



National Security Agency/Central Support Service



INFORMATION ASSURANCE DIRECTORATE

CGS Physical and Environmental Protections Capability

Version 1.1.1

Physical and Environmental Protection consists of security in-depth measures that prevent unauthorized access to facilities or resources; protects resources from natural/unnatural disasters, hazards, and physical and environmental attacks; and encompasses environmental protection, which prevents loss or compromise of facilities, resources, or information resulting from environmental impacts such as temperature, fire, or flood.

07/30/2012



CGS Physical and Environmental Protections 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.....	7
6	Organizational Implementation Considerations	7
7	Capability Interrelationships.....	10
7.1	Required Interrelationships	10
7.2	Core Interrelationships	11
7.3	Supporting Interrelationships.....	11
8	Security Controls	12
9	Directives, Policies, and Standards	18
10	Cost Considerations	23
11	Guidance Statements.....	24



CGS Physical and Environmental Protections 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 and Environmental Protections 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 and Environmental Protection consists of security in-depth measures (i.e., access controls, cameras, fencing, lighting) that prevent unauthorized access to facilities or resources (i.e., hardware, software); protects resources from natural/unnatural disasters, hazards, and physical and environmental attacks; and encompasses environmental protection, which prevents loss or compromise of facilities, resources, or information resulting from environmental impacts such as temperature, fire, or flood. This Capability allows only people with the proper authorization access to the facilities or information and provides protections for resources even when they are not inside a protected facility (i.e., in the field).

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.

Physical and environmental security controls are implemented to prevent unauthorized access to or use of personnel, equipment, installations, and information. The Physical and Environmental Protections Capability shall safeguard these resources against espionage, sabotage, terrorism, damage, and criminal activity. The determination of which controls need to be in place and the protection measures to be employed is based on the type and location of the building. These protection measures include guards, reinforced walls, gates, cameras, motion sensors, alarms, checkpoints, and locks, among others. Environmental protections shall also be in place to protect against compromise of facilities, resources, or information from various applicable environmental impacts including temperature, fire, flood, tornado, and other natural disasters or occurrences. This Capability shall work with Understand Physical Environment, Hardware Device Inventory, and Software Inventory to document the responsible party, placement of the protection mechanism, and protection capability.



CGS Physical and Environmental Protections Capability



Version 1.1.1

All plumbing shall be constructed of resilient materials. Computer equipment and other water-sensitive materials are, as much as possible, positioned away from plumbing so if there is a leak, the damage is reduced. Plumbing located near mission-critical equipment or in mission-critical areas shall feature leak detection capabilities. The locations of emergency shutoff valves shall be known, in case there is a serious leak that cannot be patched quickly enough.

During building design and construction, the Enterprise shall comply with all security precautions set forth by the Acquisition Capability with regard to acquiring materials, plans, and construction personnel. The Enterprise shall work with the Acquisition Capability to develop a Construction Security Plan (CSP) prior to the construction or rehabilitation of Sensitive Compartmented Information Facilities (SCIFs). The CSP addresses acquisition of materials, vetting of workers, escort, and use of construction surveillance technicians all in an attempt to ensure the protection and integrity of the facility from conception to grave. The Enterprise shall designate a Facility Security Officer or Physical Security personnel to oversee and ensure compliance with the security requirements during construction and operations. These personnel shall receive applicable training by the IA Training Capability.

An escort program shall be established for the purpose of escorting personnel in secure spaces when they are not cleared to the highest level of the information being handled in that area. Personnel who perform escort duties shall be cleared to the highest level of the information being handled in the area and shall receive special information assurance (IA) training that covers their specific escort practices.

The Enterprise shall identify facility services, such as electrical power, telecommunications, water, and heating, ventilation, and air conditioning (HVAC) and prioritize critical services for backup, as necessary. Secure information shall be stored in locked facilities, and all facilities shall be equipped with HVAC systems that meet heating and cooling requirements in accordance with facility size and structure.

The Enterprise shall have redundant protection mechanisms in place such that if one mechanism fails there is another that will take its place. This could mean that a backup system will activate when the primary fails or that the redundant system is already operational and will pick up the slack caused by the failed system. This includes considerations for maintaining physical security in the absence of utilities (e.g., maintaining access logs during total power failures).



