



National Security Agency/Central Support Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Physical Enterprise Monitoring Capability

Version 1.1.1

Physical Enterprise Monitoring is the monitoring of the physical and environmental controls that prevent unauthorized physical access to facilities, systems, or other resources. This Capability includes the monitoring of the environment, systems, hazards, and other resources; it ensures that the physical and environment protection systems are still effective when changes occur.

07/30/2012



# CGS Physical 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 .....	5
5	Capability Post-Conditions.....	5
6	Organizational Implementation Considerations .....	6
7	Capability Interrelationships.....	7
7.1	Required Interrelationships .....	7
7.2	Core Interrelationships .....	7
7.3	Supporting Interrelationships.....	8
8	Security Controls .....	8
9	Directives, Policies, and Standards .....	10
10	Cost Considerations .....	13
11	Guidance Statements.....	13



# CGS Physical 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 Physical 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.

Physical Enterprise Monitoring is the monitoring of the physical and environmental controls that prevent unauthorized physical access to facilities, systems, or other resources. This Capability includes the monitoring of the environment, systems, hazards, and other resources; it ensures that the physical and environment protection systems are still effective when changes occur.

## 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 Physical Enterprise Monitoring Capability addresses the ability to gather status information about the physical and environmental controls that prevent unauthorized physical access to facilities, systems, or other resources. The Capability shall continuously gather information on the environment, hazards (such as chemical, biological, and fire), physical protections on equipment (such as workstations, case sensors, or routers), environmental systems (such as heating, ventilation, and air conditioning [HVAC]), as well as unauthorized cell phone usage. Monitoring shall be performed automatically, by physical security intrusion detection systems (closed-circuit television [CCTV] on facility doors and alarmed fencing) on a 24 hours/7 days a week (24x7) basis. Monitoring shall be in real-time or near real-time, depending on what is being monitored (monitoring for alarms shall be real-time and for CCTV shall be near real-time). The Enterprise shall evaluate its physical and environmental protections and determine what needs to be real-time and near real-time depending on its priority and mission, including temperature and humidity monitoring. The Enterprise shall decide if everything physical needs to be monitored. Visual inspection shall be used when automated mechanisms are down for maintenance and may involve special requirements for personnel depending on the physical monitoring activity.



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

Physical Enterprise Monitoring is an important part of providing overall Enterprise situational awareness. Everyone in the Enterprise is responsible for physical monitoring; therefore, each department or agency shall have appropriate monitoring authorizations and agreements in place and a program, staff, and plan to administer, report, and follow up on assessments and incident investigations. The mechanisms implemented to perform monitoring shall meet high-availability requirements to perform their function of ensuring that any changes do not affect the physical and environment protection systems' effectiveness.

This Capability also addresses the ability to detect external people without appropriate access or with appropriate access but not for specific devices or systems (i.e., tamper), as well as to detect intentional and unintentional anomalies associated with the physical components of a network and with the facilities in which the network resides. Physical Enterprise Monitoring works with Personnel Enterprise Monitoring to monitor the personnel mechanisms and processes in place that provide assurance that the personnel granted access to facilities, resources, and information are properly cleared to access the resources (e.g., information, facilities). Physical Enterprise Monitoring shall monitor personnel presence information (i.e., entrance and exit timestamps and whether personnel are within the confines of the facility, not necessarily an individual's exact location). That information can then be correlated with information from Network Enterprise Monitoring and Access Management to provide a more robust monitoring capability. For example, an alert shall be provided when an individual's presence information indicates he or she is in one facility, but he or she logs onto a system in a facility where he or she is not present. The procedures that shall be followed when personnel enter and exit the facility are defined in accordance with policies set by the Community and Enterprise IA Policies, Procedures, and Standards.

The Physical Enterprise Monitoring Capability shall monitor environmental systems such as chemical, biological, fire, and HVAC. All alerts will go to incident response; however, certain alarm alerts will go to other alarm response areas as defined by policy (i.e., fire alarms will go to incident response as well as to other first responders). Although the monitoring of these environmental systems is included within the scope of this Capability, the personnel involved with the monitoring these systems may be separate from the personnel who are involved in the monitoring of the physical security systems.

This Capability shall collect information on physical and environmental controls the Enterprise needs to have monitored. The level of detail of location information provided shall be related to the intended purpose and users of that control. In the case of legacy



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

physical and environmental systems that cannot be monitored, the decision regarding what information to capture and how to report it shall be based on mission needs determined by the Enterprise. The information collected shall include the date/time stamps indicating the last time the information was captured, location, system information (unique identifier, device type), type of event, and who or what reported the alert; this information will ensure information collected about event changes is as accurate as possible. When implemented, this Capability shall provide the information to the Know the Enterprise Capabilities, ensuring that enough information is provided such that it can be included within graphical user interface presentations, which provide the ability to drill down into component detail as needed.

