



National Security Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Understand the Physical Environment Capability

Version 1.1.1

Understand the Physical Environment provides knowledge of the facilities and physical resources being used and provides Enterprise personnel, designated staff, and visitor entry and exit information as well as any interdependencies.

07/30/2012



# CGS Understand the Physical Environment 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.....	7
8	Security Controls .....	8
9	Directives, Policies, and Standards .....	8
10	Cost Considerations .....	13
11	Guidance Statements.....	14



# CGS Understand the Physical Environment 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 Understand the Physical Environment 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.

Understand the Physical Environment provides knowledge of the facilities and physical resources being used and provides Enterprise personnel, designated staff, and visitor entry and exit information as well as any interdependencies. Physical Environment includes people, facilities, geographic location, and climate, among other physical considerations.

## 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 Understand the Physical Environment Capability accounts for all people, facilities, and environmental factors within the Enterprise. The Understand the Physical Environment Capability shall have knowledge of all facilities that house system resources; the mechanisms used to support facility operation such as power (including primary and secondary back-ups), space, cooling, and telecommunications, guards, reinforced walls, gates, cameras, motion sensors, alarms, checkpoints, and locks; and people within the environment, including users, visitors, maintenance workers, as well as unauthorized personnel. This knowledge is necessary to protect against compromise of facilities, resources, or information from various applicable environmental impacts such as temperatures, fire, flood, tornado, and other natural disasters or occurrences.

Information captured by the Understand the Physical Environment Capability shall be documented, accessible, and searchable in electronic form and contain all preventative and maintenance records that contain any repairs or modifications performed on the facility or subsystems including anything that is added or removed from these systems. Capture of personnel, facilities, and environmental information shall be in electronic form:



# CGS Understand the Physical Environment Capability



Version 1.1.1

- Personnel information shall include attributes about the personnel, such as employment status (e.g., employee, contractor, visitor, full-time, part-time, and others as defined by the Enterprise); location (geographic and facility); nationality; workplace contact information; and others as determined by the Organization for environmental response considerations. These attributes shall be documented and the Understand the Physical Environment Capability shall work with the Physical and Environmental Protections Capability to ensure the appropriate protections are in place. Personnel information shall be maintained by a personnel organization. However, the data shall also be used by Personnel Security and updated with security information. The Understand the Physical Environment Capability shall pass information to Personnel Security to enable it to determine the controls in place on people such as clearance requirements, among others.
- Facilities information shall include attributes, such as physical characteristics of the facility including the location of doors, windows, power, and heating, ventilating, and air conditioning (HVAC) sources; and proximity to emergency services, physical location (geographic, proximity to other locations, location of air intakes for airborne threats, proximity to critical infrastructure services, including underground utility); manned or unmanned; type of facility (TEMPEST Zone, sensitive compartmented information facility [SCIF], partial SCIF, open); and fixed or mobile. This information shall be accessible by facility decision-makers within the Enterprise to determine physical controls that need to be implemented in accordance with Physical and Environmental Protections requirements that are levied according to the location and mission of the Enterprise.
- Environmental information shall include attributes such as climate, humidity, flood plain, natural occurrences, and geographical location. This information shall feed into Physical and Environmental Protections and Contingency Planning. Therefore, this information shall be captured and documented so that the Understand the Physical Environment Capability can use and provide this information to Physical and Environmental Protections in responding to environmental and security alerts.

Understand the Physical Environment shall capture and document physical communication link locations, as well as everything that could provide a disruption to normal business operations or allow for unauthorized physical, visual, or acoustical access during hours of operation. Planned and ongoing construction of all facilities shall



# CGS Understand the Physical Environment Capability



Version 1.1.1

be coordinated to avoid disruption of normal business operations. These conditions shall also be provided to the Contingency Planning Capability for planning purposes.

When changes are made to facilities, personnel, or environmental factors, Physical and Environmental Protections, Physical Hunting, Personnel Enterprise Monitoring, Physical Enterprise Monitoring, and Personnel Security shall be provided with the change. In addition, these Capabilities shall be provided with the following information: the persons or facilities involved, and the date and time the change was made to ensure an accurate baseline of personnel, physical, and environmental activities are in place before any personnel, facility, or environmental changes are made. Personnel information shall be reviewed and updated when new people are added to the Enterprise or terminated, or new visitors, maintenance, and other personnel are introduced.

