



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Network Intrusion Detection Capability

Version 1.1.1

The Network Intrusion Detection Capability helps to detect malicious activity incoming to, outgoing from, and on the network. Network Intrusion Detection Systems are deployed to inspect all network traffic for malicious activity, including anomalies and incidents. The network traffic is examined by passive and in-line computer network defense sensors located within the network.

07/30/2012



CGS Network Intrusion Detection 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	8
7.3	Supporting Interrelationships.....	8
8	Security Controls	9
9	Directives, Policies, and Standards	11
10	Cost Considerations	17
11	Guidance Statements.....	17



CGS Network Intrusion Detection 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 Intrusion Detection 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 Intrusion Detection Capability helps to detect malicious activity incoming to, outgoing from, and on the network. Network Intrusion Detection Systems are deployed to inspect all network traffic for malicious activity, including anomalies and incidents. The network traffic is examined by passive and in-line computer network defense sensors located within the network.

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 Intrusion Detection Capability shall detect security-relevant anomalies, incidents, and malicious activities on the Enterprise networks and generates responses. The Network Intrusion Detection Capability shall analyze network traffic at the packet level while maintaining all network availability requirements. Detected intrusions generate alerts, as described below, which are sent to the applicable security administrators, intrusion analysts or other Capabilities (such as Network Intrusion Prevention, Incident Response, or Incident Analysis).

The Network Intrusion Detection Capability shall obtain signatures from the Signature Repository Capability. Each Network Intrusion Detection device has a specific signature set. In the repository, the signatures within each set are assigned a priority that directly relates to the threat. This set is maintained by the Signature Repository Capability and distributed to the Network Intrusion Detection device. To ensure distribution can occur, the Network Intrusion Detection device shall have a secure connection to the signature repository that is protected by the Communication Protection Capability. Manual distribution of signatures is acceptable when dictated by mission need.



CGS Network Intrusion Detection Capability



Version 1.1.1

When an anomaly, incident, or malicious activity is detected, the notification shall reflect the priority of the threat to the Enterprise and mission. Priority levels shall be determined by the Enterprise. The priority level can be used to determine the recipient of the alert. For example, a high-priority alert such as the identification of an attack in progress may be sent to the Network Intrusion Prevention Capability in addition to the relevant security administrators.

There shall be, at a minimum, one Network Intrusion Detection device configured just inside each network boundary. Larger networks may need additional Network Intrusion Detection devices to be configured within the network to supplement the other(s) based on environment and mission needs.

In addition to traditional signature detection, the Network Intrusion Detection Capability shall be able to identify patterns in the network's activity in near real-time and generate alerts based on anomalies whose deviation from those patterns is statistically significant. Basic event information is not always enough to determine the complete picture of an event or why an alert was generated, so the Enterprise shall capture event packet data, when necessary. Alerts and event information shall be machine generated and readable by humans or machines.

Alerts shall occur near real-time with the detection of the event. A specific response time is established by the IA Policies, Procedures, and Standards Capability. Notification shall be automated. Network Intrusion Detection produces an event alert, which includes the following information:

- Reason for the event
- Signature or anomaly
- Internet Protocol (IP) addresses and ports (source/destination)
- Protocol
- Time stamp synchronized with a centralized authoritative and trusted source (trusted is more important in this case than authoritative time source)
- Capture packet (this could vary based on the incident/signature, and needs to be based on the Enterprise policy)

Notifications of events are sent to the appropriate consumers within the Enterprise, which may include security administrators or other capabilities, such as Network Intrusion Prevention. Regular reports of intrusion detection activity shall be produced and the consumers of these may include the previously mentioned groups in addition to other Organizations, as determined by Enterprise policy.



CGS Network Intrusion Detection Capability



Version 1.1.1

Network Intrusion Detection systems are centrally managed, where possible. Remote management enables policy changes to be applied to all devices simultaneously. Connections between detection systems and the remote management console are secured by the Communication Protection Capability. Both the central management console and all Network Intrusion Detection devices are secured by the System Protection 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. The network can support the added load of a Network Intrusion Detection System.
2. Enterprise monitoring of normal network traffic will be performed.
3. Network Intrusion Detection has access to a signature repository, unless mission need dictates manual updating.
4. The Network Intrusion Detection device will be managed and monitored by dedicated security administrators.

