



National Security Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Access Management Capability

Version 1.1.1

Access management enforces the policies that define the actions that an entity may or may not perform against a resource. The Access Management Capability provides criteria that are used to make an access decision and the rules that will be used to assess those criteria.



# CGS Access Management Capability



Version 1.1.1

## Table of Contents

1	Revisions .....	2
2	Capability Definition .....	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions.....	6
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations .....	7
7	Capability Interrelationships.....	10
7.1	Required Interrelationships .....	11
7.2	Core Interrelationships .....	11
7.3	Supporting Interrelationships.....	12
8	Security Controls .....	12
9	Directives, Policies, and Standards .....	18
10	Cost Considerations .....	23
11	Guidance Statements.....	23



# CGS Access Management 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 Access Management 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.

Access management enforces the policies that define the actions that an entity may or may not perform against a resource. The Access Management Capability provides criteria that are used to make an access decision and the rules that will be used to assess those criteria. Specifically, Access Management will validate access through these fundamental steps:

1. Authentication—Validating the identity of an entity within the system.
2. Authorization—Determining the rights of the entity with respect to a resource.
3. Enforcement—Ensuring that an entity can access only the resources for which it is authorized based on authorization and resource access policies.

Access management includes controlling access to physical spaces in addition to access to technology and electronic systems.

## 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 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.

Access is the ability of a user or non-human entity to perform an action on a resource. Users and non-human entities are uniquely identifiable by a system and can include anything that is capable of performing an action on a resource. Resources can include data systems, processes, operations, technology, machinery, environments, or physical locations. Access control encompasses physical and logical access to resources. Logical access is defined as any access that is electronic in nature or occurs only within



# CGS Access Management Capability



Version 1.1.1

the confines of a technology solution. Logical access can mean the abilities to read, write, modify, execute, or otherwise use a digital resource. Physical access can mean abilities including entering a facility, physically handling a resource, or observing something. All resources (logical and physical) are subject to access control restrictions governed by this Capability to prevent their unauthorized use.

The Access Management Capability is able to manage all resources in a robust and centralized manner and interoperate with other Enterprise systems that require access control. An Enterprise does not necessarily have to deploy its own system; instead, it shall use the infrastructure of an external organization provided that it fulfills all requirements of this Capability.

The Access Management Capability handles several components associated with managing access for users and non-human entities. These components include attributes and access policies, authentication, authorization, enforcement, and account management.

## Attributes and Access Policies

The Access Management Capability uses Attribute-Based Access Control (ABAC). Under this system, all resources, users, and non-human entities have attributes assigned to them. The assignment of these attributes is handled by the Attribute Management Capability. All resources have access policies assigned to them. Access policies can vary from being very basic (e.g., all authenticated users have full access) to very restrictive (e.g., access is granted only if three specific users are all present). The assignment of these policies is handled by the Digital Policy Management Capability. These attributes and access policies are used by the Access Management Capability to make access control decisions (see Authorization, below).

## Authentication

When a user or non-human entity requests to perform an action with or against a resource, the Access Management system shall verify the entity's current authentication status, and if required, shall prompt that entity to authenticate. Authentication is the process by which a user or non-human entity proves to the Access Management system that the entity is who it claims to be. The Access Management Capability works with the Identity Management and Credential Management Capabilities to perform the authentication function.



# CGS Access Management Capability



Version 1.1.1

Access Management systems shall use multifactor authentication to authenticate entities. There are three accepted types of factors that can be used to authenticate a user or non-human entity:

1. Something the entity knows (e.g., passphrase, security questions).
2. Something the entity possesses (e.g., Public Key Infrastructure [PKI] certificate, smart card, identification [ID] card).
3. Something the entity is (e.g., biometrics).

For greater security, all users and non-human entities shall be authenticated using at least two of the three factors from the list above each time an entity needs to authenticate (see Credential Management). Each factor shall be difficult to break (e.g., no reusable passwords), strong enough to authenticate an entity by itself, cannot be derived from the same source as another factor, and shall be unique to an individual entity.

