



National Security Agency/Central Support Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Network Enterprise Monitoring Capability

Version 1.1.1

The Network Enterprise Monitoring Capability employs active and passive monitoring of the network on an Enterprise level to detect security- or performance-relevant changes or events. This includes continuously monitoring the state of the network and networked devices across the Enterprise to share awareness of event changes. It also includes monitoring health and status, links between devices, and traffic flow.

07/30/2012



# CGS Network Enterprise Monitoring 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 .....	7
7.2	Core Interrelationships .....	8
7.3	Supporting Interrelationships.....	9
8	Security Controls .....	9
9	Directives, Policies, and Standards .....	10
10	Cost Considerations .....	14
11	Guidance Statements.....	14



# CGS Network Enterprise Monitoring 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 Network Enterprise Monitoring 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 Network Enterprise Monitoring Capability employs active and passive monitoring of the network on an Enterprise level to detect security- or performance-relevant changes or events. This includes continuously monitoring the state of the network and networked devices across the Enterprise to share awareness of event changes. It also includes monitoring health and status, links between devices, and traffic flow. Enterprise-level monitoring is used to provide inputs to the overall situational awareness picture.

## 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 Network Enterprise Monitoring Capability addresses the ability to gather status information on the network. The Capability shall continuously gather information with respect to the network and its devices’ health and status, including links between devices and traffic flow. This shall be done on a 24 hours/7 days a week (24x7) real-time or near-real-time basis. If an Enterprise cannot support this function internally, external monitoring assistance shall be implemented. Network Enterprise Monitoring is an important part in providing situational awareness, and therefore monitoring systems need to maintain high availability (as defined by the Enterprise) and integrity of the monitoring function and data collection.

When collecting health and status information, the Network Enterprise Monitoring Capability shall include capturing operational status and statistics. This information may depend on the device type and its interfaces. It is important to ensure that the appropriate events are captured, depending on the device’s capabilities and the mission need for the information. The performance statistics shall be provided from the Utilization and Performance Management Capability. All of this information shall provide situational awareness of the network operating environment. The Network Enterprise Monitoring



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

Capability shall use data from other Capabilities (such as Enterprise Audit Management, Configuration Management, Network Intrusion Detection, and Host Intrusion Detection) to provide the situational awareness picture for the Enterprise.

Network Enterprise Monitoring is also responsible for monitoring traffic flow. To be secure, networks shall be as restrictive as possible with regard to the traffic they carry, to prevent unauthorized data transmissions. To do this effectively, without obstructing the operational functionality, there needs to be a clear and complete understanding of what traffic is permitted. This means determining what services are running, what ports the traffic uses, and what the traffic looks like. In addition, it requires knowing what the expected volume is for each traffic type and reviewing traffic trends and patterns to understand the variance, which is generally predictable. Monitoring for deviation occurs in accordance with the established baseline, and the Network Enterprise Monitoring Capability provides notification when traffic flow is outside of this baseline.

As part of the Network Enterprise Monitoring Capability, there shall be a network operations center to monitor the Enterprise in near real-time. Specific frequency requirements shall be set by Enterprise Information Assurance (IA) Policies, Procedures, and Standards. Staffing for the operations center is dependent on the size of the network. The center shall be adequately staffed to ensure the operations center is capable of providing an effective real-time response to an event based on the criticality of the event.

Alerts generated within this Capability shall be reported in near real-time to the operations center. Information provided in the alert shall contain the originating device, a time stamp, an event description, and the severity of the event (as defined by Understand Mission Flows). Severity information shall be used by Incident Response to determine the best response, such as restore mission functionality.

The Network Enterprise Monitoring Capability shall employ a centralized management service that supports failover and redundancy. The systems shall be capable of reporting in a standardized format for correlation locally or with peer networks (may escalate information to reporting authorities or sister Organizations).

When implemented, the Capability shall present the monitoring information in a user interface that provides easily communicated mechanisms and the ability to drill down into component detail when needed. The Capability shall collect information on every device on the network. The level of detail of location information provided by each network device shall be related to the intended purpose and users of that device. In the case of



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

legacy systems that cannot be monitored, the decision regarding what information to capture and how to report it shall be based on mission needs determined by the Enterprise. For components or network devices that are not discoverable and require manual monitoring, date/time stamps indicating the last time the information was captured are included to ensure information collected about event changes is as accurate as possible.

