



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Signature Repository Capability

Version 1.1.1

A Signature Repository Capability provides a group of signatures for use by network security tools such as anti-virus applications, host or network sensors that require signatures (e.g., intrusion detection/prevention systems), and other monitoring and detection applications. For analysis, the Organization uses these signatures to understand the attack patterns and their relationship to specific threats or activities.



CGS Signature Repository Capability

Version 1.1.1



Table of Contents

1	Revisions.....	2
2	Capability Definition	3
3	Capability Gold Standard Guidance	3
4	Environment Pre-Conditions	5
5	Capability Post-Conditions	6
6	Organizational Implementation Considerations	6
7	Capability Interrelationships	7
7.1	Required Interrelationships.....	8
7.2	Core Interrelationships.....	8
7.3	Supporting Interrelationships	9
8	Security Controls	9
9	Directives, Policies, and Standards	10
10	Cost Considerations	12
11	Guidance Statements.....	13



CGS Signature Repository 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 Signature Repository 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.

A Signature Repository Capability provides a group of signatures for use by network security tools such as anti-virus applications, host or network sensors that require signatures (e.g., intrusion detection/prevention systems), and other monitoring and detection applications. For analysis, the Organization uses these signatures to understand the attack patterns and their relationship to specific threats or activities.

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.

A Signature Repository contains signatures, which are deployed on sensors to identify suspicious activity on a network. An Enterprise shall have separate repositories for each of their different networks. Multiple repositories may exist on the same network for purposes such as segregating signatures or load balancing, where appropriate. Signatures shall be sorted and searched by date, priority, purpose, type, product applicability, classification, and mission intent. All signatures associated with a certain mission or intrusion set shall be logically segregated by that mission or intrusion set in the repository. In addition, the security administrator shall determine the priority information that is associated with signatures through their association with the threat and its priority.

Signatures shall be provided from open sources or may be custom built. Open source signatures shall be obtained from trusted sources. Custom-built signatures shall be manually verified by the security administrator and provided to authorized subscribers. The Signature Repository shall be populated by automated means where possible (for signatures obtained from an external source) but shall also have manual procedures established for custom solutions or as a backup mechanism for automated signature downloads. The Signature Repository shall temporarily hold or stage signatures upon



CGS Signature Repository Capability



Version 1.1.1

automated receipt to ensure that the signature has been validated (verification of the integrity of the source) prior to being placed in the repository.

Signatures in the repository shall be protected from unauthorized disclosure and unauthorized modification (as provided by the Access Management, System Protection, Data Protection, and Communication Protection Capabilities). These Capabilities shall also provide protection to the signature or signature sets while in transit.

A signature shall be tested before entering into the repository. Testing signatures shall be performed in a segregated environment that mimics the operational environment with simulated live data, but does not allow a corrupt signature to adversely affect operations. During testing, signature execution shall be monitored to ensure near real-time actions can be taken should there be an issue and that the signature accurately detects the intended behavior. All signatures, whether from a trusted source or from authorized individuals, shall be tested prior to deployment (validated for operational effectiveness and applicability to the environment) to ensure the signature meets the expected functionality and interoperability requirements. The risk of using an untested signature may be accepted by the Enterprise if it is determined that the threat and risk of not implementing the signature immediately is too great.

When a signature or set of signatures is staged and available for review, Signature Repository notifications shall be sent to a set of defined repository administrators and subscribers. During staging, the Signature Repository Capability shall analyze indicators, such as Internet Protocol (IP) addresses, domain, ports, and content, in addition to other differentiators, within the signature to identify and prevent having a duplicate signature. When managing signatures (including duplicate signatures) within a repository, system administrators shall not delete signatures from the repository. If archiving is required, the signature's unique identifier shall not be reused. When signatures are modified, the new signature shall be associated with the original signature. The original signature shall be available for review, and the associated signature shall be the new modifiable version. When shared, the new signature shall retain the traceability back to the original signature.

After the signature is tested, a notification shall be sent to the subscriber that a signature is available. The Signature Repository may act in either a push or pull mode. Mission priorities and subscriber requirements shall dictate which method shall be employed. The Signature Repository shall be configurable to control access to the



CGS Signature Repository Capability



Version 1.1.1

repository by systems or users based on the system type/application or user role (e.g., host-based sensors are provided access to only host-based signatures).

All actions or changes to the Signature Repository shall be audited. For example, when a signature is populated or removed from the repository, audit records shall be provided to Enterprise Audit Management. Auditing shall provide notification of success or failure of the installation of the new signature. The Configuration Management Capability shall track the deployed signature as part of the device's configuration baseline.

Signature Repositories shall be available in accordance with availability requirements, which are dictated by the subscriber of the signature. To ensure availability, the appropriate protections, such as failover and redundant systems, shall be in place, which is provided through Contingency Planning for the Signature Repository. Additional protections, including confidentiality, integrity, authentication, and non-repudiation are afforded to this Capability by the System Protection, Data Protection, Communication Protection and Access Management Capabilities.

