



National Security Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Personnel Security Capability

Version 1.1.1

Personnel Security programs are the first line of defense in protecting personnel, the environment, physical assets, and technology. The Personnel Security Capability provides the security measures necessary to ensure all affiliates are screened prior to being granted access to facilities, systems, and information. For the purpose of this document, affiliates include employees, contractors, military, second parties, and visitors.

07/30/2012



# CGS Personnel Security 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 .....	5
5	Capability Post-Conditions.....	5
6	Organizational Implementation Considerations .....	5
7	Capability Interrelationships.....	6
7.1	Required Interrelationships .....	6
7.2	Core Interrelationships .....	7
7.3	Supporting Interrelationships.....	7
8	Security Controls .....	8
9	Directives, Policies, and Standards .....	10
10	Cost Considerations .....	15
11	Guidance Statements.....	15



# CGS Personnel Security 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 Personnel Security 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.

Personnel Security programs are the first line of defense in protecting personnel, the environment, physical assets, and technology. The Personnel Security Capability provides the security measures necessary to ensure all affiliates are screened prior to being granted access to facilities, systems, and information. For the purpose of this document, affiliates include employees, contractors, military, second parties, and visitors.

## 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 Personnel Security Capability provides the ability to gather information about affiliates, which is used to determine their access to facilities, systems, and information. The Personnel Security Capability shall provide mechanisms to screen affiliates, using a variety of mechanisms including background investigations, National Agency Checks (NACs), Local Agency Checks, and polygraph examinations.

Every affiliate accessing an information system that processes, stores, or transmits classified information shall be cleared and indoctrinated to the highest classification level of the information on the system. In all cases, affiliates shall be processed in accordance with the applicable Enterprise policy as set forth by the IA Policy, Procedures, and Standards Capability. When affiliates apply for access to classified information, they shall be notified of the Organization’s security and employment policies. A background investigation shall be conducted on all affiliates in accordance with the investigative protocols outlined in Community policy. Differing levels of review shall occur based on differing levels of required physical and system access. Depending on the Organization’s policies, additional security processing (e.g., polygraph



# CGS Personnel Security Capability



Version 1.1.1

examination) may be required. Once approved for requested level of access, the affiliate shall be indoctrinated and a nondisclosure agreement shall be signed. Each agency shall independently manage its Personnel Security Programs in accordance with internal and external policies. In each instance, Personnel Security Programs shall have appropriate support staff as needed, such as investigators, polygraph examiners, adjudicators, and legal authorities.

Minimum investigative requirements for Confidential, Secret and L clearances are a National Agency and Local Agency Check. A Top Secret, Sensitive Compartmented Information (SCI), or Q clearance requires a current Single Scope Background Investigation with a periodic reinvestigation being conducted every 5 years. Investigations shall employ the “whole person concept” and shall be the basis for evaluating an individual for initial or continued access to classified information or systems. Escort programs shall be implemented based on access needs.

The Personnel Security Capability shall include responsibility for validating clearances when a person transfers with his or her clearance to the Enterprise. When a clearance is transferred, it shall be accepted based on the Enterprise’s policy. For the transfer to be accepted, the background investigation shall be current (7 years or less). If the background investigation is 5 years or older, the receiving agency shall ensure it receives all necessary information from the sending agency to initiate a reinvestigation (see the Personnel Enterprise Monitoring Capability). In addition, a polygraph exam may be required. In cases where an exception (condition, waiver, or deviation) exists, reciprocity shall not apply and the receiving Enterprise shall make a decision according to Enterprise policy. Agencies shall accept or deny clearances based on risk analysis.

The Personnel Enterprise Monitoring Capability shall ensure that affiliates are debriefed from access when leaving the authority of the Enterprise and appropriate databases (e.g., Joint Personnel Adjudication System [JPAS], Scattered Castles) reflect the current information. An individual’s clearance remains active for 2 years after being debriefed. This allows individuals to have their clearances reinstated without additional security processing. However, if at the time of reinstatement the background investigation is out of scope, a reinvestigation shall be initiated.

Reporting shall occur on a quarterly basis to authority Organizations and on a monthly basis to Enterprise stakeholders. Reporting shall include data such as the number of initial accesses granted and the number of background investigations completed.