## Authorization

After a user or non-human entity is authenticated, the Access Management Capability shall determine whether that entity is authorized to perform the requested action on the requested resource. This is determined by examining the access policy assigned to that resource. The access policy contains rules that specify how to determine authorization by comparing the requesting entity's attributes against the resource's attributes.

## Enforcement

The Access Management Capability does not handle this function directly. Once an access decision has been made, this Capability coordinates with other Capabilities that will enforce those decisions (see System Protection, Data Protection, and Communication Protection). The enforcement component of the Access Management Capability cannot be bypassed.

## Account Maintenance

The Access Management Capability is responsible for revoking access for users or non-human entities. This revocation can be the result of a policy, account expiration, or manual deletion by an authorized system administrator.

The Access Management Capability shall engage in periodic reviews of which users and non-human entities have access to which resources. The frequency of these reviews shall be determined by the Organization or applicable policy. Feedback from these reviews shall be provided to the Attribute Management and Digital Policy



# CGS Access Management Capability



Version 1.1.1

Management Capabilities so they can make the necessary adjustments to revoke entity access that is unnecessary in accordance with applicable Enterprise policies.

Systems that provide access control decisions shall maintain high availability to provide their services when they are needed. High availability shall be defined by the Enterprise according to policy.

An Enterprise implements both internal and external access control mechanisms. Internal access controls are a logical means of separating what defined entities can or cannot do with resources. External access controls are a means of controlling interactions between the system and outside people, systems, and services. The Access Management Capability is invoked whenever an internal or external user or non-human entity requests access to an internal resource.

This Capability shall undergo periodic audits that are established and conducted as part of the Enterprise Audit Management Capability. These audits shall verify that all access control measures in place are effective and fulfill their tasks as efficiently as possible.

## 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. Every resource will have a policy for access.
2. All entities are uniquely identifiable.
3. All entities and resources have attributes.
4. A policy exists that governs how attributes are assigned and used.
5. Entities use credentials to authenticate themselves.
6. An entity's authentication information is passed via a trusted mechanism between systems when implementing a single-sign-on solution (e.g., Kerberos).
7. The environment provides a standard schema for storing attributes as metadata.

## 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 Access Management Capability



Version 1.1.1

1. The Capability uses the access policies provided by the environment.
2. The Capability protects resources from unauthorized access based on the access control policies.
3. The Capability uses standards-based authentication and authorization mechanisms to ensure interoperability across the Enterprise.

## 6 Organizational Implementation Considerations

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

The Organization will develop access policies to govern access to each resource. Resource access policies are stored as digital policies for each resource (see Digital Policy Management). These policies contain rules that are used to make access decisions by comparing the associated attributes of each resource with the entity trying to access it. Access policies are robust enough to cover all use cases that can occur in the system. By definition, if there is no rule for a scenario, that scenario does not matter to the Enterprise.

The Organization will implement access control based on policy made by a management official responsible for a particular resource. The policy will balance the competing interests of security, operational requirements, and user friendliness.

The Organization will deploy a system so that once a user or non-human entity has been authenticated by a system on the network, that authentication will be passed along to other systems using a form of single-sign-on technology (e.g., Kerberos). The goal of this is to reduce the delay that would occur if entities had to reauthenticate with every network resource. Once an entity is authenticated on one system, an authentication token, tied to that entity, is passed along to other systems instead of forcing that entity to reauthenticate. This token will be passed along, stored, and handled securely (see Data Protection, System Protection, Communication Protection) so as to not reduce the level of security created by the multifactor authentication paradigm or any other system. When the entity logs out on one system on the network, that entity will also be logged out of every other system on the network.



# CGS Access Management Capability



Version 1.1.1

The Organization will establish appropriate security controls for managing physical access to data and facilities. Security controls will be put in place to prevent an authorized user from granting access to an unauthorized user (e.g., holding open a locked door to a secure room). Access control will be centrally managed where possible through the use of centrally controlled electronic locks that use secure credentials, such as ID badges, for authentication. Facilities will employ the use of checkpoints to segregate resources, where appropriate.

