



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Personnel Enterprise Monitoring Capability

Version 1.1.1

Personnel Enterprise Monitoring is the monitoring of the personnel mechanisms and processes that prevent unauthorized access to facilities, systems, and information. The Personnel Enterprise Monitoring Capability provides assurance that the affiliates granted access to facilities, systems, and information have proper authorization and clearances and follow information assurance (IA) policies and practices.

07/30/2012



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

Table of Contents

1	Revisions	2
2	Capability Definition	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions.....	6
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations	7
7	Capability Interrelationships.....	8
7.1	Required Interrelationships	9
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 Personnel Enterprise Monitoring 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 Enterprise Monitoring 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 Enterprise Monitoring is the monitoring of the personnel mechanisms and processes that prevent unauthorized access to facilities, systems, and information. The Personnel Enterprise Monitoring Capability provides assurance that the affiliates granted access to facilities, systems, and information have proper authorization and clearances and follow information assurance (IA) policies and practices. The Personnel Enterprise Monitoring Capability establishes and executes the ongoing procedures that occur after the initial personnel security verifications, which provide a basis for granting access. 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 Enterprise Monitoring Capability provides the ability to proactively monitor and reactively gather information about affiliates, which is used to determine their continued access to facilities, systems, and information. The Personnel Enterprise Monitoring Capability shall provide mechanisms to monitor affiliates including conducting periodic investigations, polygraphs, financial disclosures, and response to adverse events. Response to adverse events is the cycle of investigation and reevaluation that occurs following an event or disclosure regarding an affiliate, such as an adverse result of a drug test, changing financial situation, or unofficial foreign travel to certain locations. This process is used to determine the impact of an event on an affiliate’s ability to maintain his or her clearance or access.

Periodic investigations shall be conducted to determine the continued security worthiness of affiliates. These investigations shall be conducted, when appropriate, in accordance with the Enterprise’s clearance adjudication policies. Investigations, along



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

with a personal interview, shall occur within 5 years of the date of the last investigation. Special investigations also shall be initiated to resolve issues that might affect continued clearance eligibility. All investigations shall be conducted by the employing agency, the Office of Personnel Management, or a contractor on behalf of the agency. Overarching policy shall determine when investigations performed by other agencies are acceptable. Agencies may expand upon the policy to define further conditions for their agency. All investigations shall be conducted according to applicable national standards, and results shall be reported to the Central Adjudication Facility (CAF) for each agency. All investigations shall be performed by trained and authorized investigators who understand standards for conducting investigations. Initial and ongoing training shall be provided by the Enterprise.

Aperiodic polygraphs shall be conducted if a polygraph is required for clearance or access. An event may occur that triggers a polygraph at any time; however, polygraphs shall be performed at least every 7 years from the last polygraph. These trigger events shall be defined within the Enterprise according to policy. Polygraphs shall be performed by trained, certified, and authorized polygraph examiners.

National adjudication criteria shall be used to measure whether an individual meets the standards for maintaining a clearance. The trained, certified, and authorized adjudicator shall review the information provided and determine if risk is acceptable for issuing a clearance based on risk analysis.

When classified information is involved, the Enterprise shall require personnel to participate annually in a financial disclosure program. This program enables an Enterprise to monitor the financial status of affiliates in accordance with national policy for information that may indicate a risk to the Enterprise. The information included in the disclosure program shall be defined by Enterprise policy. When anomalous information is discovered (e.g., unexplained debt or wealth) it shall be evaluated and adjudicated based on Enterprise standards and guidelines.

Watch profiles shall be established for affiliates with derogatory information. The profile shall be based on affiliate behaviors and criteria as established by the Enterprise Policy. A watch profile may exist because of foreign affiliations, financial issues, or some other indicator enumerated in adjudicative criteria. These profiles shall be used in conjunction with event response and other personnel monitoring activities to determine what level of analysis shall occur.



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

Additional processing shall be required when special accesses are required. The Enterprise shall define policy and standards for these events and the actions that shall occur based on the access needed. For example, when a person is submitted for additional clearances, the affiliate shall undergo verifications to ensure that no open investigations or unresolved issues are present. The Enterprise shall perform a manual review of information if a watch profile has been established for the affiliate.

The Office of Security shall review affiliate security files as needed. There shall be accountability as to why a file is reviewed, and a reason/explanation for the review shall be recorded. To ensure affiliates within the Enterprise understand that reviews may occur as needed, affiliates shall sign the appropriate agreements when becoming part of the Enterprise.