The reporting format of the Network Enterprise Monitoring Capability shall be in both human- and machine-readable format to facilitate collaboration and automated notification and analysis for various monitoring tools. Network Monitoring shall also be able to use information from other Capabilities (Configuration Management, Utilization and Performance, and Network Mapping) to display information relevant to the network components.

The information gathered from the other Capabilities by the Network Enterprise Monitoring Capability shall be used for trend analysis across the Enterprise. By having insight to network health and status, traffic flows, and the other Capability information, the Network Enterprise Monitoring Capability shall aggregate this information to provide statistical analysis on trending, which shall then provide feedback to the operations of other CGS Capabilities. Enterprise monitoring data may be shared with other Organizations when appropriate in accordance with IA Policies, Procedures, and Standards.

The monitoring activities of this Capability shall be conducted out of band. This is to ensure that Monitoring Capabilities do not interfere with normal network operations and, even more important, do not place the information on the network that is directly related to the Capability and operation of a network.

## 4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. System availability, usability, and performance requirements are known.
2. Performance and utilization baselines are defined.
3. A unified time server is provided.



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

4. The monitoring data will be protected by the environment and at the same level as the data within the environment.
5. The environment provides an accurate network map.
6. The environment tracks the assets that will be monitored.
7. Only authorized system administrators can modify system configurations of the monitoring devices.

## 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 provides manned 24x7 near real-time network monitoring.
2. The Capability identifies events on the network in a proactive manner, where possible.
3. The Capability will not degrade network performance beyond established acceptable amounts.

## 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 Network Monitoring is employed correctly, the Organization will possess a capability to identify information about event changes on a network through automated network monitoring tools in a near-real-time capacity. The Organization will employ high-availability systems to perform monitoring activities or provide near-real-time information to an external Organization for monitoring. The Organization will continuously monitor activities that leverage health and status and traffic flow information to maintain an accurate situational awareness picture. The Organization will also leverage data from other Capabilities such as Network Mapping, Configuration Management, and Understand Data Flow to maintain awareness of changes in network components and configuration baselines. The Organization may use this information if anomalous activity is detected.



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

An Organization will establish a 24-hour network operations center, which is to be appropriately staffed to monitor system status. The Organization will make decisions on the placement of monitoring mechanisms based on mission needs for monitoring and the type of monitoring data required. The data collected will also be maintained based on mission need for that data. The Organization will use its Capabilities (such as Network Intrusion Detection or Host Intrusion Detection) to send near-real-time alerts to the operations center. Notifications will be sent to the appropriate deciding authority for action to be taken, as dictated in Incident Response.

For a proper implementation of the Network Enterprise Monitoring Capability, the Organization will use a suite of tools to collect and analyze all relevant network data. The tools used will generate output that provides a graphical representation and machine-readable data, which can be monitored by both humans and automated machine processes. Data collection will include systems that run critical services and critical devices for interface statistics. The interface statistics of each vendor's component devices will be specific to the vendor's devices. The Organization will use this information to determine what monitoring is available on a particular device and what information needs to be captured. The Organization will use standard protocols to describe the system configurations of devices on the network.

## 7 Capability Interrelationships

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

### 7.1 Required Interrelationships

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

- Network Mapping—The Network Enterprise Monitoring Capability relies on the Network Mapping Capability to provide information about the location of all Enterprise network assets that is used to determine monitoring requirements.
- Network Boundaries and Interfaces—The Network Enterprise Monitoring Capability relies on the Network Boundary and Interfaces Capability to provide information about the boundaries and interfaces of the Enterprise network that is used to determine monitoring requirements.



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

- Utilization and Performance Management–The Network Enterprise Monitoring Capability relies on the Utilization and Performance Management Capability to provide information about normal traffic patterns and network usage.
- Understand Mission Flows–The Network Enterprise Monitoring Capability relies on the Understand Mission Flows Capability to provide information about mission flows within the Enterprise, also contributing to the situational awareness picture.
- Understand Data Flows–The Network Enterprise Monitoring Capability relies on the Understand Data Flows Capability to provide information about data flows within the Enterprise, also contributing to the situational awareness picture.
- Hardware Device Inventory–The Network Enterprise Monitoring Capability relies on the Hardware Device Inventory Capability to provide detailed information about network devices for situational awareness.
- Software Inventory–The Network Enterprise Monitoring Capability relies on the Software Inventory Capability to provide detailed information about software components for situational awareness.
- Configuration Management–The Network Enterprise Monitoring Capability relies on the Configuration Management Capability to maintain awareness of changes in network components and configuration baselines.
- Physical Enterprise Monitoring–The Network Enterprise Monitoring Capability relies on the Physical Enterprise Monitoring Capability to provide information that contributes to the situational awareness picture (e.g., identify if an individual has not entered a facility and is trying to log into network devices located within the facility).

