrics based on the Enterprise needs to evaluate the 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. Personnel have a variety of IA backgrounds, job functions, and IA needs.
2. Mission execution employs sound IA practices.
3. IA is the responsibility of all personnel.
4. The Enterprise has an overall training program that will be leveraged to ensure instructor qualifications.
5. Policies exist that define training requirements for the Organization.
6. The Enterprise has implemented an IA Awareness program.
7. Resources and management buy-in exists for the implementation of an IA Training program.

## 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 enhances the Enterprise's ability to ensure the mission.
2. The Capability provides personnel the skills needed to execute IA functions based on role.

## 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



# CGS IA Training Capability



Version 1.1.1

Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When this Capability is implemented correctly, the department or agency will possess an effective IA Training program for personnel to understand and abide by security practices and the ability to conduct cybersecurity operations in all areas of the cyber domain. The Organization will ensure adequate resources, such as funding, instructors, tools, and equipment, are effective. An effective security training program requires proper planning, implementation, maintenance, and periodic evaluation.

An Organization will conduct relevant IA Training for all personnel including contractors or outside personnel with access to the Enterprise or Enterprise resources. All personnel affiliated with an Organization will hold some level of responsibility for the overall security and IA of that Organization, such as a percentage of the staff/personnel time allocated to training.

The IA Training Capability will leverage other CGS Capabilities, such as IA Awareness, Detect Events, Incident Response, and IA Policies, Procedures, and Standards, to help senior officials and training personnel identify, categorize, and prioritize IA Training needs within the Organization. IA Training will be identified in accordance with the Organization's specific needs. This will include IA Training based on job roles, because not all personnel will need the same degree or type of IA Training to do their jobs. The Organization's IA Training program will distinguish between groups of personnel and will present only the information needed by the particular role. Because personnel will need training that relates directly to their use of particular systems, an Enterprise training program will be supplemented by more system-specific programs.

An Organization will administer or implement IA Training programs including visibility, selection of appropriate training methods, topics, materials, and presentation techniques. To successfully implement a training program, it is important to gain the support of management and employees through feedback from a training course.

An Organization will maintain IA Training efforts and ensure the courses keep pace with changes in technology, security, threats, and vulnerabilities, as necessary. A training program that meets an Organization's immediate needs may become ineffective when the Organization implements a new application or changes its environment.



# CGS IA Training Capability



Version 1.1.1

An Organization will store met requirements for personnel training in a centralized repository. This information will be in a standard format for tracking and reporting purposes. The Organization will exercise identification anonymity for sensitive personnel information.

An Organization will evaluate IA Training programs for requirements based on job roles. An evaluation will measure effectiveness of an IA course. Through understanding of requirements, an Organization will meet the objectives of IA Training.

The Organization will focus on all IA Training programs to ensure personnel understand why IA is critical to the operational security and sustainability of the Organization. The goal of the IA Training program is to create a security-aware culture in the Organization and include not only IA awareness training but also training that teaches the cybersecurity disciplines that include Computer Network Exploitation/Computer Network Attack/ Computer Network Defense (CNE/CAN/CND) and all Network Operations (NetOps) functions. Teaching secure practices, relating the importance of Enterprise security to individual users, and showing how personnel fit into the bigger picture of IA are the first steps to a secure culture. It lays the foundation for a successful IA Training program.

## 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 Enterprise Monitoring–The IA Training Capability relies on the Network Enterprise Monitoring Capability to provide information about Enterprise activity so it can be incorporated into training curricula, as necessary.
- Physical Enterprise Monitoring–The IA Training Capability relies on the Physical Enterprise Monitoring Capability to provide information about Enterprise activity so it can be incorporated into training curricula, as necessary.