The Organization may outsource the Access Management systems to another organization or department provided that the outsourced system complies with all of the Gold Standard requirements for this Capability. The Organization will comply with any Community-established policies governing this.

The Organization will design its Access Management systems to use standards established by the Community, where applicable, to ensure interoperability with other Enterprises. Internal Access Management systems will also provide application programming interfaces (APIs) and specification documents, as necessary, to developers to ensure interoperability with other systems and Enterprises.

The Organization will establish a function that revokes user and non-human entity access to resources, when appropriate. This function will maintain a list of dates when accounts are set to expire. Notifications will be sent to the appropriate personnel before that date so access can be extended if necessary. Otherwise, this function will remove user or non-human entity access to resources in coordination with the Attribute Management and Digital Policy Management Capabilities. This function will also remove entity access according to other policies set by the Organization. For example, there will be a policy specifying that users will have their access revoked upon employment termination with the Organization.

Organization-wide access decisions are carefully controlled by access policies assigned to each resource. Some of the access criteria used within these policies will include one or more the following, as appropriate:

- Identity (entity ID). The identity is usually unique to support individual accountability, but it can be a group identification or even anonymous.
- Roles. Access to information will be controlled by the job assignment or function (i.e., the role) of the entity who is seeking access. The process of defining roles will be based on a thorough analysis of how an organization operates and will include input from a wide spectrum of users in an Enterprise.



# CGS Access Management Capability



Version 1.1.1

- **Location.** Access to particular system resources will be based on physical or logical location. Similarly, entities can be restricted based on network addresses. For example, entities operating from within a given network will be permitted greater access than those from outside, such as in the case of an intranet.
- **Time.** Time-of-day and day-of-week/month restrictions are as fine grained as necessary. For example, use of confidential personnel files may be allowed only during normal working hours.
- **Transaction.** Access may be restricted based on the status and duration of a transaction. For example, in an account inquiry, a caller would enter an account number and pin. A service representative would be given read access to that account. When completed, the access authorization would be terminated. This means that entities have no choice in the accounts to which they have access.
- **Service Constraints.** Service constraints refer to those restrictions that depend on the parameters that may arise during use of the application or that are preestablished by the resource owner/manager. For example, a particular software package may be licensed by the Organization for only five users at a time. Access would be denied for a sixth user, even if the user were otherwise authorized to use the application. Another type of service constraint is based on application content or numerical thresholds. For example, an automated teller machine (ATM) may restrict transfers of money between accounts to certain dollar limits or may limit maximum ATM withdrawals to \$500 per day. A third type of constraint is when resources require simultaneous access by multiple users. For example, a weapons system may require authorization codes from two different users in order to activate.
- **Access Modes.** Organizations will consider the types of access, or access modes. The concept of access modes is fundamental to access control. Common access modes, which can be used in both applications and operating systems, can include read, write, execute, and delete. Other specialized access modes (more often found in applications) may include create or search.

When setting up access controls, the Organization will consider the following mechanisms or combinations thereof:

- **Attribute-Based Access Control.** All entities and resources are assigned attributes. When an entity wants to access a resource or another entity, their attributes are compared according to an access policy assigned to the latter entity or resource.
- **Constrained User Interfaces.** Access to specific functions is restricted by never allowing entities to request information, functions, or other resources for which



# CGS Access Management Capability



Version 1.1.1

they do not have access. Three major types exist: menus, database views, and physically constrained user interface (e.g., an ATM).

- **Host-Based Authentication.** Host-based authentication grants access based on the identity of the host originating the request, instead of the identity of the user, service, or application making the request.

