



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Software Inventory Capability

Version 1.1.1

The Software Inventory Capability provides the Enterprise with the methods and schemas necessary to identify and track its software assets. Software may include operating systems, applications, plug-ins, firmware, drivers, and patches.



CGS Software Inventory Capability

Version 1.1.1



Table of Contents

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



CGS Software Inventory 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 Software Inventory 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.

The Software Inventory Capability provides the Enterprise with the methods and schemas necessary to identify and track its software assets. Software may include operating systems, applications, plug-ins, firmware, drivers, and patches.

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 Software Inventory Capability is used to maintain a complete, accurate, and up-to-date asset database of all software in use by an Enterprise. Software items or assets inventoried shall include all applications, plug-ins, operating systems, firmware, drivers, and patches. Data stored about each software item shall include, at a minimum, software name, version number, manufacturer, serial number, install date (see the Configuration Management Capability for baseline installation reference), registered users (only if the software is purchased for individual use), license information (e.g., number of licenses purchased), and/or association with baseline hardware assignment for legacy software justification.

To maintain a Software Inventory, each software asset shall be associated with an identification scheme. The Software Inventory Capability shall contain an identification scheme for a unique naming of software assets. The naming scheme of assets shall not be associated with the agency or mission support needs. An Enterprise shall be responsible for determining the naming scheme of the software assets, which shall indicate the software and version of assets. Multiple copies of assets shall be tracked individually, such as limited licenses, and then a copy number (or other method for identifying different versions of the same software) shall be associated with the naming scheme. This includes the tracking of installation media and virtual machines, such that



CGS Software Inventory Capability



Version 1.1.1

the installation media and virtual machines are uniquely marked (may not be able to uniquely track, but shall follow a standardized naming convention).

The Software Inventory Capability shall have accountability for all software assets. All assets in the Software Inventory shall be held in the asset database. This Capability also shall maintain a software repository where software is stored. Any available production source code shall also be inventoried and stored in a repository. Some software requires licensing for its use; therefore, any relevant licenses or license keys shall be stored in the software repository (maintained and enforced by the Configuration Management Capability) with the relevant software. Integrity information for each piece of software asset shall be maintained with the Software Inventory for use in forensic comparison for this Capability.

The process of populating Software Inventory shall be as automated as possible. Software that is not configured to be discoverable by automated means, such as installation media, shall be accounted for by manual processes. The asset database shall indicate how software assets are included in the inventory (i.e., through a manual or automated process).

The asset database for the Software Inventory shall be scalable and stored and maintained centrally. If the information is not available for a particular asset, the Enterprise shall be responsible for capturing and documenting the available information and providing exceptions on an as-needed basis. The information included in the identification schema shall depend on what information the Configuration Management Capability needs for baseline tracking.

The Software Inventory Capability shall provide a near real-time account (Enterprise will establish requirements to respond for timeliness) of discoverable software in the environment and an up-to-date inventory of portable media. This information is housed in the asset database. The Configuration Management Capability shall monitor the database, and subsequent inventories within, for changes as well as version or other information about the software assets. This information is used by the Configuration Management Capability to determine compliance with the appropriate baseline. The Software Inventory Capability shall maintain an inventory of the software repository, which is maintained by the Configuration Management Capability. Configuration Management shall be responsible for the removal of unauthorized deployed software as well as unauthorized software in the repository. The Configuration Management Capability shall maintain a record of changes for the addition/removal of software.



CGS Software Inventory Capability



Version 1.1.1

Verification of the Software Inventory shall provide verification of what is expected (asset database Software Inventory) versus what exists on the network (near real-time or up-to-date inventories based on scanning or manual checks). In some cases, verification or auditing of the asset database and inventory may be carried out by external sources. Policy shall dictate periodic or recurring inventory activities and inventory reporting requirements.

The Software Inventory shall indicate software association with an accredited system. When a change to a Software Inventory item occurs, automated notification shall be sent to the system owner(s) for the associated accredited system so that updates can occur to the system security plans (SSP) or subsequent security documentation. Changes to the inventory shall be recorded and sent to the Enterprise Audit Management Capability.