CGS Physical and Environmental Protections Capability



Version 1.1.1

The facility itself and all protection mechanisms in use shall be in compliance with any applicable building codes, zoning ordinances, and security policies established either by the Community or the IA Policies, Procedures, and Standards Capability. The Enterprise shall also comply with any inspection or accreditation procedures that may be applicable.

The Enterprise shall employ the use of Supervisory Control and Data Access (SCADA) systems. These systems are used to monitor critical infrastructure services such as heating, cooling, and water flow. SCADA systems shall be deployed in a closed environment and not enabled for remote access to prevent unauthorized tampering.

All US government facilities or US government-sponsored contractor facilities where classified information may be stored, used, discussed, and/or processed shall be constructed and protected in accordance with applicable Community protection standards. The Enterprise shall implement controls consistent with those standards for building location, perimeter around the building, and additional controls such as TEMPEST, tamper, and other external controls. HVAC, heating and cooling, filters for air intake, humidity, and positive building pressure shall be maintained.

Physical protections between systems and people shall be implemented:

1. Physical access controls—Depending on the location and facility being accessed and the Organization's policy, identification technology shall be implemented, which requires individual identification based on more than a single authentication factor (see Access Management).
2. Door sensors/IR (infrared) sensors—Depending on what the Organization is protecting, the threat environment, and policy, the Organization shall consider placing electronic sensors in critical locations to ensure accountability of facility access.
3. Water versus non-water agents—Depending on what is being protected, the use of non-water agents in server rooms shall be determined/balanced for protecting personnel and equipment when combating fires and other hazards. Unified Facilities Criteria shall be used when making this determination.
4. Tamper—Depending on what is being protected, the use of tamper technology applied at entrances and on equipment shall be considered. Conduits located on the roof and other exposed locations may need to have tamper seals that are inspected weekly. Tamper protections are of no use without an inspection program (employed by the Physical Enterprise Monitoring Capability). For devices used in the field, personnel shall verify tamper protections prior to use.



CGS Physical and Environmental Protections Capability



Version 1.1.1

5. Portable media—The Cognizant Security Authority (CSA) for a SCIF shall determine the storage requirements for classified data within the SCIF. Guidance as to what is acceptable is provided by Community policies. If Top Secret (TS) data is inside a SCIF with the appropriate protection such as guards, tamper technology, gates, and sensors, it may be acceptable to lock TS data in a drawer locked by a key. Buildings and offices shall have the appropriate storage mechanisms such as safes, which Organizations shall ensure can be supported by the building's floors. Government buildings shall be designed to adequately support the protections needed, which may be greater than required for commercial buildings.
6. Leased buildings—If leasing, Organizations shall ensure that the built facility will support the Organization's protection needs. In areas that are less secure, there may be limitations on what can be put into those facilities. Level of internal security shall be raised to meet protection requirements.
7. Physical protections—Priority may dictate a direct link to an appropriate emergency response team (fire may require an external team, while a break-in may warrant an internal team) if an alarm is tripped.
8. Separation—Physical separation of information technology resources may be necessary to protect information of differing security levels (e.g., a classified network would not share any physical connections with an unclassified network).

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 makes a risk decision regarding which protections and where they need to be implemented.
2. The Enterprise is responsible for the protections outside of the Physical and Environmental Protections.
3. Personnel are provided with access credentials that the physical protections will use to make access decisions.
4. The Enterprise monitors Physical and Environmental Protections.
5. The Enterprise provides the requirements for the facility mission.
6. The Enterprise is aware of its physical and environmental assets.
7. The Enterprise is assumed to conduct periodic drills (fire, tornado, etc.) to maintain preparedness.



CGS Physical and Environmental Protections Capability



Version 1.1.1

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 is responsible for enforcing physical access restrictions.
2. The Capability is responsible for providing environmental protections of facilities and equipment.
3. The Capability provides the ability to detect whether physical protections have been tampered with.
4. The Capability provides an alert if an anomaly occurs with a protection mechanism.
5. The Capability provides protections that are commensurate with the threat 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).

Organizations will implement Physical and Environmental Protections to ensure that they are protected from unauthorized physical access and environmental impact. Measures that are employed can vary greatly between different agencies or departments, by geographic location, and even building by building. The determination of which controls need to be in place and the protection measures to be employed will be based on the type and location of the building and/or by the threat environment. All facilities will have HVAC systems that meet heating and cooling requirements in accordance with facility size and structure and fire detection and suppression systems, installed and kept in full operational condition. All facilities will also perform periodic and unannounced emergency procedure drills to test current policies and procedures, and so that when something does go wrong, users will know what to do and where to go.