The Organization will find it useful to develop a tiered access control model for digital resources similar to the following example:

1. **Public access.** Users and non-human entities are all authenticated as anonymous. There are no restrictions on access, use, or sharing of data objects used for resources such as press releases or other information freely available to the general public (e.g., public websites). Access logs and auditing are optional.
2. **Authenticated access.** Users and non-human entities are required to authenticate after which there is no restriction on use (e.g., Enterprise-wide intranets). Access is enforced at the system level. Access logs and auditing are required.
3. **Attribute-based access.** Users and non-human entities are required to authenticate where authorization uses an access policy that restricts access based on the entity's attributes. Access can be enforced at the system or data object level. Although access is restricted, subsequent use and sharing of data are less restricted. Access logs and auditing are required.
4. **Enhanced data protection.** Users and non-human entities are required to authenticate where authorization uses an access policy that restricts access based on the entity's attributes. Access is enforced at the data object level. Access, use, and sharing are restricted. Access logs and auditing are required.
5. **Persistent data protection.** Users and non-human entities are required to authenticate where authorization uses an access policy that restricts access based on the entity's attributes. The number of users with access is limited. Access is enforced at the data object level. Access, use, and sharing are restricted and enforced by system architecture. Access logs and auditing are required.

## 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.



# CGS Access Management Capability



Version 1.1.1

## 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.

- System Protection—The Access Management Capability relies on the System Protection Capability to enforce access management decisions.
- Communication Protection—The Access Management Capability relies on the Communication Protection Capability to enforce access management decisions.
- Physical and Environmental Protections—The Access Management Capability relies on the Physical and Environmental Protection Capability to enforce access management decisions.
- Identity Management—The Access Management Capability relies on the Identity Management Capability to provide identifiers for entities.
- Digital Policy Management—The Access Management Capability relies on the Digital Policy Management Capability to manage and define resource access policies that are used to make access control decisions.
- Metadata Management—The Access Management Capability relies on the Metadata Management Capability to tag entities and resources with attributes that are used to make access control decisions [Use this character “-” for dashes.]
- Credential Management—The Access Management Capability relies on the Credential Management Capability to manage the credentials used by entities to authenticate.
- Attribute Management—The Access Management Capability relies on the Attribute Management Capability to assign attributes to entities and resources that are used for access control decisions.

## 7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- IA Policies, Procedures, and Standards—The Access Management 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 Access Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.



# CGS Access Management Capability



Version 1.1.1

- IA Training–The Access Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Access Management 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 Mitigation–The Access Management 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>	
AC-2 ACCOUNT MANAGEMENT	Control: The organization manages information system accounts, including: <ul style="list-style-type: none"> <li>a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);</li> <li>c. Identifying authorized users of the information system and specifying access privileges;</li> <li>d. Requiring appropriate approvals for requests to establish accounts;</li> <li>f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;</li> <li>g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;</li> <li>i. Granting access to the system based on: (i) a valid access</li> </ul>



# CGS Access Management Capability



Version 1.1.1

	<p>authorization;            (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions;            and            j. Reviewing accounts [Assignment: organization-defined frequency]Enhancement/s:            (6) The information system dynamically manages user privileges and associated access authorizations.            (7) The organization:            (b) Tracks and monitors privileged role assignments.</p>
<p><b>AC-3 ACCESS ENFORCEMENT</b></p>	<p>Control: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.            Enhancement/s:            (2) The information system enforces dual authorization, based on organizational policies and procedures for [Assignment: organization defined privileged commands].            (3) The information system enforces [Assignment: organization-defined nondiscretionary access control policies] over [Assignment: organization defined set of users and resources] where the policy rule set for each policy specifies:            (a) Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and            (b) Required relationships among the access control information to permit access.            (4) The information system enforces a Discretionary Access Control (DAC) policy that:            (a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both;            (b) Limits propagation of access rights; and            (c) Includes or excludes access to the granularity of a single user.            (5) The information system prevents access to [Assignment: organization defined security-relevant information] except during secure, non-operable system states.</p>
<p><b>AC-4 INFORMATION FLOW</b></p>	<p>Enhancement/s:            (17) The information system:</p>