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. All software deployed on the network is configured to be discoverable and is assigned a unique identifier.
2. Necessary physical and environmental protection mechanisms are employed within the environment.
3. Approved software is procured and licenses are obtained during the acquisition process.

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 ensures all software is identified whether deployed, within the repository, or on portable media.

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.



CGS Software Inventory Capability



Version 1.1.1

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 Software Inventory is implemented correctly, the Organization will possess a mechanism for accurately tracking all software assets' origin and functionality to comply with supporting the mission needs of the Enterprise.

An Organization will maintain software asset information within the established asset database, while the actual software assets and their accompanying licenses and/or license keys will be stored in the software repository (as part of Configuration Management Capability). Organizations will ensure that coordination with other Capabilities, such as the Configuration Management, Network Mapping, and the Hardware Device Inventory Capabilities, is employed to enable Software Inventory data to assist in overall Software Inventory management for the Enterprise.

An Organization will determine a unique naming scheme for the identification schema of software assets. This includes a nomenclature for installation media, for instance a unique identifier will encompass the number of asset copies (e.g., virtual machines) of a particular software asset.

The Organization will employ industry standard tools and formats to conduct automated inventory collection. In addition, when selecting a tool, consideration will be given to the relationship between the Software Inventory Capability and other Capabilities.

An Organization will provide verification of the available software assets and expected software assets (e.g., versions and upgrades) for intended use on a network. Software assets will be periodically reviewed for accuracy and compliance with relevant management policies. The Organization will have a current list of software that will indicate the existing assets on the network. This list will be confirmed against the actual software assets held in the software repository for verification of assets.

The Organization will ensure that notification by the Software Inventory Capability of reported changes in accreditation of a software asset will be sent to the system owner. This notification will help the Organization make the appropriate decisions and ensure that software changes do not affect the integrity or mission it supports.



CGS Software Inventory Capability



Version 1.1.1

7 Capability Interrelationships

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

7.1 Required Interrelationships

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

- Understand Mission Flows—The Software Inventory Capability relies on the Understand Mission Flows Capability for mission information that is used for asset management purposes.
- Understand Data Flows—The Software Inventory Capability relies on the Understand Data Flows Capability for data flow information that is used for asset management purposes.
- Hardware Device Inventory—The Software Inventory Capability relies on the Hardware Device Inventory Capability for information used to track which hardware and software assets are associated.
- Deployment—The Software Inventory Capability relies on the Deployment Capability to provide information about hardware systems that are deployed.

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



CGS Software Inventory Capability



Version 1.1.1

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

- Data Protection–The Software Inventory Capability relies on the Data Protection Capability to provide protection services to assets stored in the software inventory.
- Network Security Evaluations–The Software Inventory Capability relies on the Network Security Evaluations Capability to supply information that is used to fill any gaps that may exist in the inventory.
- Risk Mitigation–The Software Inventory Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.
- Acquisition–The Software Inventory Capability relies on the Acquisition Capability to provide information about software assets as soon as they are acquired by the Enterprise so that they can be monitored.

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>	
CM-8 INFORMATION SYSTEM COMPONENT INVENTORY	Control: The organization develops, documents, and maintains an inventory of information system components that: <ol style="list-style-type: none"> Accurately reflects the current information system; Is consistent with the authorization boundary of the information system; Is at the level of granularity deemed necessary for tracking



CGS Software Inventory Capability



Version 1.1.1

	<p>and reporting;</p> <p>d. Includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]; and</p> <p>e. Is available for review and audit by designated organizational officials.</p> <p>Enhancement/s:</p> <p>(1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.</p> <p>(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.</p> <p>(4) The organization includes in property accountability information for information system components, a means for identifying by [Selection (one or more): name; position; role] individuals responsible for administering those components.</p> <p>(5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.</p>
<p>SA-6 SOFTWARE USAGE RESTRICTIONS</p>	<p>Control: The organization:</p> <p>b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and</p> <p>c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.</p> <p>Enhancement/s: None Applicable</p>
<p>SA-7 USER-INSTALLED SOFTWARE</p>	<p>Control: The organization enforces explicit rules governing the installation of software by users.</p> <p>Enhancement/s: None Specified</p>



CGS Software Inventory 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.