# CGS Personnel Security Capability



Version 1.1.1

## 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. Data and communication protection mechanisms exist to safeguard personnel information.
2. The Enterprise has identified the affiliates that need to be vetted and approved, as well as out-processed.
3. Policies exist that govern the screening processes.

## 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 a mechanism to investigate affiliates to verify they can be given access to facilities, systems, and information.
2. All affiliates have successfully passed a security screening process appropriate to the resource access needs prior to being granted access to facilities, systems, or information.

## 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 Personnel Security Capability provides an Organization the ability to screen personnel through mechanisms such as background investigations, NACs, credit checks, and polygraph examinations. Each Organization will ensure screenings are conducted in accordance with policy and guidelines to substantiate resource access and denial decisions.

Personnel involved in the Personnel Security process will be appropriately trained and certified, when needed. They will be aware of the governing policies for conducting investigations or polygraph examinations. Adjudication decisions will be made in



# CGS Personnel Security Capability



Version 1.1.1

accordance with the adjudicative guidelines provided by the appropriate clearance authority. Continuous evaluation will take place for all affiliates who have access to classified information.

Once an affiliate is indoctrinated for classified information, each Organization will ensure agreements are signed by applicants acknowledging their responsibilities and recognizing the Enterprise's policy regarding drug screening. This briefing will be provided through the IA Training and IA Awareness Capabilities.

Each Organization will establish policy and guidelines for how maintenance personnel and visitors will be granted short-duration access to facilities, systems, and information. Consideration will be given to the type of system and the potential information that may be within that system. For example, maintenance personnel working on copy machines may need special clearances because of the electronic information that may be stored within the system. In any case, NCIC checks will be run on personnel, and polygraphs may be required, depending on the Organization's policy.

Each Organization will provide quarterly reporting to authority Organizations and monthly reporting to Enterprise stakeholders. Reporting will include, but not be limited to, the following data: number of initial accesses granted, number of background investigations completed, number of people submitted for a clearance, number of people who received a clearance, number of people out-processed, and different types of processing that occurred.

## 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.

- Understand Mission Flows—The Personnel Security Capability relies on the Understand Mission Flows Capability to provide information about missions that feeds into decisions made regarding personnel accesses and clearances.



# CGS Personnel Security Capability



Version 1.1.1

- Understand the Physical Environment—The Personnel Security Capability relies on the Understand the Physical Environment Capability for knowledge about the personnel that use or maintain the facility and the location and activities associated with their functional role(s) to ensure that personnel have the appropriate clearances.
- Personnel Enterprise Monitoring—The Personnel Security Capability relies on the Personnel Enterprise Monitoring Capability to conduct reinvestigations and to transfer and revoke clearances.

## 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 Personnel Security 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 Personnel Security 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 Personnel Security Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Personnel Security Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities—The Personnel Security 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.

- Communication Protection—The Personnel Security Capability relies on the Communication Protection Capability to provide protection for information about personnel while in transit.
- Data Protection—The Personnel Security Capability relies on the Data Protection Capability to provide protection for personnel information.



# CGS Personnel Security Capability



Version 1.1.1

- Risk Mitigation—The Personnel Security Capability relies on the Risk Mitigation Capability to establish the necessary safeguards to ensure the continued security of the Enterprise.

## 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>	
MA-5 MAINTENANCE PERSONNEL	<p>Control: The organization:</p> <ul style="list-style-type: none"> <li>a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and</li> <li>b. Ensures that personnel performing maintenance on the information system have required access authorizations or designate organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.</li> </ul> <p>Enhancement/s:</p> <ul style="list-style-type: none"> <li>(1) The organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:               <ul style="list-style-type: none"> <li>(a) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;</li> <li>(2) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are</li> </ul> </li> </ul>