# CGS Access Management Capability



Version 1.1.1

<i>ENFORCEMENT</i>	(a) Uniquely identifies and authenticates source and destination domains for information transfer
<i>AC-6 LEAST PRIVILEGE</i>	<p>Enhancement/s:</p> <p>(4) The information system provides separate processing domains to enable finer-grained allocation of user privileges.</p> <p>(5) The organization limits authorization to super user accounts on the information system to designated system administration personnel.</p> <p>(6) The organization prohibits privileged access to the information system by non-organizational users.</p>
<i>AC-19 ACCESS CONTROL FOR MOBILE DEVICES</i>	<p>Control: The organization:</p> <p>d. Enforces requirements for the connection of mobile [e.] devices to organizational information systems;</p> <p>f. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;</p> <p>Enhancement/s:</p> <p>(4b) Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information:</p> <p>Connection of unclassified mobile devices to classified information systems is prohibited;</p> <p>Connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s);</p> <p>Use of internal or external modems or wireless interfaces within the mobile devices is prohibited; and</p> <p>Mobile devices and the information stored on those devices are subject to random reviews/inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed.</p>
<i>AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING</i>	<p>Control: The organization:</p> <p>a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and</p>



# CGS Access Management Capability



Version 1.1.1

	<p>b. Employs [Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required] to assist users in making information sharing/collaboration decisions.</p> <p>Enhancement/s:</p> <p>(1) The information system employs automated mechanisms to enable authorized users to make information-sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.</p>
<p>AU-9 PROTECTION OF AUDIT INFORMATION</p>	<p>Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.</p>
<p>IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)</p>	<p>Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).</p> <p>Enhancement/s:</p> <p>(1) The information system uses multifactor authentication for network access to privileged accounts.</p> <p>(2) The information system uses multifactor authentication for network access to non-privileged accounts.</p> <p>(3) The information system uses multifactor authentication for local access to privileged accounts.</p> <p>(4) The information system uses multifactor authentication for local access to non-privileged accounts.</p> <p>(6) The information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.</p> <p>(7) The information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.</p> <p>(8) The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to privileged accounts.</p> <p>(9) The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to non-privileged accounts.</p>



# CGS Access Management Capability



Version 1.1.1

<p>IA-5 <i>AUTHENTICATOR MANAGEMENT</i></p>	<p>Control: The organization manages information system authenticators for users and devices: (8) The organization takes [Assignment: organization-defined measures] to manage the risk of compromise due to individuals having accounts on multiple information systems.</p>
<p>MA-4 <i>NON-LOCAL MAINTENANCE</i></p>	<p>Control: The organization: c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; e. Terminates all sessions and network connections when non-local maintenance is completed. Enhancement/s: None Applicable to this capability</p>
<p>MA-4 <i>NON-LOCAL MAINTENANCE</i></p>	<p>Control: The organization: c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;</p>
<p>MP-2 <i>MEDIA ACCESS</i></p>	<p>Control: The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures]. Enhancement/s: (1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.</p>
<p>MP-2 <i>MEDIA ACCESS</i></p>	<p>Control: The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures]. Enhancement/s: (1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.</p>
<p>PE-3 <i>PHYSICAL ACCESS CONTROL</i></p>	<p>Control: The organization: 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);</p>



# CGS Access Management Capability



Version 1.1.1

	<p>b. Verifies individual access authorizations before granting access to the facility;</p> <p>c. Controls entry to the facility containing the information system using physical access devices and/or guards;</p> <p>d. Controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk;</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><b>PS-6 ACCESS AGREEMENTS</b></p>	<p>Control: The organization:</p> <p>a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and</p> <p>b. Reviews/updates the access agreements [Assignment: organization-defined frequency].</p> <p>Enhancement/s:</p> <p>(1) The organization ensures that access to information with special protection measures is granted only to individuals who:</p> <p>(a) Have a valid access authorization that is demonstrated by assigned official government duties; and</p> <p>(b) Satisfy associated personnel security criteria.</p> <p>(2) The organization ensures that access to classified information with special protection measures is granted only to individuals who:</p> <p>(a) Have a valid access authorization that is demonstrated by assigned official government duties;</p> <p>(b) Satisfy associated personnel security criteria consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and</p> <p>(c) Have read, understand, and signed a nondisclosure agreement.</p>
<p><b>SI-4 INFORMATION SYSTEM MONITORING</b></p>	<p>Enhancement/s:</p> <p>(6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.</p>