# CGS IA Training Capability



Version 1.1.1

- Personnel Enterprise Monitoring–The IA Training Capability relies on the Personnel Enterprise Monitoring Capability to provide information about Enterprise activity so it can be incorporated into training curricula, as necessary.
- Network Intrusion Detection–The IA Training Capability relies on the Network Intrusion Detection Capability to provide information about Enterprise activity so it can be incorporated into training curricula, as necessary.
- Host Intrusion Detection–The IA Training Capability relies on the Host Intrusion Detection Capability to provide information about Enterprise activity so it can be incorporated into training curricula, as necessary.
- Network Hunting–The IA Training Capability relies on the Network Hunting Capability to provide information about Enterprise activity so it can be incorporated into training curricula, as necessary.
- Physical Hunting–The IA Training Capability relies on the Physical Hunting Capability to provide information about Enterprise activity so it can be incorporated into training curricula, as necessary.
- Enterprise Audit Management–The IA Training Capability relies on the Enterprise Audit Management Capability to provide information about Enterprise activity so it can be incorporated into training curricula, as necessary.
- Incident Response–The IA Training Capability relies on the Incident Response Capability to provide information about incident response procedures so they can be incorporated into training curricula, as necessary.
- Incident Analysis–The IA Training Capability relies on the Incident Analysis Capability to provide information about incident response procedures so they can be incorporated into training curricula, as necessary.
- Contingency Planning–The IA Training Capability relies on the Contingency Planning Capability to provide information about incident response procedures so they can be incorporated into training curricula, as necessary.
- Risk Mitigation–The IA Training Capability relies on the Risk Mitigation Capability to identify training needs as a form of mitigation for specific risks.

## 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 Training 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 Training Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about



# CGS IA Training Capability



Version 1.1.1

applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness–The IA Training Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- Organizations and Authorities–The IA Training 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.

- None

## 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-22 PUBLICLY ACCESSIBLE CONTENT	Control: The organization: b. Trains authorized individuals to ensure publically accessible information does not contain nonpublic information.
AT-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-3 SECURITY TRAINING	Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system



# CGS IA Training Capability



Version 1.1.1

	<p>changes; and (iii) [Assignment: organization-defined frequency] thereafter.</p> <p>Enhancement/s:</p> <p>(1) The organization provides employees with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.</p> <p>(2) The organization provides employees with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.</p>
AT-4 SECURITY TRAINING RECORDS	<p>Control: The organization:</p> <p>a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and</p> <p>b. Retains individual training records for [Assignment: organization-defined time period].</p> <p>Enhancement/s: None Specified</p>
AT-4 SECURITY TRAINING RECORDS	<p>Control: The organization:</p> <p>a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and</p> <p>b. Retains individual training records for [Assignment: organization-defined time period].</p> <p>Enhancement/s: None Specified</p>
AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	<p>Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:</p> <ul style="list-style-type: none"> <li>– To facilitate ongoing security education and training for organizational personnel;</li> <li>– To stay up to date with the latest recommended security practices, techniques, and technologies; and</li> <li>– To share current security-related information including threats, vulnerabilities, and incidents.</li> </ul> <p>Enhancement/s: None Specified</p>
CP-3 CONTINGENCY TRAINING	<p>Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency].</p> <p>Enhancement/s:</p>



# CGS IA Training Capability



Version 1.1.1

	<p>(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.</p> <p>(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.</p>
IR-2 <i>INCIDENT RESPONSE TRAINING</i>	<p>Control: The organization:</p> <p>a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and</p> <p>b. Provides refresher training [Assignment: organization-defined frequency].</p> <p>Enhancement/s:</p> <p>(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.</p> <p>(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.</p>
SA-5 <i>INFORMATION SYSTEM DOCUMENTATION</i>	<p>Control: The organization:</p> <p>b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:</p> <ul style="list-style-type: none"> <li>– User-accessible security features/functions and how to effectively use those security features/functions;</li> <li>– Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and</li> <li>– User responsibilities in maintaining the security of the information and information system.</li> </ul>

## 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 Training Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	



# CGS IA Training Capability



Version 1.1.1

<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
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.
<b>Department of Defense (DoD)</b>	
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.
<b>Committee for National Security Systems (CNSS)</b>	
CNSSD-500 Information Assurance (IA) Education, Training, and Awareness, dated August 2006, Unclassified	Summary: This directive established the requirement for federal departments and agencies to establish and implement IA education, training, and awareness programs for personnel with responsibilities related to National Security Systems.
CNSSI-4012, National Information Assurance Training Standard for Senior System Managers,	Summary: This instruction establishes the minimum standard for the development and implementation of IA Training for Senior System Managers, CIOs, Designated Approval Authorities (DAAs), and Chief Technology