Each Enterprise shall allow for clearance reciprocity in accordance with national policy; however, each Enterprise has the authority to reevaluate a clearance if there are waivers, exceptions, or deviations from national standards. For a clearance to be accepted under reciprocity policy, 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 an investigation. In addition, a polygraph exam may be required in accordance with Enterprise policy.

The Personnel Enterprise Monitoring Capability shall ensure that affiliates are debriefed from access when leaving the authority of the Enterprise, or for cause, and the appropriate databases (Joint Personnel Adjudication System [JPAS,], Scattered Castles, etc.) reflect this 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, an investigation shall be initiated in accordance with the Personnel Security Capability.

The mechanisms discussed may be implemented both proactively and reactively. There are numerous events (such as drug testing and foreign travel) that may trigger a reactive measure. This occurs any time notification is provided to the Personnel Enterprise Monitoring Capability. Unofficial foreign travel records shall be centralized and kept electronically for searching. Records shall be protected in accordance with the Data Protection and Communication Protection Capabilities. The Personnel Monitoring Capability also relies on affiliates to provide monitoring. All affiliates are provided



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

training to report activities of others or their own that is suspicious or anomalous. Affiliates within the environment shall be educated through the IA Awareness and IA Training Capabilities to ensure they are aware of acceptable behavior. Network Enterprise Monitoring and Physical Enterprise Monitoring provide monitoring of affiliate activities regarding access once a person is logged onto the system or is within a facility. These Capabilities provide a complete personnel monitoring picture by providing notifications to the Personnel Enterprise Monitoring Capability via the Incident Response Capability. The Personnel Enterprise Monitoring Capability is responsible for determining the impact of the event on the affiliate, the risk it creates to the Enterprise, and the impact of the event on the affiliate's ability to maintain clearances and access.

All information about affiliates that is discovered by this Capability shall be passed to the Risk Analysis Capability for a risk decision. The Risk Mitigation Capability shall determine which actions shall occur to mitigate the risk. If the mitigation requires that an affiliate be terminated because of loss of clearance, information shall be provided to the Understand the Physical Environment, Access Management, and Identity Management Capabilities to update affiliate records.

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. The Enterprise has established a Security Office.
2. Affiliates are vetted and approved prior to being granted access to facilities or resources.
3. Personnel security measures have been implemented.
4. Affiliates have been properly indoctrinated and have legally, by signature, agreed to abide by the relevant Enterprise's policies.

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 employs automated monitoring of affiliates, such as periodic investigations and financial disclosures, among others. Automated monitoring occurs when a triggering event has transpired.



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

2. This Capability provides the ability to monitor affiliates based on affiliate-related events.

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).

By employing Personnel Enterprise Monitoring, the Organization will possess a capability to monitor personnel through mechanisms such as periodic investigations, polygraphs, financial disclosures, and event response. Each Organization will use a CAF, which consists of investigators, polygraph examiners (when applicable), adjudicators, and legal authorities. Each Organization will ensure policies/guidelines exist to substantiate access and denial decisions in accordance with national standards.

The Organization will perform periodic investigations to ensure that personnel remain trustworthy and reliable, and resources are protected. The Organization will ensure a personal interview and background investigation occur within 5 years of the last investigation in accordance with policy. The Organization will provide uniform training to ensure all levels of investigation are performed by qualified investigators.

When access to classified information is involved, each Organization will ensure every affiliate annually files a financial disclosure report in accordance with national policy. Depending on the size of the Organization, there may be a phased approach to include all employees. If a phased approach is used, the Organization will align the rollout with investigation cycles or some other defined trigger.

Each Organization that uses polygraph examinations for personnel security purposes will ensure they occur within established timeframes in accordance with policy. The type of polygraph examination conducted will depend on the Organization. The Organization will supply standardized training and ensure each polygraph examiner is properly trained and certified to ensure fairness and consistency.

As part of the CAF, adjudicators will review all information gathered in this Capability and determine whether an affiliate will retain his or her clearance and access based on



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

established criteria. Each Organization will ensure the CAF reviews all documentation and follows proper procedures prior to the affiliate under review receiving a denial response.

Each Organization will accept a clearance on a conditional basis if the clearance is from another Organization unless it reflects waivers, exceptions, or deviations. If so, the Organization will perform additional validation that the person is acceptable in accordance with national standards. Additional validation may be required if the Enterprise requires a polygraph.

As part of the Personnel Enterprise Monitoring Capability, each Organization will establish watch profiles for high-risk personnel or personnel with derogatory history to support event response. Watch profiles will be used along with event response to aid in determining the appropriate level of analysis that will occur upon receiving notification.