Organizations will require facilities to have a combination of guards, gates, door locks, checkpoints, and credentials to enforce access restrictions to secure areas, and policies to prevent users from circumventing any of these measures. Upon entry and exit, users will be searched for unauthorized materials such as mobile phones, removable media,



CGS Physical and Environmental Protections Capability



Version 1.1.1

recording devices, and sensitive paperwork, among others. Windows will be reinforced to prevent unauthorized entry or exit.

Organizations will ensure that policies are established and enforced to keep secure networks or systems completely segregated, as necessary, in cases where some networks or systems are isolated from others. Only approved types of removable media will be allowed. The Organization will have specific policies in place detailing the process by which secure information will be transferred onto or off of a secure network or system.

Organizations will require that secure facilities be surrounded by fences or walls and constructed with reinforced walls and doors, and that vehicle barriers are in place to prevent any cars from getting too close. Signs will be posted to alert people of restricted areas. Interior ventilation ducts will use reinforced mesh and motion sensors.

Organizations will ensure that guards are responsible for protecting facility entry and exit points and patrolling the perimeter and passageways. Closed-circuit television systems (CCTV), cameras, and motion detectors may be used to supplement guard patrols and provide visual records of incidents. Records will be kept for a reasonable length of time. Lights will be used to reduce or eliminate dark areas where someone could hide. Alarm systems will be used to alert security personnel to potential intrusions.

Organizations will store sensitive information in a secure manner. In addition to whatever cyber security techniques are used (e.g., encryption, file permissions), all sensitive information will be stored in approved locked storage areas. Depending on the mission and threat environment, the contents of these storage areas may be kept inventoried and information may have to be signed out when it is removed. Sensitive information will be openly handled only in secured areas. Within a SCIF, specific handling and storage procedures will be established by a CSA. When sensitive information has to be destroyed, it will be destroyed in accordance with Organization or Community policy. Chain of custody will be maintained up until the information has been destroyed, as necessary.

Organizations will require that during the design stage of a facility or the planning stage of a security policy, the idea of “failing well” will be incorporated from the beginning. The idea of “failing well” is that if a security measure fails, the system or facility as a whole remains secure and that failure is compartmentalized as much as possible. An example of this is building a system of layered protection; if an intruder breaks through one defense mechanism, he or she still does not have full access to the facility or system. In a facility



CGS Physical and Environmental Protections Capability



Version 1.1.1

with layered protection, an intruder might have to scale a perimeter fence, break through a locked door, bypass a security checkpoint, and then find a way into a secure store room, while avoiding guard patrols and cameras, before getting access to sensitive information. Going a step further, that facility may use a compartmentalized checkpoint system to keep intruders contained in a single area if they do break in. By accepting the fact that no security system is fail proof, the security system can be designed so that when a component does fail, the whole system does not fail completely. This process provides defense in depth.

Organizations will ensure that facilities have redundant connections or backup services for utilities such as telephone, power, and network, as dictated by mission needs. When necessary, each connection of a given type will be from a different service provider and connect at opposite ends of the building. In the event of a total power outage, certain facilities will have backup generators powerful enough to drive all necessary systems in the building or facility. If something trips an alarm, there will be automated notification to ensure that if a life-threatening situation exists, or security information is at risk, there is a real-time response. Notification could be from this Capability or the Physical Enterprise Monitoring Capability.

The prevalence of wireless technologies, including cellular phones and Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi), makes it very easy to transfer information quickly. While this can make networking and communication easy, it also presents an added layer of risk when handling sensitive information. Organizations will ensure that facilities will employ the use of radio frequency jamming technology, such as Faraday cages, as necessary to prevent the unauthorized transfer of sensitive materials via the use of wireless technologies.

Organizations will ensure that all facilities that store, handle, or in any way manage secure information are built to withstand any reasonable form of natural disaster, and that there is proper insulation, ventilation, heating, and cooling capacities to handle temperature extremes. Facilities will be intentionally built in areas less prone to flooding, and all measures will be taken to clear excess rain water, snow, and ice. Facilities that are built in areas prone to earthquakes, hurricanes, or tornados will be reinforced to withstand such events.