## 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 appropriate physical and environmental protections are in place.
2. Everyone in the Enterprise is responsible for physical monitoring.
3. All Enterprise personnel are properly trained to assist with physical enterprise monitoring.

## 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 monitoring of surveillance equipment.
2. The Capability provides secure storage of surveillance recordings for a reasonable length of time.
3. Facilities uses physical alarm systems, CCTV, human guards, and other physical monitoring mechanisms.
4. Facilities uses environmental alarm systems and monitors for hazards such as chemical, biological, and fire.
5. The Capability provides alerts and forensic data that can be analyzed at a later time.



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

## 6 Organizational Implementation Considerations

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

When Physical Enterprise Monitoring is employed correctly, the Organization will possess a capability to monitor physical and environmental changes through automated monitoring tools in a near-real-time capacity. The Organization will employ high-availability systems to perform continuous monitoring activities automatically, by physical security intrusion detection systems (CCTV on facility doors, and alarmed fencing) on a 24x7 basis in real-time or near real-time, depending on what is being monitored (monitoring of alarms will be in real-time and of CCTV will be in near real-time). The Organization will continuously monitor physical Enterprise activities and physical and environmental health and status and maintain an accurate situational awareness picture. The Organization will also leverage data from other Capabilities such as Network Enterprise Monitoring, Personnel Enterprise Monitoring, and Incident Response to maintain awareness of changes in network components and configuration baselines to ensure that any changes do not impact the physical and environment protection systems' effectiveness. The Organization may use this information if anomalous activity is detected.

The Organization will establish a 24-hour physical operations center, appropriately staffed to monitor the physical and environment status; and determine the location of physical or environmental mechanisms being monitored based on mission needs for monitoring and the type of monitoring data required. The data collected will also be maintained based on mission need for that data. Notifications will be sent to incident response; however, certain alarm alerts will go to other alarm response areas as defined by policy (i.e., fire alarms will go to incident alerts response as well as to other first responder areas).

The Organization will ensure that it has the appropriate monitoring authorizations and agreements in place and a program, staff, and plan to administer, report, and follow up on assessments and incident investigations. The Organization will also ensure that the mechanisms implemented to perform monitoring meet the high-availability requirements to perform their function of ensuring that any changes do not impact the physical and environment protection systems' effectiveness.



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

## 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 Physical Enterprise Monitoring Capability relies on the Understand Mission Flows Capability to provide information about mission flows within the Enterprise, also contributing to the situational awareness picture.
- Understand the Physical Environment—The Physical Enterprise Monitoring Capability relies on the Understand the Physical Environment Capability for knowledge of the physical and environmental resources within the environment (i.e., personnel, gates, doors, surveillance equipment, fences, and mechanical and electrical machinery).
- Physical and Environmental Protections—The Physical and Environmental Protections Capability relies on the Physical Enterprise Monitoring Capability to monitor the physical controls that prevent unauthorized access to facilities or resources.
- Network Enterprise Monitoring—The Physical Enterprise Monitoring Capability relies on the Network Enterprise Monitoring Capability to provide information that contributes to the situational awareness picture (e.g., identify if an individual has not entered a facility and is trying to log into network devices located within the facility).

### 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 Physical 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 Physical 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.



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

- IA Awareness–The Physical 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 Physical Enterprise Monitoring Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Physical 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 Physical 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>	
PE-3 <i>PHYSICAL ACCESS CONTROL</i>	Enhancement/s: (3) The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week. (5) The information system detects/prevents physical tampering or alteration of hardware components within the system.
PE-6 <i>MONITORING PHYSICAL ACCESS</i>	Control: The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency]; and



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

	<p>c. Coordinates results of reviews and investigations with the organization's incident response capability.</p> <p>Enhancement/s:</p> <p>(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.</p> <p>(2) The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.</p>
PE-7 VISITOR CONTROL	<p>Enhancement/s:</p> <p>(1) The organization escorts visitors and monitors visitor activity, when required.</p>
PE-8 ACCESS RECORDS	<p>Control: The organization:</p> <p>b. Reviews visitor access records [Assignment: organization-defined frequency].</p> <p>Enhancement/s:</p> <p>(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.</p>
PE-13 FIRE PROTECTION	<p>Enhancement/s:</p> <p>(1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.</p> <p>(2) The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.</p>
PE-14 TEMPERATURE AND HUMIDITY CONTROLS	<p>Control: The organization:</p> <p>b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].</p> <p>Enhancement/s:</p> <p>(2) The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.</p>
PE-16 DELIVERY AND REMOVAL	<p>Control: The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.</p> <p>Enhancement/s: None Specified.</p>