# CGS Personnel Security Capability



Version 1.1.1

	<p>cleared (i.e., possess appropriate security clearances) for the highest level of information on the system.</p> <p>(3) The organization ensures that personnel performing maintenance and diagnostic activities on information system processing, storing, or transmitting classified information are U.S. citizens.</p> <p>(4) The organization ensures that:</p> <p>(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on an information system only when the system is jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments;</p>
<p><i>PL-4 RULES OF BEHAVIOR</i></p>	<p>Control: The organization:</p> <p>a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and</p> <p>b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.</p> <p>Enhancement/s:</p> <p>(1) The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.</p>
<p><i>PS-2 POSITION CATEGORIZATION</i></p>	<p>Control: The organization:</p> <p>a. Assigns a risk designation to all positions;</p> <p>b. Establishes screening criteria for individuals filling those positions; and</p> <p>Enhancement/s: None Specified</p>
<p><i>PS-3 PERSONNEL SCREENING</i></p>	<p>Control: The organization:</p> <p>a. Screens individuals prior to authorizing access to the information system; and</p> <p>Enhancement/s:</p> <p>(1) The organization ensures that every user accessing an information system processing, storing, or transmitting</p>



# CGS Personnel Security Capability



Version 1.1.1

	<p>classified information is cleared and indoctrinated to the highest classification level of the information on the system.</p> <p>(2) The organization ensures that every user accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, is formally indoctrinated for all of the relevant types of information on the system.</p>
PS-6 ACCESS AGREEMENTS	<p>Enhancement/s:</p> <p>(1) The organization ensures that access to information with special protection measures is granted only to individuals who:</p> <p>(b) Satisfy associated personnel security criteria.</p> <p>(2) The organization ensures that access to classified information with special protection measures is granted only to individuals who:</p> <p>(b) Satisfy associated personnel security criteria consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.</p>
PS-7 THIRD-PARTY PERSONNEL SECURITY	<p>Control: The organization:</p> <p>a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;</p> <p>b. Documents personnel security requirements; and</p> <p>Enhancement/s: None Specified</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.

### Personnel Security Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other	Summary: This directive establishes personnel security policy governing eligibility for access to Sensitive Compartmented Information (SCI) and information protected within other controlled access programs. It directs application of uniform personnel security standards and procedures to facilitate effective initial vetting,



# CGS Personnel Security Capability



Version 1.1.1

Controlled Access Program Information, 1 October 2008, Unclassified	continuing personnel security evaluation, and reciprocity throughout the Intelligence Community (IC).
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. ...
<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 5200.2, DoD Personnel Security Program, 9 April 1999, Unclassified	Summary: This document establishes policy that the objective of the Department of Defense (DoD) personnel security program is that military, civilian, and contractor personnel assigned to and retained in sensitive positions, in which they could potentially damage national security, are and remain reliable and trustworthy, and there is no reasonable basis for doubting their allegiance to the United States.
DoD 5200.2-R, Personnel Security Program, January 1987, Unclassified	Summary: This document establishes policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the DoD, and granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security.
DoDD 5220.6, Defense	This directive updates policy, responsibilities, and



# CGS Personnel Security Capability



Version 1.1.1

<p>Industrial Personnel Security Clearance Review Program, 20 April 1999, Unclassified</p>	<p>procedures of the Defense Industrial Personnel Security Clearance Review Program implementing Executive Order (EO) 10865, Safeguarding Classified Information Within Industry, 20 February 1960, as amended by EO 10909, 17 January 1961; EO 11382, 28 November 1967; and EO 12829, 6 January 1993.</p>
<p>Administrative Instruction No. 23, Personnel Security Program and Civilian Personnel Suitability Investigation Program, 20 December 2006, Unclassified</p>	<p>Summary: This document implements guidance in DoD Directive (DoDD) 5200.2-R, DoD Personnel Security Program, and assigns responsibilities and prescribes procedures for administering the Personnel Security Program (PSP) and the Civilian Personnel Suitability Program (CPSP) ...</p>
<p><b>Committee for National Security Systems (CNSS)</b></p>	
<p>Nothing found</p>	
<p><b>Other Federal (OMB, NIST, ...)</b></p>	
<p>Nothing found</p>	
<p><b>Executive Branch (EO, PD, NSD, HSPD, ...)</b></p>	
<p>Executive Order 12968, Access to Classified Information, 2 August 1995, Unclassified</p>	<p>Summary: This EO establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information.</p>
<p>Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility or Access to Classified National Security Information, 30 June 2008, Unclassified</p>	<p>Summary: Executive branch policies and procedures relating to suitability, contractor employee fitness, eligibility to hold a sensitive position, access to federally controlled facilities and information systems, and eligibility for access to classified information shall be aligned using consistent standards to the extent possible, provide for reciprocal recognition, and shall ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the Federal Government relies to conduct our nation's business and protect national security.</p>
<p><b>Legislative</b></p>	