## 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 Network Enterprise Monitoring 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 Network Enterprise Monitoring 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 Network Enterprise Monitoring Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

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

- Network Security Evaluations–The Network Enterprise Monitoring Capability relies on the Network Security Evaluations Capability for feedback used to adjust what data it is collecting.
- Host Intrusion Detection–The Network Enterprise Monitoring Capability relies on the Host Intrusion Detection Capability to provide real-time information about host state, events, and changes of the network and networked devices across the Enterprise for situational awareness.
- Risk Monitoring–The Network Enterprise Monitoring Capability relies on information from the Risk Monitoring Capability to make adjustments to its functions as the Enterprise risk posture changes over time.

## 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-17 REMOTE ACCESS	Control: The organization: c. Monitors for unauthorized remote access to the information system;
CA-3 INFORMATION SYSTEM CONNECTIONS	Control: The organization: c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements. Enhancement/s: None Applicable.



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

<p><i>CA-7 CONTINUOUS MONITORING</i></p>	<p>Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <p>c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and</p> <p>Enhancement/s: None Applicable</p>
<p><i>SI-4 INFORMATION SYSTEM MONITORING</i></p>	<p>Control: The organization:</p> <p>c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;</p> <p>e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.</p> <p>Enhancement/s:</p> <p>(16) The organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness.</p>
<p><i>SI-11 ERROR HANDLING</i></p>	<p>Control: The information system:</p> <p>a. Identifies potentially security-relevant error conditions;</p> <p>b. Generates error messages that provide information necessary for corrective actions without revealing [Assignment: organization-defined sensitive or potentially harmful information] in error logs and administrative messages that could be exploited by adversaries; and</p> <p>c. Reveals error messages only to authorized personnel.</p> <p>Enhancement/s: None Specified.</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.

### Network Enterprise Monitoring Directives and Policies

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



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

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 8410.02, NetOps for the Global Information Grid (GIG), 19 December 2008, Unclassified	Summary: This instruction institutionalizes Network Operations (NetOps) as an integral part of the Global Information Grid (GIG). It is DoD policy that: a. NetOps shall be instituted and conducted to support DoD missions, functions, and operations in a manner that enables authorized users and their mission partners to access and share timely and trusted information on the GIG from any location at any time, to the maximum extent allowed by law and DoD policy .... c. GIG Enterprise Management (GEM), GIG Net Assurance (GNA), and GIG Content Management (GCM) functions shall be operationally and technically integrated to ensure simultaneous and effective monitoring, management, and security of the enterprise...
DoDD 8500.01E, Information Assurance (IA), 23 April 2007, Unclassified	Summary: This directive establishes policy and assigns responsibilities to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology and supports the Unclassified evolution to network-centric warfare. It includes policy that DoD information systems shall be monitored based on the assigned Mission Assurance Category (MAC) and assessed risk to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the IA of DoD operations or information technology (IT) resources, including internal misuse. DoD information systems also shall be subject to active penetrations and other forms of testing used to complement monitoring activities in



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

	accordance with DoD and component policy and restrictions.
DoDD O-8530.1, Computer Network Defense (CND), 8 January 2001, Unclassified	Summary: This directive establishes the Computer Network Defense (CND) policy, definition, and responsibilities necessary to provide the essential structure and support.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction provides joint policy and guidance for IA and CND operations. It includes policy that DoD information systems (e.g., enclaves, applications, outsourced IT-based process, and platform IT interconnections) will be monitored based on the assigned Mission Assurance Category (MAC), confidentiality level (CL), and assessed risk to detect, isolate, and react to incidents, intrusions, disruption of services, or other unauthorized activities (including insider threat) that threaten the security of DoD operations or IT resources, including internal misuse.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
DHS 4300A, Sensitive Systems Policy Directive, version 5.5, 30 September 2007, Unclassified	Summary: This directive provides direction for managing and protecting sensitive Department of Homeland Security (DHS) systems by outlining policies relating to management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and non-repudiation within the DHS IT infrastructure and operations. Includes policy that DHS components shall provide continuous monitoring of their networks for security events and shall report any event that is a security incident to the DHS Security Operations Center.
DHS 4300A, Sensitive Systems Handbook, version 5.5, 30 September 2007, Unclassified	Summary: This document provides specific techniques and procedures for implementing the requirements of the DHS IT Security Program for Sensitive Systems in accordance with security policies published in DHS Sensitive Systems Policy Directive 4300A. It includes policy that DHS components shall provide continuous monitoring of their networks for security events and shall report any event that is a security