## 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. Protections are in place to ensure the security of personnel as well as physical and environmental resources.
2. The Organization provides a human resources organization responsible for tracking new, current, or former employees.
3. The Organization has a facilities oversight organization responsible for tracking facilities, maintaining environments, and ensuring that changes have been reviewed and approved.
4. Other mission assets may inherit some environment safeguards (e.g., physical locks safeguard against theft of asset).
5. The Organization has identified the functional role of the facility and the personnel as related to supporting the mission.
6. The Organization has personnel and processes in place to identify visitors and maintenance personnel.

## 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.



# CGS Understand the Physical Environment Capability



Version 1.1.1

1. This Capability provides an understanding of the dynamics of the environment and the changes that occur.
2. This Capability documents the information assurance (IA) or IA-related attributes associated with people, facilities, and the environment.

## 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 the Understand the Physical Environment Capability is employed correctly, the Organization will possess the ability to know, document, and correlate the locations and attributes associated with people, facilities, and the environment within its Enterprise. This Capability will work with Physical and Environmental Protections to document storage of sensitive information; geographic location; climate environment; facility housing system resources, the system resources themselves, and the mechanisms used to support their operation; and people within the environment, including users, visitors, maintenance workers, as well as unauthorized personnel associated with this Capability.

An Organization will ensure that it has knowledge of the protections that are in place to protect against compromise of facilities, resources, or information from various applicable environmental impacts such as temperatures, fire, flood, tornado, and other natural disasters or occurrences. This information will be well documented, available, accessible, and searchable in electronic form within the Understand the Physical Environment Capability.

Organizations will ensure that any changes made to facilities, personnel, or environmental factors are provided to Physical and Environmental Protections, Physical Hunting, and Personnel Security. This information will include the change, the persons or facilities involved, and the date and time the change was approved and implemented so that they may ensure the appropriate protections are in place.



# CGS Understand the Physical Environment 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.

- Personnel Enterprise Monitoring–The Understand Physical Environment Capability relies on the Personnel Enterprise Monitoring Capability for notification when an affiliate leaves the purview of the Organization.

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



# CGS Understand the Physical Environment Capability



Version 1.1.1

- Network Security Evaluations—Understand the Physical Environment Capability relies on the Network Security Evaluations Capability for information that is used to fill any gaps that may exist.
- Risk Mitigation—The Understand the Physical Environment Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.

## 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-2 PHYSICAL ACCESS AUTHORIZATIONS	Control: The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible)
PE-3 PHYSICAL ACCESS CONTROL	Control: The organization: f. Inventories physical access devices [Assignment: organization-defined frequency]

## 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.

### Understand the Physical Environment 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



# CGS Understand the Physical Environment Capability



Version 1.1.1

	<p>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, <i>Physical Security Standards for Sensitive Compartmented Information Facilities</i>, including the <i>Manual for Physical Security Standards for Sensitive Compartmented Information Facilities</i>, and all DCID 6/9 Annexes. This directive also rescinds IC Policy Memorandum (ICPM) 2005-700-1, <i>Intelligence Community Update to Director of Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)</i>; ICPM 2006-700-7, <i>Intelligence Community Modifications to DCID 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)”</i>; and ICPM 2007-700-2, <i>Intelligence Community Modifications to Annex C of Director of Central Intelligence Directive 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs).”</i>”</p>
<p><b>Comprehensive National Cybersecurity Initiative (CNCI)</b></p>	
<p>NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified</p>	<p>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.</p>
<p><b>Department of Defense (DoD)</b></p>	
<p>DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 28 February 2006,</p>	<p>Summary: This manual contains detailed security requirements to be followed by U.S. contractors for safeguarding classified information. It addresses the conduct of industrial security surveys (purpose to obtain sufficient facts to permit an administrative determination to</p>