# CGS IA Training Capability



Version 1.1.1

June 2004, Unclassified	Officers (CTO). It encompasses both IA Training and Awareness.
CNSSI-4013 National Information Assurance Training Standard for System Administrators, March 2004, Unclassified	Summary: This instruction establishes the minimum standard for the development and implementation of IA Training for System Administrators. It encompasses both IA Training and Awareness.
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,	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.
NSTISSI-4015 National Training Standard for System Certifiers, December 2000, Unclassified	Summary: This instruction establishes the minimum education and training standard for System Certifiers.
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

## IA Training Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	



# CGS IA Training Capability



Version 1.1.1

<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
Nothing found	
<b>Department of Defense (DoD)</b>	
Nothing found	
<b>Committee for National Security Systems (CNSS)</b>	
Nothing found	
<b>Other Federal (OMB, NIST, ...)</b>	
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 information technology (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.
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
Nothing found	
<b>Legislative</b>	
Nothing found	



# CGS IA Training Capability

Version 1.1.1



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:

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 will need to provide various types of training and management for that training based on relevant mission needs.
2. Location—Training programs require facilities in which to hold the training courses.
3. Certification costs—Trainers or trainees may need to obtain certifications.
4. Lifecycle maintenance—Curricula, courses, teaching software, and delivery methods need to be developed, reviewed, and updated with new material.
5. Impact/dependency of existing services—Loss or gain of productivity due to training.
6. Necessary training—Training instructors will need to be trained to do their job(s).

## 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



# CGS IA Training Capability



Version 1.1.1

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 Training Capability.

- The Enterprise shall provide IA training of users and IA practitioners on IA policies, requirements, processes, and procedures. It includes technical and operational IA training to all personnel based on user and/or role and includes the identification, administration, maintenance, and evaluation of the training activities and materials.
- The Enterprise shall establish an IA training program including addressing funding, personnel, tools, methods, equipment, and courses.
- The IA training program shall identify the training needs of the Enterprise and implement, maintain, and evaluate training courses as necessary.
- The IA training program shall work with Enterprise stakeholders to gather training requirements and identify gaps in existing training programs.
- The IA training program shall identify training needs that are technical and non-technical in nature and span basic through advanced requirements.
- The IA training program shall identify distinct training needs based on the role and level of responsibility of the various personnel within the Enterprise. The different methodologies for providing IA training shall be used to align with identified training and student needs to provide training to the widest audience.
- The Enterprise shall establish partnerships, when appropriate, with outside vendors or universities to fulfill additional or specialized training needs.
- The Enterprise shall ensure that when all new training courses are developed, whether they are specific to IA or not, they include an IA component.
- The IA training program shall provide training to all personnel, including contractors, who have access to the Enterprise's internal resources in accordance with Organizational policy.
- Personnel shall be held accountable for compliance with training policies and procedures.
- The Enterprise shall ensure that all personnel have received an appropriate amount of training to fulfill their assigned functions. Regarding frequency, the training shall be available on demand or on a defined schedule, according to the training course, student needs, environment, and roles.
- All personnel shall go through a minimum level of training to ensure compliance with Enterprise IA policies and procedures.
- The IA training program shall maintain IA training courses, materials, and personnel training requirements and undergo periodic reviews and updates to



# CGS IA Training Capability

Version 1.1.1



ensure that all information is up to date with current technologies, policies, and Enterprise needs.

- The IA training program shall use a centralized mechanism to track personnel training requirements and completed training. This information shall be accessible across the Enterprise in a standard format, be searchable, and be reportable to external (authority or peer) Organizations, when necessary.
- To ensure effectiveness, the IA training program shall evaluate the effectiveness of its training courses and instructors through feedback from personnel and through Enterprise-determined metrics.