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

	incident to the DHS Security Operations Center.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

## Network Enterprise Monitoring 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, ...)	
RFC 2263 – SNMPv3 Applications, Unclassified	This memo describes five types of Simple Network Management Protocol (SNMP) applications, which use an SNMP engine as described in RFC2261. The types of



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

	<p>application described are Command Generators, Command Responders, Notification Originators, Notification Receivers, and Proxy Forwarders. SNMPv3 uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules.</p>

## 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. Scope of work—Complexity of the network and the number of connections will affect the cost of the Capability.
2. Building of an operations center—A centralized operations center is necessary for monitoring the network.
3. Internal versus external capability—Maintaining this Capability versus outsourcing its functions will change the cost structure of the Capability.
4. Solution used for implementation—Building of an out-of-band network may be necessary to safeguard network information. Redundant systems may also be necessary to maintain monitoring functions.



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

## 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 Network Enterprise Monitoring Capability.

- The Enterprise shall employ active and passive monitoring of the network on an Enterprise level to detect security- or performance-relevant changes or events. This includes continuously monitoring the state of the network and networked devices across the Enterprise to share awareness of event changes. It also includes monitoring health and status, links between devices, and traffic flow. Enterprise-level monitoring is used to provide inputs to the overall situational awareness picture.
- The Enterprise shall continuously gather status information with respect to the network and its devices' health and status, including links between devices and traffic flow.
- Network status information shall be gathered on a 24 hours/7 days a week (24x7) real-time or near real-time basis.
- If an Enterprise cannot gather network status information internally, external monitoring assistance shall be implemented.
- Network enterprise monitoring systems shall maintain high availability (as defined by the Enterprise) and integrity of the monitoring function and data collection.
- The Enterprise shall include capturing operational status and statistics when collecting health and status information, including the device type and its interfaces
- The network enterprise monitoring system shall use data from other systems (such as Enterprise Audit Management, Configuration Management, Network Intrusion Detection, and Host Intrusion Detection) to provide the situational awareness view for the Enterprise.
- The Enterprise shall monitor traffic flow, including deviations, in accordance with the established baseline and provide notification when traffic flow is outside of this baseline.
- The Enterprise shall establish a network operations center, which shall be adequately staffed to provide effective real-time response to an event, based on the criticality of the event.
- Specific frequency requirements for network enterprise monitoring shall be set based on Enterprise policy.



# CGS Network Enterprise Monitoring Capability



Version 1.1.1

- Alerts containing the originating device, time stamp, event description, and the severity of the event shall be reported in near real-time to the network operations center.
- The Enterprise shall employ a centralized management service, which is capable of reporting in a standardized format for correlation locally or with peer networks (may escalate information to reporting authorities or sister Organizations).
- The centralized management service shall support failover and redundancy.
- The Enterprise shall present monitoring information in a user interface that provides easily communicated mechanisms and the ability to drill down into component detail when needed. The level of detail of location information provided by each network device shall be related to the intended purpose and users of that device.
- When legacy systems cannot be monitored, the decision regarding what information to capture and how to report it shall be based on mission needs determined by the Enterprise. For components or network devices that are not discoverable and require manual monitoring, date-time stamps indicating the last time the information was captured shall be included to ensure information collected about event changes is as accurate as possible.
- The reporting format shall be in both human- and machine-readable format to facilitate collaboration and automated notification and analysis for various monitoring tools.
- The Enterprise shall be able to use external information received to display information relevant to the network components.
- The Enterprise shall aggregate network health and status, traffic flows, and the other external information to provide statistical analysis on trending across the Enterprise.
- Enterprise monitoring data shall be shared with other Organizations when appropriate in accordance with IA policies, procedures, and standards.
- The monitoring activities shall be conducted out of band to ensure that monitoring does not interfere with normal network operations and does not place the information on the network that is directly related to the monitoring and operation of a network.