The use of underground facilities can be popular for a number of legitimate security reasons such as difficulty of access, and protection against terrorist attacks. However, underground facilities are at a particular risk of collapse from earthquakes, and they have



CGS Physical and Environmental Protections Capability



Version 1.1.1

a potential for flooding. Therefore, Organizations will ensure that where underground facilities are used, measures are taken to reinforce the structure against earthquakes (where geographically applicable). Building such facilities in elevated areas, including inside hills or mountains, reduces the risk of flooding. Underground facilities will all be carefully maintained and have adequate drainage capabilities to prevent flooding.

Organizations will ensure that in addition to regular users being issued physical credentials, all authorized visitors to a facility will be issued a form of temporary physical credential, more commonly known as a visitor badge. This will allow security to monitor them and their movements and let other users know the visitor is allowed to be there.

The Organization will develop secure usage and storage controls for information, devices, and other resources that are used outside of controlled facilities (i.e., in the field). These controls will vary based on the sensitivity of the resources and the threat environment in which they are being used.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping—The Physical and Environmental Protections Capability relies on the Network Mapping Capability to provide information about the location of network components in the Enterprise to provide appropriate protection.
- Understand the Physical Environment—The Physical and Environmental Protections Capability relies on the Understand the Physical Environment Capability for knowledge of physical and environmental factors and their location as a basis for physical and environmental protections.
- Personnel Security—The Physical and Environmental Protections Capability relies on Personnel Security to ensure that individuals are screened prior to being granted access to facilities.



CGS Physical and Environmental Protections Capability



Version 1.1.1

- Access Management—The Physical and Environmental Protections Capability relies on the Access Management Capability to establish policies and processes that define user access rights to the facility, system, and its resources.
- Contingency Planning—The Physical and Environmental Protections Capability relies on the Contingency Planning Capability to establish plans that ensure the continued operation of physical and environmental protection measures in the event of a disruptive incident, attack, or disaster.
- Acquisition—The Physical and Environmental Protections Capability relies on the Acquisition Capability to provide procedures for vetting materials and construction personnel used to build or refurbish facilities.

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 and Environmental Protections 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 and Environmental Protections 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 Physical and Environmental Protections Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Physical and Environmental Protections 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 and Environmental Protections 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.

- Hardware Device Inventory—The Physical and Environmental Protections Capability relies on the Hardware Device Inventory Capability to maintain the



CGS Physical and Environmental Protections Capability



Version 1.1.1

hardware device inventory, which identifies the hardware as well as its components.

- Physical Enterprise Monitoring–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.
- Physical Hunting–The Physical and Environmental Protections Capability relies on the Physical Hunting Capability to identify deficiencies in the physical protection mechanisms.
- Risk Mitigation–The Physical and Environmental Protections Capability relies on the Risk Mitigation Capability to establish the necessary safeguards to ensure the continued security of the Enterprise.
- Operations and Maintenance–The Physical and Environmental Protections relies on information from the Operations and Maintenance Capability to ensure that approved maintenance procedures that use and maintain IA are employed.

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>	
CP-6 ALTERNATE STORAGE SITE	Enhancement/s: (1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.
MP-5 MEDIA TRANSPORT	Control: The organization: a. Protects and controls [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures]; b. Maintains accountability for information system media during a transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personal. Enhancement/s:



CGS Physical and Environmental Protections Capability



Version 1.1.1

	<p>(2) The organization documents activities associated with the transport of information media.</p> <p>(3) The organization employs an identified custodian throughout the transport of information system media.</p>
<p>PE-2 <i>PHYSICAL ACCESS AUTHORIZATIONS</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> 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); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [Assignment: organization-defined frequency], removing from the access list personnel no longer requiring access. <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization authorizes physical access to the facility where the information system resides based on position or role. (2) The organization requires two forms of identification to gain access to the facility where the information system resides. (3) The organization restricts physical access to the facility containing an information system that processes classified information to authorized personnel with appropriate clearances and access authorizations.
<p>PE-3 <i>PHYSICAL ACCESS CONTROL</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and other physical access devices;