# CGS Understand the Physical Environment Capability



Version 1.1.1

<p>Unclassified</p>	<p>grant or deny a facility security clearance) and facility security clearance surveys (purpose to obtain information about a facility to determine if it is and/or remains capable of properly safeguarding classified information).</p>
<p>DoD 5220.22-R, Industrial Security Regulation, 4 December 1985, Unclassified</p>	<p>Summary: Regulation sets forth policies, practices, and procedures of the Department of Defense (DoD) Industrial Security Program to ensure the safeguarding of classified information in the hands of U.S. industrial Organizations, educational institutions, and all Organizations and facilities used by prime and subcontractors. It implements DoD 5220.22-M (see above).</p>
<p>DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007, Unclassified</p>	<p>Summary: This instruction establishes the DoD Information Assurance Certification and Accreditation Process (DIACAP) for authorizing the operation of DoD information systems (IS). The process manages the implementation of information assurance (IA) capabilities and services and provides visibility of accreditation decisions. The process includes the need to fully understand and document the IS's physical environment.</p>
<p>DoD Intelligence Information Systems (DoDIIS) Certification and Accreditation Guide, April 2001, Classified</p>	<p>Summary: This document provides security guidance for developing or modifying an IS designed to process SCI under the purview of the Director, Defense Intelligence Agency (DIA). It describes the structured process of achieving security certification and accreditation (C&amp;A) of DoD intelligence ISs and defines the security roles and responsibilities of the various Organizations involved. The first phase is "Definition," which focuses on understanding the IS requirement, the environment in which the IS will operate, the uses of the IS, the security requirements that apply to the IS, and the level of effort necessary to achieve accreditation.</p>
<p>DISA Enclave Security Technical Implementation Guide (STIG), version 4.2, 10 March 2008,</p>	<p>Summary: This Security Technical Implementation Guide (STIG) provides Organizations an overview of the applicable policy and additional STIG documents required to implement secure ISs and networks while ensuring</p>



# CGS Understand the Physical Environment Capability



Version 1.1.1

Unclassified	interoperability. It describes the minimum requirements, standards, controls, and options for securing the enclave as a whole and presents technical guidance to secure specific enclave components in detail. Establishing a detailed understanding of the enclave—consists of the “Enclave Perimeter” and “Computing Environment” layers in the Defense-in-Depth architecture (includes all components of the network, application, and host layers)—leading to a clear and concise security policy is prerequisite to the application of sufficiently robust security safeguards.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

## Understand the Physical Environment Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Joint DoDIIS /Cryptologic SCI Information Systems Security Standards,	Summary: This document provides procedural guidance for the protection, use, management, and dissemination of SCI. The combination of security safeguards and



# CGS Understand the Physical Environment Capability



Version 1.1.1

<p>Revision 4, 1 January 2006, Unclassified</p>	<p>procedures used for IS shall achieve U.S. government policy that all classified information must be appropriately safeguarded to ensure the confidentiality, integrity, and availability of that information. It describes the structured process of achieving security C&amp;A of DoD intelligence ISs and defines the security roles and responsibilities of the various Organizations involved. The first phase is "Definition," which focuses on understanding the IS requirement, the environment in which the IS will operate, the uses of the IS, the security requirements that apply to the IS, and the level of effort necessary to achieve accreditation.</p>
<p>Committee for National Security Systems (CNSS)</p>	
<p>Nothing found</p>	
<p>Other Federal (OMB, NIST, ...)</p>	
<p>NIST SP 800-35, Guide to Information Technology Security Services, October 2003, Unclassified</p>	<p>Summary: This special publication (SP) provides assistance with the selection, implementation, and management of information technology (IT) security services by guiding Organizations through the various phases of the IT security services lifecycle. Phase 2 of the six-step cycle is Assessment, which begins with establishing a baseline understanding of the current environment.</p>
<p>NIST SP 800-37 Rev-1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010, Unclassified</p>	<p>This publication transforms the traditional C&amp;A process into the six-step risk management framework (RMF). It provides guidelines for applying the RMF to federal IS including conducting the activities of security categorization, security control selection and implementation, security control assessment, IS authorization, and security control monitoring. Before the security controls that implement physical and environmental protections can be selected and deployed, it is necessary to fully understand the IS's physical environment.</p>
<p>NIST SP 800-39,</p>	<p>Summary: This SP provides guidelines for managing risk to</p>