Software Inventory 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)	
DoDI 8100.3 Department of Defense (DoD) Voice Networks, 16 January 2004, Unclassified	Summary: This directive requires "...DoD Components, an annual inventory of DSN and DRSN telecommunications...a single comprehensive DoD inventory of telecommunications switches...DSN and DRSN and submit this inventory to the ASD(NII)/DoD CIO...accreditation data on software and hardware of all telecommunications...
DoDI 8552.01, Use of Mobile Code Technologies in DoD Information Systems, 23 October 2006, Unclassified	Summary: This instruction addresses hardware and/or software that protects enclave boundaries and requires...includes "Software inventory tools capable of monitoring servers and workstations and detecting the presence of prohibited types of mobile code."
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction requires a current and comprehensive baseline inventory of hardware and software.



CGS Software Inventory Capability



Version 1.1.1

Committee for National Security Systems (CNSS)	
CNSSP-17 Policy on Wireless Communications: Protecting National Security Information, May 2010, Classified	Summary: This policy to help agencies better safeguard National Security Information (NSI) during wireless transmission and delivery, while stored on mobile systems, and while stored on fixed systems that can be accessed by wireless media. It addresses the use of wireless technologies in areas where NSI is discussed or processed.
Other Federal (OMB, NIST, ...)	
NIST SP 800-126, The Technical Specification for the Security Content Automation Protocol, November 2009, Unclassified	Summary: This special publication (SP) provides the definitive technical specification for Version 1.0 of the Security Content Automation Protocol (SCAP), consisting of a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. The Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, software, and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Software Inventory Standards

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



CGS Software Inventory Capability



Version 1.1.1

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:

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



CGS Software Inventory Capability



Version 1.1.1

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

1. Solution used for implementation—The Enterprise will need to provide a variety of tools for use by the Capability including discovery and inventory tools.
2. Storage requirements—This Capability provides a software repository for the Enterprise. Adequate storage space must be provided for this purpose.
3. Network bandwidth availability and consumption—This Capability will need to have bandwidth allocated so that it can disseminate software packages from the repository.

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 [capability name] Capability.

- The Enterprise shall use a software inventory to maintain a complete, accurate, and up-to-date asset database of all software in use by an Enterprise, which includes all applications, plug-ins, operating systems, firmware, drivers, and patches.
- The software inventory shall store the following data, at a minimum, for each software asset: software name, version number, manufacturer, serial number, install date, registered users (for software purchased for individual use), license information (e.g., number of licenses purchased), and/or association with baseline hardware assignment for legacy software justification.
- The Enterprise shall use an identification schema that is not associated with the agency or mission support needs to uniquely name the software assets (including the version of assets).
- The Enterprise shall track multiple copies of software assets including the tracking of installation media and virtual machines, such that they are uniquely marked (may not always be able to uniquely track, but shall follow a standardized naming convention).
- The software inventory shall maintain a software repository to store all software assets, including production source code, relevant licenses, and associated keys.
- The software inventory shall store and maintain integrity information for each software asset for use in forensic comparison.
- Populating the software inventory shall be automated, when possible.



CGS Software Inventory Capability



Version 1.1.1

- The software inventory shall indicate whether software assets are automatically or manually included in the inventory.
- The software inventory shall be centrally managed.
- The software inventory shall be scalable.
- The software inventory shall update its information on discoverable software in near real-time (as changes occur).
- The software inventory shall update its information on portable media in near real-time (as changes occur).
- Contents of the software inventory shall be verified for accuracy (to ensure what is in the inventory coincides with what is on the Enterprise).
- The software inventory shall indicate software association with an accredited system.
- Automated notification shall be sent to the system owner(s) of changes to a software inventory item for updates to the associated accredited system.