Each Organization will investigate events when notified by the Incident Response Capability in accordance with policy. Past history for foreign travel may trigger additional checks. The Organization has the authority to review this information for any reason. If there is a trigger event such as a foreign travel request, or request for special access, the Organization will conduct an electronic review. However, if the person has a watch profile, the Organization will conduct a manual review and perform more analysis for approval. Each Organization will centrally maintain records for unofficial foreign travel in support of electronic reviews.

Events may also be triggered by personnel who perform monitoring within the Organization. To do this effectively, personnel will need to gain a clear understanding of what is permitted. This is provided through the IA Training and IA Awareness Capabilities. The Organization will ensure that personnel understand roles and responsibilities with regard to operational security. Personnel will report suspicious behavior in accordance with policy. Depending on the event, notification may need to be sent to the Network Enterprise Monitoring Capability to provide overall situational awareness.

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



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

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 Enterprise Monitoring Capability relies on the Understand Mission Flows Capability to provide information about missions that feeds into decisions made regarding personnel accesses and clearances.
- Understand the Physical Environment—The Personnel Enterprise Monitoring 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 Security—The Personnel Enterprise Monitoring Capability relies on the Personnel Security Capability to perform initial investigations and assign clearances to personnel within the Enterprise.

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



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

- Organizations and Authorities–The Personnel Enterprise Monitoring 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.

- Risk Monitoring–The Personnel Enterprise Monitoring Capability relies on the Risk Monitoring Capability to make adjustments to its functions as the Enterprise risk posture changes over time.

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>	
PS-2 POSITION CATEGORIZATION	Control: The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [Assignment: organization-defined frequency]. Enhancement/s: None Specified
PS-3 PERSONNEL SCREENING	Control: The organization: b. Rescreens individuals according to [Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening]. Enhancement/s: None Applicable
PS-4 PERSONNEL TERMINATION	Control: The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews;



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

	<p>c. Retrieves all security-related organizational information system-related property; and</p> <p>d. Retains access to organizational information and information systems formerly controlled by terminated individual.</p> <p>Enhancement/s: None Specified</p>
PS-5 PERSONNEL TRANSFER	<p>Control: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action].</p> <p>Enhancement/s: None Specified</p>
PS-6 ACCESS AGREEMENTS	<p>Control: The organization:</p> <p>b. Reviews/updates the access agreements [Assignment: organization-defined frequency].</p> <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>c. Monitors provider compliance.</p> <p>Enhancement/s: None Specified</p>
PS-8 PERSONNEL SANCTIONS	<p>Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.</p> <p>Enhancement/s: None Specified</p>



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

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 Enterprise Monitoring Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 501, Discovery and Dissemination or Retrieval of Information with the Intelligence Community, 21 January 2009, Unclassified	Summary: Policy: This directive establishes in part the Director of National Intelligence (DNI) guidelines called for in Section 1.3(b)(9)(B) of EO 12333, as amended, addresses mandates in the Intelligence Reform and Terrorism Prevention Act of 2004 to strengthen the sharing, integration, and management of information within the Intelligence Community (IC), and establishes policies for: (1) discovery; and (2) dissemination or retrieval of intelligence and intelligence-related information collected or analysis produced by the IC.
ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, 1 October 2008, Unclassified	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, continuing personnel security evaluation, and reciprocity throughout the Intelligence Community (IC).
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

<p>DoDD 5200.2, DoD Personnel Security Program, 9 April 1999, Unclassified</p>	<p>Summary: This directive 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.</p>
<p>DoD 5200.2-R, Personnel Security Program, January 1987, Unclassified</p>	<p>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.</p>
<p>DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program, 20 April 1999, Unclassified</p>	<p>This directive updates policy, responsibilities, and 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 instruction implements guidance in Department of Defense 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>Committee for National Security Systems (CNSS)</p>	
<p>Nothing found</p>	
<p>Other Federal (OMB, NIST, ...)</p>	
<p>DHS Management Directive 11052, Internal Security Program, 12</p>	<p>Summary: This directive establishes the Department of Homeland Security (DHS) Internal Security Program with the mission to conduct defensive activities to analyze and</p>



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

October 2004, Unclassified	identify espionage, foreign intelligence service elicitation activities, and terrorist collection efforts directed against DHS.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Executive Order 12968, (Amended in part by EO 13467), Access to Classified Information, 2 August 1995, Unclassified	Summary: This EO establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information.
Legislative	
Nothing found	

Personnel Enterprise Monitoring 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 (NACLC); Single Scope Background Investigations (SSBI), to include access to SCI and other Controlled Access Programs; and periodic reinvestigations (PR). NACLCs, 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	Summary: This policy guidance establishes the adjudicative guidelines for determining eligibility for access to SCI and other controlled access program information.