# CGS Understand the Physical Environment Capability



Version 1.1.1

Managing Information Security Risk: Organization, Mission, and Information System View, March 2011, Unclassified	organizational operations, organizational assets, individuals, other Organizations, and the nation resulting from the operation and use of ISs. It implements an RMF, a structured, yet flexible approach for managing that portion of risk resulting from the incorporation of IS into the mission and business processes of Organizations. Selecting and deploying security controls that implement physical and environmental protections require a complete understanding of the IS's physical environment.
NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, Revision 1, February 2006, Unclassified	Summary: This SP provides guidance and describes a process for developing system security plans. Understanding a system's operating environment is an important step in the process.
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



# CGS Understand the Physical Environment Capability



Version 1.1.1

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. Size of facility—Larger facilities will be more difficult and costlier to monitor. If the size of the facility changes, scalability of the solution may become an issue.
2. Geographic location—The environment and location of the facility may add additional costs to its monitoring.
3. Number of personnel—The personnel who use and visit a facility will affect operations and the environment and so they must be tracked as well.

## 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 Understand the Physical Environment Capability.

- The Enterprise shall possess complete knowledge of its physical environment including facilities that house system resources; the mechanisms used to support facility operation such as power (including primary and secondary backups), space, cooling, and telecommunications, guards, reinforced walls, gates, cameras, motion sensors, alarms, checkpoints, and locks; and people within the environment, including users, visitors, maintenance workers, as well as unauthorized personnel.
- The Enterprise shall account for all people, facilities, and environmental factors within its Enterprise.
- Knowledge of the Enterprise's physical environment shall be used to protect against compromise of facilities, resources, or information from various applicable environmental impacts such as temperatures, fire, flood, tornado, and other natural disasters or occurrences.
- Information related to the Enterprise's physical environment shall be documented, accessible, and searchable in electronic form and contain all preventative and maintenance records that contain any repairs or modifications



# CGS Understand the Physical Environment Capability



Version 1.1.1

performed on the facility or subsystems including anything that is added or removed from these systems.

- Personnel information shall include attributes about the personnel, such as employment status (e.g., employee, contractor, visitor, full-time, part-time, and others as defined by the Enterprise); location (geographic and facility); nationality; workplace contact information; and others as determined by the organization for environmental response considerations.
- Personnel attributes shall be documented to ensure the appropriate protections are in place.
- The Enterprise shall pass information from the physical environment to personnel security to determine the controls in place on people, such as clearance requirements, among others.
- Enterprise facilities information shall include attributes, such as physical characteristics of the facility, including the location of doors, windows, power, and heating, ventilating, and air conditioning (HVAC) sources; and proximity to emergency services, physical location (geographic, proximity to other locations, location of air intakes for airborne threats, proximity to critical infrastructure services, including underground utility); manned or unmanned; type of facility (TEMPEST Zone, sensitive compartmented information facility [SCIF], partial SCIF, open); and fixed or mobile.
- Enterprise facilities information shall be accessible by facility decision-makers within the Enterprise to determine physical controls that need to be implemented in accordance with requirements that are levied according to the location and mission of the Enterprise.
- Environmental information shall include attributes such as climate, humidity, flood plain, natural occurrences, and geographical location.
- The Enterprise shall capture and document environmental information so that the physical environment can use and provide this information in responding to environmental and security alerts.
- The Enterprise shall capture and document physical communication link locations, as well as other connections that could provide a disruption to normal business operations or allow for unauthorized physical, visual, or acoustical access during hours of operation.
- Planned and ongoing construction of all facilities shall be coordinated to avoid disruption of normal business operations.
- All changes made to a facility, personnel, or environmental factors shall be updated on other Enterprise systems, such as physical and environmental



# CGS Understand the Physical Environment Capability



Version 1.1.1

protections, physical hunting, personnel enterprise monitoring, physical enterprise monitoring, and personnel security systems.

- The Enterprise shall ensure that an accurate baseline of personnel, physical, and environmental activities is in place before any personnel, facility, or environmental changes are made. Such changes shall include the persons or facilities involved, and the date and time the change was made.
- Personnel information shall be reviewed and updated when new people are added to the Enterprise or terminated, or new visitors, maintenance, and other personnel are introduced.