Signatures shall be shareable within and between Enterprises. Sharing agreements (e.g., Memorandums of Understanding [MoUs] and others) shall be in place with cooperating agencies, Enterprises, private sector, and commercial entities to ensure legalities, and the connecting Enterprise's current risk/security posture shall be understood prior to sharing of signatures. Within these agreements, there shall be an agreed-upon schema for sharing of signatures to ensure interoperability between Signature Repositories. In addition, signature repositories shall be able to uniquely identify a signature or signature set including identification of the mandatory attributes, which shall be provided in the data schema. When needed, non-attribution protection agreements shall be in place to facilitate the sharing of sensitive information.

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. Consumers of the signatures have been identified and their credentials are verified.
2. The Enterprise provides the mechanisms to detect incidents and identify/provide responses.



CGS Signature Repository Capability



Version 1.1.1

3. The Enterprise infrastructure supports deployment of signatures from the repository to the endpoint.
4. The infrastructure is in place to share signatures across security domains, where applicable.
5. Configuration management is in place to manage the deployed signatures.
6. Access management provides the access controls for the repositories and signatures.

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 defines how signatures are to be added to the repository.
2. The Capability defines how signatures are to be stored and accessed.
3. The Capability keeps the signatures up to date.

6 Organizational Implementation Considerations

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

When a Signature Repository Capability is implemented correctly, the Organization will possess the ability to identify and analyze known attack patterns that directly relate to specified threats and anomalous behavior patterns that indicate unauthorized activity. Signatures for specific threats will be ranked and segmented according to the mission.

An Organization will receive signatures for its repository from trusted open sources (e.g., via cooperating agencies, Organizations, private sector, and commercial entities) or by developing approved customized in-house signatures. An Organization will employ automated methods to populate its Signature Repository with signatures obtained from a trusted source. Each Organization will ensure that the automated tool selected for populating the repository encompasses a procedure to verify signatures before placing them into the repository so that there are no anomalies within the repository (e.g., a pull/push staging method to prevent duplicate signatures,



CGS Signature Repository Capability



Version 1.1.1

cryptographic hash functions to verify signature integrity). The Organization will establish procedures for adding custom signatures to the repository.

Organizations will ensure that coordination with other Capabilities, such as the Access Management, System Protection, Data Protection, and Communication Protection Capabilities, is in place to assist in protecting the signatures in the repository. In addition, an Organization will ensure that notifications of available signatures will be sent by the Signature Repository Capability to the system administrator and subscribers. Notifications will also be sent to the security administrator alerting all actions and/or changes to signatures.

An Organization will manage the repository to ensure traceability to the original signature or signature set, by ensuring that signatures are not deleted from the repository and by providing unique signature identifiers. The Organization will be able to trace to the original signature in the case of signature modifications or enhancements either received from a sharing partner or developed internally.

An Organization will provide a testing environment for signatures before submission to the repository. Where possible, signatures will be tested in the Organization test network to determine the effectiveness, functionality, adverse effects on operations, and reaction in real-time during operations. Testing will occur in a network that mimics the operational network and simulates live data. The Organization will conduct these tests prior to signature deployment. In some cases, the Organization may make the risk decision that testing is not necessary because the signature is of a certain type or is from a certain sharing partner. The Organization will record when signatures are accepted without testing.

An Organization will collect audit information about signatures in the repository. The Organization's Enterprise Audit Management Capability will log activity about signature removal or modifications. The Organization will use the Configuration Management Capability to include the signature or signature set for the device as part of its baseline.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary



CGS Signature Repository Capability



Version 1.1.1

relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

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

- Network Boundary Protection—The Signature Repository Capability relies on the Network Boundary Protection Capability to provide the inspection and protection mechanisms necessary when sharing signatures across domains.
- Access Management—The Signature Repository Capability relies on the Access Management Capability to ensure that only authorized users or processes have access to the Signature Repository.
- Threat Assessment—The Signature Repository Capability relies on the Threat Assessment Capability to provide information to define known attack patterns. This information is used to understand attack patterns and their relationship to specific threats.
- Risk Identification—The Signature Repository Capability relies on information from the Risk Identification Capability to make adjustments to its signatures as the Enterprise risk posture changes over time.
- Risk Analysis—The Signature Repository Capability relies on information from the Risk Analysis Capability to make adjustments to its functions as the Enterprise risk posture changes over time.

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 Signature Repository 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 Signature Repository 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 Signature Repository Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.



CGS Signature Repository Capability



Version 1.1.1

- IA Training–The Signature Repository Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Signature Repository 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.

- System Protection–The Signature Repository Capability relies on the System Protection Capability to ensure the necessary systems protections are in place for the repository.
- Communication Protection–The Signature Repository Capability relies on the protections provided by the Communication Protection Capability to protect the signature while in transit.
- Configuration Management–The Signature Repository Capability relies on the Configuration Management Capability to maintain the deployed signature as part of the device’s baseline.
- Data Protection–The Signature Repository Capability relies on the Data Protection Capability for the protection of signatures while in use, at rest, and in transit.

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>	
SI-3 MALICIOUS CODE PROTECTION	Enhancement/s: (1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms (including signature definitions).