CGS Physical and Environmental Protections Capability



Version 1.1.1

	<p>f. Inventories physical access devices [Assignment: organization-defined frequency]; and</p> <p>g. Changes combinations and keys [Assignment: organization-defined frequency] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.</p> <p>Enhancement/s:</p> <p>(1) The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.</p> <p>(2) The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.</p> <p>(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.</p> <p>(4) The organization uses lockable physical casings to protect [Assignment: organization-defined information system components] from unauthorized physical access.</p> <p>(5) The information system detects/prevents physical tampering or alteration of hardware components within the system.</p> <p>(6) The organization employs a penetration testing process that includes [Assignment: organization-defined frequency], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.</p>
<p>PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM</p>	<p>Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.</p> <p>Enhancement/s: None Specified.</p>
<p>PE-5 ACCESS CONTROL FOR OUTPUT DEVICES</p>	<p>Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.</p> <p>Enhancement/s: None specified</p>
<p>PE-6 MONITORING PHYSICAL ACCESS</p>	<p>Control: The organization:</p> <p>a. Monitors physical access to the information system to detect and respond to physical security incidents;</p> <p>b. Reviews physical access logs [Assignment: organization-defined frequency]; and</p> <p>c. Coordinates results of reviews and investigations with the</p>



CGS Physical and Environmental Protections Capability



Version 1.1.1

	<p>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>Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.</p> <p>Enhancement/s:</p> <p>(1) The organization escorts visitors and monitors visitor activity, when required.</p> <p>(2) The organization requires two forms of identification for visitor access to the facility.</p>
PE-8 ACCESS RECORDS	<p>Control: The organization:</p> <p>a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and</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> <p>(2) The organization maintains a record of all physical access, both visitor and authorized individuals.</p>
PE-9 POWER EQUIPMENT AND POWER CABLING	<p>Control: The organization protects power equipment and power cabling for the information system from damage and destruction.</p> <p>Enhancement/s:</p> <p>(1) The organization employs redundant and parallel power cabling paths.</p> <p>(2) The organization employs automatic voltage controls for [Assignment: organization-defined list of critical information system components].</p>
PE-10 EMERGENCY SHUTOFF	<p>Control: The organization:</p> <p>a. Provides the capability of shutting off power to the information system or individual system components in emergency</p>



CGS Physical and Environmental Protections Capability



Version 1.1.1

	<p>situations;</p> <p>b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and</p> <p>c. Protects emergency power shutoff capability from unauthorized activation.</p> <p>Enhancement/s: None Specified</p>
<p>PE-11 <i>EMERGENCY POWER</i></p>	<p>Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.</p> <p>Enhancement/s:</p> <p>(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.</p> <p>(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.</p>
<p>PE-12 <i>EMERGENCY LIGHTING</i></p>	<p>Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.</p> <p>Enhancement/s:</p> <p>(1) The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.</p>
<p>PE-13 <i>FIRE PROTECTION</i></p>	<p>Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.</p> <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> <p>(3) The organization employs an automatic fire suppression capability for the information system when the facility is not</p>



CGS Physical and Environmental Protections Capability



Version 1.1.1

	<p>staffed on a continuous basis.</p> <p>(4) The organization ensures that the facility undergoes [Assignment: organization-defined frequency] fire marshal inspections and promptly resolves identified deficiencies.</p>
<p>PE-14 <i>TEMPERATURE AND HUMIDITY CONTROLS</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [Assignment: organization-defined frequency]. <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system. (2) The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.
<p>PE-15 <i>WATER DAMAGE PROTECTION</i></p>	<p>Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.</p> <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.
<p>PE-16 <i>DELIVERY AND REMOVAL</i></p>	<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>
<p>PE-17 <i>ALTERNATE WORK SITE</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Employs [Assignment: organization-defined management, operational, and technical information system security controls] at alternate work sites; c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. b. Assesses as feasible, the effectiveness of security controls at



CGS Physical and Environmental Protections Capability



Version 1.1.1

	alternate work sites; and Enhancement/s: None Specified.
PE-18 <i>LOCATION OF INFORMATION SYSTEM COMPONENTS</i>	Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. Enhancement/s: (1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.
PE-19 <i>INFORMATION LEAKAGE</i>	Control: The organization protects the information system from information leakage due to electromagnetic signals emanations. Enhancement/s: (1) The organization ensures that information system components, associated data communications, and networks are protected in accordance with: (i) national emissions and TEMPEST policies and procedures; and (ii) the sensitivity of the information being transmitted.