# CGS Access Management 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.

### Access Management Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Intelligence Community Public Key Infrastructure (PKI) Overarching Policy for the SCI Fabric, 25 October 1999, Classified	Summary: It is the policy of the Intelligence Community (IC) that a single-root, hierarchical PKI be established for use on sensitive compartmented information (SCI) networks between members of the Community. The IC PKI will provide IC member organizations, for those applications that require them, strong identification and authentication, data integrity, digital signature, non-repudiation, and encryption services for all information system-based communications and services traversing community SCI networks. These services shall be used for communications and services between IC member organizations and those organizations and their customers.
Intelligence Community Certificate Policy, Version 4.3.3, 25 September 2008, Classified	Summary: This policy provides uniform policy guidance and requirements for ensuring interoperability between Certification Authorities (CAs) within the IC PKI. It establishes standard operating policies and procedures to be used by IC agencies/components for services between members of the U.S. IC, IC customers, and others as approved by the Information and Technology Governance Board (ITGB) and the Intelligence Community Chief information Officer (IC CIO). IC PKI public certificates and associated private keys have applicability to areas such as, but not limited to, confidentiality of information, digital signatures, and identification and authentication of individuals, as well as information system infrastructure components.
ODNI/CIO-2009-310, Intelligence Community CIO Council Decisions Regarding IC Unique	Summary: In response to a decision briefing presented to the IC CIO Council on 4 August 2009, the Council committed to leveraging the Distinguished Name (DN) as the standard "system ID" for person and non-person



# CGS Access Management Capability



Version 1.1.1

<p>Identifiers for the Intelligence Community: Intelligence Community Digital Identifier (IC-ID) and Distinguished Name (DN), 26 August 2009, Classified</p>	<p>entities supporting identity and access management within the IC Enterprise.</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:</p> <ul style="list-style-type: none"> <li>b. Implement Director of National Intelligence (DNI) approved information technology (IT), personnel/physical security standards, and procedures for providing and protecting intelligence information.</li> <li>c. Implement a DNI-approved attribute-based identity management capability to enable attribute-based access, user authorization, and user auditing services.</li> </ul>
<p>Intelligence Community Information Assurance Architecture, Version 1.1 (final draft), 30 September 2010, Classified</p>	<p>Summary: This document provides Enterprise-level architectural direction and guidance.</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>DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security</p>	<p>Summary: This directive defines a capability-focused, effects-based approach to advance IT and National Security Systems (NSS) interoperability and supportability across the Department of Defense (DoD). Stated DoD policy includes IT and NSS, of the DoD Global Information</p>



# CGS Access Management Capability



Version 1.1.1

Systems (NSS), 23 April 2007, Unclassified	Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant IA.
DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004, Unclassified	Summary: This instruction implements a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability throughout the DoD. Guidance includes that IT and NSS, of the DoD GIG, shall provide for easy access to information, anytime and anyplace, with attendant IA.
DoDD 8500.01E, Information Assurance (IA), 23 April 2007, Unclassified	Summary: This directive establishes policy to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology and supports the evolution to network-centric warfare. All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability ... Access to all DoD information systems shall be based on a demonstrated need-to-know, and be granted in accordance with applicable laws and DoD regulations.
DoDI 8500.2, Information Assurance (IA) Implementation, 6 February 2003, Unclassified	Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of DoD information systems and networks in accordance with Department of Defense Directive (DoDD) 8500.01E, IA, 23 April 2007.
DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 1 April 2004, Unclassified	Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a department-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption. It aligns DoD PKI and Public Key (PK) enabling activities with DoDD 8500.1, as implemented by DoD Instruction (DODI) 8500.2, and the DoD Common Access Card (CAC) program, as specified by DoDD 8190.3.
DISA Access Control in Support of Information Systems Infrastructure Security Technical	Summary: This guidance details a security framework for use when planning and selecting access control for protecting sensitive and classified information in the DoD, including the process of identification, authentication, and