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

Information and other Controlled Access Program Information, 2 October 2008, Unclassified	
ICPG 704.3, Denial or Revocation of Access to Sensitive Compartmented Information, other Controlled Access Program Information, and Appeals Processes, 2 October 2008, Unclassified	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.
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-PRs, and Phased Periodic Reinvestigations 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.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

Nothing found	
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:

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 scope of work should be considered for this Capability. The number of people needing reinvestigation, polygraphs, or other monitoring activities will affect the cost, speed, and efficiency of this Capability's functions.

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



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Personnel Enterprise Monitoring Capability.

- The Enterprise shall proactively monitor and reactively gather information about affiliates, which shall be used to determine their continued access to facilities, systems, and information.
- The Enterprise shall provide mechanisms to monitor affiliates including periodic investigations, polygraphs, financial disclosures, and response to adverse events, such as drug test, changing financial situation, or unofficial foreign travel.
- Periodic investigations shall be conducted in accordance with the Enterprise's clearance adjudication policies to determine the continued security worthiness of affiliates.
- Investigations, along with a personal interview, shall occur within 5 years of the date of the last investigation.
- Special Investigations shall be initiated to resolve issues that might affect continued clearance eligibility.
- All investigations shall be conducted by the employing agency, the Office of Personnel Management, or a contract provider on behalf of the agency. Overarching policy shall determine when investigations performed by other agencies are acceptable.
- All investigations shall be conducted according to applicable national standards, and results shall be reported to the CAF for each agency.
- All investigations shall be performed by trained and authorized investigators who understand standards for conducting investigations. Initial and ongoing training shall be provided by the Enterprise.
- A periodic polygraph shall be conducted by trained, certified, and authorized polygraph examiners if a polygraph is required for clearance or access.
- A periodic polygraph shall occur at anytime but not to exceed 7 years. However, an event may occur that triggers a polygraph at any time. These trigger events shall be defined within the Enterprise according to policy.
- A trained, certified, and authorized adjudicator shall review the information provided and use national adjudication criteria to measure whether an individual meets the standards for maintaining a clearance.
- When classified information is involved, the Enterprise shall require personnel to participate annually in a financial disclosure program in order to monitor the financial status of affiliates in accordance with national policy.
- The information included in the financial disclosure program shall be defined by Enterprise policy and when anomalous information is discovered (e.g.,



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

unexplained debt or wealth), it shall be evaluated and adjudicated based on Enterprise standards and guidelines.

- Watch profiles shall be established for affiliates with derogatory information, based on criteria established by Enterprise Policy and affiliate behaviors, such as foreign affiliations or financial issues.
- Watch profiles shall be used in conjunction with event response and other personnel monitoring activities to determine what level of analysis shall occur.
- Additional processing may be required when special accesses are required. The Enterprise shall define policy and standards regarding when additional processing is required for special access requests.
- The Office of Security shall review affiliate security files as needed and the reason/explanation for the review shall be recorded.
- Affiliates shall sign the appropriate agreements when joining the Enterprise to ensure they understand that review of security files may occur as needed.
- Each Enterprise shall allow for clearance reciprocity in accordance with national policy; however, each Enterprise shall reevaluate a clearance if there are waivers, exceptions, or deviations from national standards.
- A clearance shall be accepted under reciprocity policy only if the background investigation is 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 an investigation and conduct a polygraph exam if required by policy.
- The Enterprise shall ensure that affiliates are debriefed from access when leaving the authority of the Enterprise or for cause, and appropriate databases (JPAS, Scattered Castles, etc.) reflect the current information.
- An individual's clearance shall remain active for 2 years after being debriefed to allow individuals to have their clearances reinstated without additional security processing.
- If at the time of reinstatement an individual's background investigation is out of scope, an investigation shall be initiated.
- Unofficial foreign travel records shall be electronically maintained in a centralized manner and protected.
- All affiliates shall be educated in IA Awareness to ensure they are aware of acceptable behavior and to report suspicious or anomalous activities of self and others.



CGS Personnel Enterprise Monitoring Capability



Version 1.1.1

- The Enterprise shall receive notifications of events regarding access once a person is logged onto the system or is within a facility to provide a complete personnel monitoring picture.
- The Enterprise shall determine the impact of an event on the affiliate, the risk it creates to the Enterprise, and the impact of the event on the affiliate's ability to maintain clearances and access.