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 and Environmental Protections 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



CGS Physical and Environmental Protections Capability



Version 1.1.1

	<p>discussed. This directive rescinds Director of Central Intelligence Directive (DCID) 6/9, <i>Physical Security Standards for Sensitive Compartmented Information Facilities, including the 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, Intelligence Community Update to Director of Central Intelligence Directive (DCID) 6/9, <i>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>ICPM 2007-500-3, Intelligence Information Sharing, 22 December 2007, Unclassified</p>	<p>Summary: Policy: To maximize the dissemination of intelligence information to IC customers relevant to their missions, while balancing the obligation to protect intelligence sources and methods, the IC elements shall: ... b. Implement Director of National Intelligence (DNI) approved information technology, personnel/physical security standards, and procedures for providing and protecting intelligence information.</p>
<p>Comprehensive National Cybersecurity Initiative (CNCI)</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>Department of Defense (DoD)</p>	
<p>DoD 5105.21-M-1, Sensitive Compartmented Information Administrative</p>	<p>Summary: This manual contains security policy and procedures for the protection, use, and dissemination of SCI. SCI is classified information concerning or derived from</p>



CGS Physical and Environmental Protections Capability



Version 1.1.1

Security Manual, August 1998, Classified	intelligence sources, methods, or analytical processes and required to be handled within formal access control systems.
DoD 5200.08-R, Physical Security Program, 27 May 2009, Unclassified	Summary: This regulation implements the policies and minimum standards for the physical security of Department of Defense (DoD) installations and resources.
DoDI 5200.08, Security of DoD Installations and Resources, 10 December 2005, Unclassified	Summary: This instruction authorizes commanders to issue regulations for the protection or security of property or places under their command, consistent with minimum standards for protecting Department of Defense (DoD) installations and resources.
DoD 5200.1-R, Information Security Program, 14 January 1997, Unclassified	Summary: This document establishes the 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-R, Industrial Security Regulation, 4 December 1985, Unclassified	Summary: This regulation sets forth policies, practices, and procedures of the 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.
DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 28 February 2006, Unclassified	Summary: This manual is a companion document to DoD 5220-R that contains detailed security requirements to be followed by U.S. contractors for safeguarding classified information.
DoD 5220.22-M-Sup-1, National Industrial Security Program Operating Manual (NISPOM) Supplement 1, February 1995, Unclassified	Summary: This supplement provides special security measures to ensure the integrity of Special Access Programs (SAPs), Critical Secret Restricted Data (SRD), and Top Secret Restricted Data (TSRD) and imposes controls supplemental to security measures prescribed in the National Industrial Security Program Operating Manual (NISPOM) for classified contracts.
DoDI 6055.06, DoD Fire	Summary: This document updates policy and criteria for the



CGS Physical and Environmental Protections Capability



Version 1.1.1

and Emergency Services (F&ES) Program, 21 December 2006, Unclassified	allocation, assignment, operation, and administration of the DoD Fire and Emergency Services (F&ES) Program, establishes a DoD Fire and Emergency Services Working Group (F&ESWG), and authorizes other publications such as guides, handbooks, and manuals to provide specific information on the DoD F&ES Program.
UFC 3-600-01, Fire Protection for Facilities Engineering, Design, and Construction, Change 1, 14 July 2009, Unclassified	Summary: This document establishes minimum protection requirements for DoD facilities. These criteria are based on commercial requirements set forth by national insurance underwriters and may exceed minimum national code requirements. The requirements in this Unified Facilities Criteria (UFC) reflect the need for the protection of life, mission, and property (building or contents) while taking into account the costs of implementing the criterion and risks associated with the facility.
UFC 3-600-02, Operations and Maintenance: Inspection, Testing, and Maintenance of Fire Protection Systems, 1 January 2001, Unclassified	Summary: This document provides requirements for inspection, test, and maintenance (ITM) of engineered fire protection features in DoD facilities.
UFC 4-010-01, DoD Minimum Antiterrorism Standards For Buildings, 8 October 2003, Classified	This document establishes physical security standards governing the construction and protection of government facilities.
UFC 4-021-01, Design and O&M: Mass Notification Systems, 9 April 2008, Unclassified	Summary: This document provides technical criteria for systems that will implement mass notification in compliance with the DoD antiterrorism requirements as specified in UFC 4-010-01, implement national design standards and recommendations for mass notification systems as provided in National Fire Protection Association (NFPA) Standard 72 (including Annex E), and achieve coordination of DoD mass notification capabilities with national systems as required by Executive Order 13407.
Committee for National Security Systems (CNSS)	
Nothing found	