CGS Signature Repository Capability



Version 1.1.1

	<p>(4) The information system updates malicious code protection mechanisms only when directed by a privileged user.</p> <p>(5) The organization does not allow users to introduce removable media into the information system.</p> <p>(6) The organization tests malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.</p>
<p><i>SI-4 INFORMATION SYSTEM MONITORING</i></p>	<p>Enhancement/s:</p> <p>(13) The organization:</p> <p>(a) Analyzes communications traffic/event patterns for the information system;</p> <p>(b) Develops profiles representing common traffic patterns and/or events; and</p> <p>(c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives to [Assignment: organization-defined measure of false positives] and the number of false negatives to [Assignment: organization-defined measure of false negatives].</p>
<p><i>SI-8 SPAM PROTECTION</i></p>	<p>Control: The organization:</p> <p>b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.</p> <p>Enhancement/s:</p> <p>(1) The organization centrally manages spam protection mechanisms.</p> <p>(2) The information system automatically updates spam protection mechanisms (including signature definitions).</p>

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.



CGS Signature Repository Capability



Version 1.1.1

Signature Repository Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 5250.01 Management of Signature Support Within the Department of Defense, 31 January 2008, Unclassified	Summary: This directive sets policy for the Transformation of the Force. It is DoD policy that: 4.1. The Department shall have standardized signatures collection, processing, development, storage, maintenance, and dissemination processes to achieve the highest degree of efficiency and effectiveness within a net-centric enterprise information environment...
DoDD 8320.03, Unique Identification (UID) Standards for a Net-Centric DoD, 23 March 2007, Unclassified	Summary: This directive sets policy: 4.2. UID be used as an enabler of DoD business transformation. Management of business, warfighter, intelligence, and information environment mission area transactions will be achieved by the DoD components' information technology applications through the use of unique identifiers.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	



CGS Signature Repository Capability



Version 1.1.1

Legislative	
Nothing found	

Signature Repository Standards

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



CGS Signature Repository Capability



Version 1.1.1

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. Storage requirements—This Capability provides a repository that will require storage space and must be accessible when necessary.
2. Licensing—There are likely to be subscription fees for commercial signatures. Software may need additional licenses for each device that needs signatures. There may also be a license required to host the signature repository inside the Enterprise.
3. Lifecycle maintenance—This Capability requires effort to maintain the repository, test signatures, and update the database. Custom signatures will need to be created and analyzed.
4. Manpower to implement, maintain, and execute—The Enterprise will need to provide administration for the products that use the signatures.

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 Signature Repository Capability.

- The Enterprise shall provide a group of signatures for use by network security tools such as anti-virus applications, host or network sensors that require signatures (e.g., intrusion detection/prevention systems), and other monitoring and detection applications. For analysis, the Organization shall use these signatures to understand the attack patterns and their relationship to specific threats or activities.



CGS Signature Repository Capability



Version 1.1.1

- Signatures in the repository shall be protected from unauthorized disclosure and unauthorized modification.
- All signatures shall be tested before entering into the repository.
- Testing signatures shall be performed in a segregated environment that mimics the operational environment with simulated live data, but does not allow a corrupt signature to adversely affect operations.
- During testing, signature execution shall be monitored to ensure near real-time actions (as they occur) can be taken if an issue arises.
- All signatures, whether from a trusted source or from authorized individuals, shall be tested prior to deployment (validated for operational effectiveness and applicability to the environment) to ensure the signature meets the expected functionality and interoperability requirements.
- When a signature or set of signatures is staged and available for review, signature repository notifications shall be sent to a set of defined repository administrators and subscribers.
- During staging, the signature repository shall analyze indicators, such as IP addresses, domain, ports, and content, in addition to other differentiators, within the signature to identify and prevent having a duplicate signature.
- When managing signatures (including duplicate signatures) within a repository, system administrators shall not delete signatures from the repository and the signature's unique identifier shall not be reused.
- When signatures are modified, the new signature shall be associated with the original signature. The original signature shall be available for review, and the associated signature shall be the new modifiable version.
- After a signature is tested, a notification shall be sent to the subscriber that a signature is available.
- The signature repository shall act in either a push or pull mode, depending on the mission priorities and subscriber requirements.
- The signature repository shall be configurable to control access to the repository by systems or users based on the system type/application or user role (e.g., host-based sensors are provided access to only host-based signatures).
- Signature repositories shall be available in accordance with availability requirements, which are dictated by the subscriber of the signature.
- Signatures shall be shareable within and between Enterprises. Sharing agreements shall be in place with cooperating agencies, Enterprises, private sector, and commercial entities to ensure legalities, and the connecting



CGS Signature Repository Capability



Version 1.1.1

Enterprise's current risk/security posture shall be understood prior to sharing of signatures.

- When needed, non-attribution protection agreements shall be in place to facilitate the sharing of sensitive information.
- There shall be an agreed-upon schema within sharing agreements for the sharing of signatures to ensure interoperability between signature repositories.
- Signature repositories shall be able to uniquely identify a signature or signature set including identification of the mandatory attributes, which shall be provided in the data schema.