# CGS Access Management Capability



Version 1.1.1

Implementation Guidance (STIG), version 2.2, 15 December 2008, Unclassified	authorization for access to protected assets.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 1.0, 10 November 2009, Unclassified	Summary: This guidance outlines a common framework for Identity, Credential, and Access Management (ICAM) within the Federal Government and provides supporting implementation guidance for program managers, leadership, and stakeholders planning to execute a segment architecture for ICAM management programs. It includes courses of action, planning considerations, and technical solution information across multiple federal programs spanning the disciplines of ICAM. Authentication is a key capability referenced throughout the Federal Identity, Credential, and Access Management (FICAM) Roadmap. Goal 4 "Enable Trust and Interoperability" includes authorization. Section 3.2.4.5 "Authorization and Access Service Descriptions" describes several services related to authorization.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
PL 108-458, Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), 17 December 2004, Unclassified	Summary: Section 1016 Information Sharing, (b) Information Sharing Environment, (2) Attributes.–(...) <ul style="list-style-type: none"> <li>- (E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security</li> <li>- (I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls</li> </ul>



# CGS Access Management Capability



Version 1.1.1

--	--

## Access Management Standards

Title, Date, Status	Excerpt / Summary
<b>Intelligence Community (IC)</b>	
Intelligence Community Public Key Infrastructure (PKI) Interface Specification (Draft), Version 2.9.4, September 2009, Classified	Summary: This specification describes the interfaces to the IC PKI, defines the interface requirements for creating X.509 Version 3 (V3) certificates and X.509 Version 2 (V2) Certificate Revocation Lists (CRLs), provides a baseline for IC PKI certificate profiles (largely mirroring those of the DoD's PKI certificate profiles), and establishes the content for PKI certificates.
<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
Nothing found	
<b>Department of Defense (DoD)</b>	
Nothing found	
<b>Committee for National Security Systems (CNSS)</b>	
Nothing found	
<b>Other Federal (OMB, NIST, ...)</b>	
Nothing found	
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
Nothing found	
<b>Legislative</b>	
Nothing found	
<b>Other Standards Bodies (ISO, ANSI, IEEE, ...)</b>	
Nothing found	



# CGS Access Management Capability



Version 1.1.1

## 10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

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

1. Inconvenience of delay gaining access to system—Otherwise productive time may be spent waiting for a system to grant access to a user. Alternatively, a user may need to take time to obtain the necessary access for a task.
2. Authentication mechanisms—The mechanisms used for authentication need to reflect Enterprise policies regarding their strength and if they need to be multifactor.

## 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 Access Management Capability.

- The Enterprise shall use access management to provide criteria that will be used to make an access decision and the rules that will be used to assess those criteria. Access management includes controlling access to physical spaces in addition to access to technology and electronic systems.
- All Enterprise resources shall be subject to access control restrictions to prevent unauthorized use.



# CGS Access Management Capability



Version 1.1.1

- The Enterprise shall manage all resources through a robust and centralized access management system.
- The access management system shall use Attribute-Based Access Control (ABAC).
- All resources, users, and non-human entities shall have attributes assigned to them.
- All resources shall have access policies assigned to them.
- The access management system shall use resource attributes and access policies to make access control decisions.
- When a user or non-human entity requests access to a resource, the access management system shall verify that entity's current authentication status, and if required, shall prompt that entity to authenticate.
- Access management systems shall use multifactor authentication to authenticate entities.
- When using multifactor authentication, all users and non-human entities shall be authenticated using at least two of the three factors to authenticate.
- When using multifactor authentication, each factor shall be difficult to break (e.g., no reusable passwords), strong enough to authenticate an entity by itself, shall not be derived from the same source as another factor, and shall be unique to an individual entity.
- Once an entity has been authenticated, the access management system shall determine whether that entity is authorized to perform the requested action with a resource based on the rules specified in the access policy for that resource.
- The access management system shall revoke access for users or non-human entities, as necessary.
- The access management system shall periodically review which users and non-human entities have access to which resources to support revoking entity access.
- Access management systems shall maintain high availability to provide their services when needed.
- Access management systems shall be invoked whenever an internal or external user or non-human entity requests access to an internal resource.
- Access management systems shall undergo periodic audits to verify that all access control measures are effective and operate efficiently.