# CGS Personnel Security Capability



Version 1.1.1

Nothing found	

## Personnel Security Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICPG 704-1, Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, 2 October 2008, Unclassified	Summary: This policy guidance establishes the investigative standards to be used as the basis for conducting: National Agency Check with Local Agency Checks and Credit Check (NACLIC); Single Scope Background Investigations (SSBI), to include access to SCI and other Controlled Access Programs; and periodic reinvestigations (PR). NACLICs, SSBIs, and PRs shall be conducted in a comprehensive manner to collect and develop complete information, both favorable and unfavorable, from applicable sources. Investigations shall employ the “whole person concept” and shall be the basis for evaluating individual backgrounds and granting initial or continued access to classified national intelligence.
ICPG 704-2, Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, 2 October 2008, Unclassified	Summary: This policy guidance documents the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, as promulgated under an Office of Management and Budget memorandum dated 29 December 2005, from the Assistant for National Security Affairs.
ICPG 704-3, Denial or Revocation of Access to Sensitive Compartmented Information, other Controlled Access Program Information, and Appeals Processes , 2	Summary: This policy guidance establishes the guidelines for the denial or revocation of access to SCI and other controlled access programs and the appeal process.



# CGS Personnel Security Capability



Version 1.1.1

October 2008, Unclassified	
ICPG 704-4, Reciprocity of Personnel Security Clearance and Access Determinations, 2 October 2008, Unclassified	Summary: This policy guidance provides guidance that IC elements shall accept SSBI, SSBI-PR, and Phased PRs less than 7 years old (“in scope”) as the basis for initial or continuing access to SCI and other controlled access programs.
ICPG 704-5, Intelligence Community Personnel Security Database Scattered Castles, 2 October 2008, Unclassified	Summary: This policy guidance mandates the recognition and use of the Scattered Castles (SC) database, or successor database, as the IC's authoritative personnel security repository for verifying personnel security access approvals regarding SCI and other controlled access programs, visit certifications, and documented exceptions to personnel security standards.
<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>	
Nothing found	
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
Nothing found	
<b>Legislative</b>	
Nothing found	
<b>Other Standards Bodies (ISO, ANSI, IEEE, ...)</b>	
Nothing found	



# CGS Personnel Security Capability



Version 1.1.1

## 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. Number of people—The people needing to go through investigation, polygraphs, or other security checks will require manpower, time, and resources to process.
2. Time to implement, maintain, and execute—Otherwise productive time is lost while personnel are waiting for access.

## 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 Personnel Security Capability.

- The Enterprise shall provide mechanisms to screen affiliates, using a variety of mechanisms including background investigations, NACs, Local Agency Checks, and polygraph examinations.
- Every affiliate accessing an information system that processes, stores, or transmits classified information shall be cleared and indoctrinated to the highest classification level of the information on the system.
- Personnel security programs shall have appropriate support staff as needed, such as investigators, polygraph examiners, adjudicators, and legal authorities to independently manage its personnel security programs.



# CGS Personnel Security Capability



Version 1.1.1

- Confidential, Secret, and L clearances shall require National Agency and Local Agency Checks at a minimum.
- Top Secret, SCI, or Q clearances shall require a Single Scope Background Investigation with a periodic reinvestigation conducted every 5 years.
- Investigations shall employ the “whole person concept” and shall be the basis for evaluating an individual for initial or continued access to classified information or systems.
- Escort programs shall be implemented based on access needs.
- The Enterprise shall establish a system by which to transfer clearances to and accept clearances transferred from other Organizations, provided that the clearance is current and passes a risk assessment.
- Affiliates shall be debriefed from access when leaving the authority of the Enterprise.
- The Enterprise shall ensure that clearance databases are kept up to date with the security clearance information of affiliates.
- Clearances shall remain valid for a period of 2 years following an individual leaving the authority of the Enterprise, provided the background investigation is current.
- The Enterprise shall provide reports to its stakeholders of activity involving the clearance processing of its affiliates.