CGS Physical and Environmental Protections Capability



Version 1.1.1

Other Federal (OMB, NIST, ...)	
DHS Management Directive 11030.1, Physical Protection of Facilities and Real Property, 21 April 2003, Unclassified	Summary: This directive establishes Department of Homeland Security (DHS) policy regarding the physical protection of facilities and real property.
DHS Management Directive 11035, Industrial Security Program, 2 October 2005, Unclassified	Summary: This document establishes the Industrial Security Program for DHS to ensure that U.S. industry partners performing work for DHS as contractors, subcontractors, consultants, licensees, and grantees, and involving access to classified information, comply with the standards for safeguarding such information pursuant to the National Industrial Security Program (NISP), administered by DoD as executive agent and to which DHS is a signatory.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Executive Order 12977, Interagency Security Committee, 19 October 1995, as amended by Executive Order 13286, 5 March 2003, Unclassified	Summary: This Executive Order established the Interagency Security Committee within the executive branch with responsibilities to establish policies for security in and protection of federal facilities; develop and evaluate security standards for federal facilities, develop a strategy for ensuring compliance with such standards, and oversee the implementation of appropriate security measures in federal facilities; and take such actions as may be necessary to enhance the quality and effectiveness of security and protection of federal facilities, ...
Legislative	
Nothing found	

Physical and Environmental Protections Standards

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



CGS Physical and Environmental Protections Capability



Version 1.1.1

Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, Revision 4, 1 January 2006, Unclassified	Summary: This document provides procedural guidance for the protection, use, management, and dissemination of SCI. The combination of security safeguards and procedures used for information systems shall achieve U.S. government policy that all classified information must be appropriately safeguarded to ensure the confidentiality, integrity, and availability of that information.
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	
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



CGS Physical and Environmental Protections Capability



Version 1.1.1

5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Leased or owned versus new construction—There may be different policies and costs associated with the verification, maintenance, and compliance of protection mechanisms if they are purchased, leased, or outsourced in another fashion.
2. Manpower to implement, maintain, and execute—The size of the facility may dictate the need for a dedicated office to manage this Capability.
3. Time to implement, maintain, and execute—Productive time is lost while personnel are authenticating themselves to a physical protection mechanism. The size of the facility may impact the amount of time being spent for this purpose.

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 and Environmental Protections Capability.

- The Enterprise shall have sufficient physical protection measures in place to prevent unauthorized physical access from any reasonable intrusion attempts.
- All plumbing shall be constructed of resilient materials.
- Computer equipment and other water-sensitive materials shall be positioned away from plumbing, as much as possible, so if there is a leak, the damage is reduced.
- Plumbing located near mission-critical equipment or in mission-critical areas shall feature leak detection capabilities.
- During building design and construction, the Enterprise shall comply with all security acquisition precautions with regard to acquiring materials, plans, and construction personnel.
- The Enterprise shall designate a Facility Security Officer or Physical Security personnel to oversee and ensure compliance with the requirements during construction and operations.



CGS Physical and Environmental Protections Capability



Version 1.1.1

- All personnel shall receive physical security training as applicable to their duties.
- An escort program shall be established to escort personnel, which are not cleared to the highest level of the information being handled in that area, into secure areas.
- Critical facility services, such as electrical power, telephone communications, water, heat, and air conditioning, shall be identified and prioritized for backup services either building-wide or at selected areas within the building.
- Secure information shall be stored in locked facilities.
- All facilities shall be equipped with HVAC systems that meet heating and cooling requirements in accordance with facility size and structure.
- Redundant physical protection mechanisms shall be in place such that if one mechanism fails, there is another that will take its place.
- All facilities shall comply with any applicable building codes, zoning ordinances, security policies, or certification and accreditation (C&A) procedures.
- All US government facilities or US government-sponsored contractor facilities where classified information may be stored, used, discussed, and/or processed shall be constructed and protected in accordance with applicable Community protection standards.
- Physical access controls shall be deployed at all facility locations to prevent unauthorized physical access to resources.
- Non-water fire suppression agents shall be used where necessary to protect water-sensitive resources in the event of a fire.
- Tamper prevention techniques (including an inspection program) shall be used to prevent unauthorized modifications to physical resources.
- The Enterprise shall establish policies and protection mechanisms to protect physical media stored, handled, or removed from secure facilities.
- Incident response mechanisms shall be in place to react to physical intrusions or environmental incidents that may occur.
- Resources shall be physically separated from one another, as necessary, to prevent unauthorized access to or use of resources, such as in the case of a classified system not sharing any physical connections with an unclassified system.