# CGS Physical 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.

### Physical Enterprise Monitoring Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 705, Sensitive Compartmented Information Facilities, 26 May 2010, Unclassified	Summary: 1. This directive establishes that all Intelligence Community (IC) Sensitive Compartmented Information Facilities (SCIF) shall comply with uniform IC physical and technical security requirements (hereinafter “uniform security requirements”). This mandate is designed to ensure the protection of information and foster efficient, consistent, and reciprocal use of SCIFs in the IC. This directive applies to all facilities accredited by IC elements where Sensitive Compartmented Information (SCI) is processed, stored, or discussed. This directive rescinds Director of Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, including the Manual for Physical Security Standards for Sensitive Compartmented Information Facilities, and all DCID 6/9 Annexes. This directive also rescinds IC Policy Memorandum (ICPM)2005-700-1, Intelligence Community Update to Director of Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs); ICPM 2006-700-7, Intelligence Community Modifications to DCID 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)”; and ICPM 2007-700-2, Intelligence Community Modifications to Annex C of Director of Central Intelligence Directive 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs).”
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoD 5200.1-R, Information Security Program, 14 January 1997, Unclassified	Summary: This document establishes the Department of Defense (DoD) Information Security Program to promote proper and effective classification, protection, and downgrading of official information requiring protection in the interest of national security. It specifies requirements for an intrusion detection system (IDS) to be used for the effective storage of classified information to prevent access by unauthorized persons.
DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 28 February 2006, Unclassified	Summary: The National Industrial Security Program (NISP) was established by Executive Order (E.O.) 12829 for the protection of classified information ... The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense has been designated Executive Agent for the NISP by the President. The Director, Information Security Oversight Office (ISOO), is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies. Among other things, the National Industrial Security Program Operating Manual (NISPOM) specifies the minimum standards for an approved IDS when supplemental protection is required for Top Secret and Secret material. The IDS shall be connected to, and monitored by, a central monitoring station.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
DHS Management Directive 11035, Industrial Security Program, 2 October 2005,	Summary: This directive establishes the Industrial Security Program for the Department of Homeland Security (DHS) to ensure that U.S. industry partners performing work for DHS as contractors, subcontractors, consultants, licensees, and



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

Unclassified	grantees, and involving access to classified information, comply with the standards for safeguarding such information pursuant to the NISP, administered by DoD as Executive Agent and to which DHS is a signatory. The NISPOM (DoD 5220.22-M) gives practical application to the objectives of the NISP. Among other things, the NISPOM specifies the minimum standards for an approved IDS when supplemental protection is required for Top Secret and Secret material. The IDS shall be connected to, and monitored by, a central monitoring station.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

## Physical Enterprise Monitoring Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

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 storage requirements should be considered for this Capability. This Capability requires storage facilities for security monitoring data.

## 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 Physical Enterprise Monitoring Capability.

- The Enterprise shall have appropriate monitoring authorizations and agreements in place and a program, staff, and plan to administer, report, and follow up on assessments and incident investigations.



# CGS Physical Enterprise Monitoring Capability



Version 1.1.1

- The mechanisms implemented to perform monitoring shall meet high-availability requirements to perform their function of ensuring that any changes do not affect the physical and environment protection systems' effectiveness.
- The Enterprise shall monitor the physical and environmental controls that prevent unauthorized physical access to facilities, systems, or other resources. Monitoring of the environment, systems, hazards, and other resources will be supported by the Enterprise to ensure that the physical and environment protection systems are still effective when changes occur.
- The Enterprise shall detect external people without appropriate access or with appropriate access but not for specific devices or systems (i.e., tamper).
- The Enterprise shall detect intentional and unintentional anomalies associated with the physical components of a network and with the facilities in which the network resides.
- The Enterprise shall monitor the personnel mechanisms and processes in place that provide assurance that the personnel granted access to facilities, resources, and information are properly cleared to access the resources (e.g., information, facilities).
- The Enterprise shall monitor personnel presence information (i.e., entrance and exit time stamps and whether personnel are within the confines of the facility, not necessarily an individual's exact location).
- Physical enterprise monitoring information shall be correlated with information from network enterprise monitoring and access management information to provide for more robust monitoring.
- The procedures followed when personnel enter and exit the facility shall be defined in accordance with policies set by the Community and Enterprise IA Policies, Procedures, and Standards.
- The Enterprise shall monitor environmental systems such as chemical, biological, fire, and HVAC and provide alarm alerts.
- The Enterprise shall collect information on physical and environmental controls that require monitoring including date-time stamps indicating the last time the information was captured, location, system information (unique identifier, device type), type of event, and who or what reported the alert.
- In the case of legacy physical and environmental systems that cannot be monitored, the Enterprise shall determine what information should be captured and how to report the information, based on mission needs.
- Information collected for physical and environmental controls shall be visible through graphical user interface presentations, which provide the ability to drill down into component detail as needed.