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 detects anomalies and malicious activity.
2. The Capability provides information and alerts of anomalies, intrusions, and malicious activity.
3. The Capability employs mechanisms to keep the Network Intrusion Detection definitions 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



CGS Network Intrusion Detection Capability



Version 1.1.1

Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

The Network Intrusion Detection Capability is implemented in the form of a security device that all network traffic must flow past. Network Intrusion Detection provides the Organization with the ability to effectively detect intrusions on the network. As part of the Capability, Organizations will regularly and methodically inspect network traffic. In addition, Organizations will implement the Network Intrusion Detection Capability to protect extremely critical/sensitive data centers by deploying the Capability at key points within the network. Upon detection of a possible intrusion attempt, Network Intrusion Detection will generate a useful alert, which can be sent via multiple means (email, Short Message Service [SMS], etc.) to the applicable security administrators.

Organizations will determine how many Network Intrusion Detection devices to use, depending on the network size and layout. There will be, at a minimum, one Network Intrusion Detection configured for each access point to an external network. Larger networks may need additional Network Intrusion Detection devices to be configured within the network to supplement the other(s). Placement of the Network Intrusion Detection devices will depend on the Organization deployment goal. Placement outside the enclave would be to detect malicious activity that might affect the boundary device. General deployment is within the network in locations that allow for the capture of the most network traffic (for example, just inside the boundary at the enclave perimeter). This is used to detect events on inbound and outbound traffic. The other location would be within the enclave to detect malicious activity between internal hosts. The exact number and placement of Network Intrusion Detection devices are dependent on the Organization threat and risk posture and network availability needs. In a high-risk environment, Network Intrusion Detection devices are placed at the network boundary. Placement of Network Intrusion Detection could also correspond with the specific mechanisms employed under the Network Boundary Protection Capability.

Organizations will make decisions based on the fact that basic event information is not always enough to figure out what is going on, and therefore the Enterprise uses full capture packet data to complete the picture for the alert, when necessary. Policy will define the Capability to dynamically capture packets when a specific signature hits or turns on other signatures or signature configuration (application) and relationships. This in turn will also dynamically change network threat levels.



CGS Network Intrusion Detection Capability



Version 1.1.1

Network traffic tends to follow patterns over time. Patterns cover all kinds of network activity including the breakdown of different types of traffic, network loads, and user login times. The Capability will be able to identify patterns in the network's activity and generate alerts based on pattern anomalies. For example, when a network that is normally very quiet at 2:00 a.m. has a user log in and start dumping files to an external File Transfer Protocol (FTP) site, that is an anomaly. That might be a legitimate user performing authorized work, but it is different enough from the normal course of network traffic that the Network Intrusion Detection will be able to identify it and generate an appropriate alert.

Each Network Intrusion Detection device is kept up to date with the latest attack signatures. Updates are pulled by the Network Intrusion Detection Capability from a centrally managed signature repository. Manual updating is acceptable for use when dictated by mission need.

Organizations will determine how long stored data is maintained and the type of storage. High-speed storage may be required depending on an enclave's network bandwidth. Organizations will ensure they are using the storage device that best meets the Enterprise needs.

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 Boundary and Interfaces—The Network Intrusion Detection Capability relies on the Network Boundary and Interfaces Capability for information used to understand and define the trust relationship between the connecting networks and enclaves to determine whether an intrusion has taken place.
- Network Boundary Protection—The Network Intrusion Detection Capability relies on the Network Boundary Protection Capability for information used to



CGS Network Intrusion Detection Capability



Version 1.1.1

understand and define the trust relationship between the connecting networks and enclaves to determine whether an intrusion has taken place.

- Vulnerability Assessment—The Network Intrusion Detection Capability relies on the Vulnerability Assessment Capability for information so that network-based intrusion detection techniques remain cognizant of emerging vulnerabilities.
- Threat Assessment—The Network Intrusion Detection Capability relies on the Threat Assessment Capability to provide threat information that feeds into detection patterns.
- Signature Repository—The Network Intrusion Detection Capability relies on the Signature Repository Capability to obtain signatures.

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 Intrusion Detection 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 Intrusion Detection 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 Intrusion Detection Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Network Intrusion Detection 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 Intrusion Detection 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 Network Intrusion Detection Capability relies on the System Protection Capability to secure the central management console and all intrusion detection devices.



CGS Network Intrusion Detection Capability



Version 1.1.1

- Communication Protection—The Network Intrusion Detection Capability relies on the Communication Protection Capability to protect the communications between the Network Intrusion Detection device and the Signature Repository or remote management console.
- Network Security Evaluation—The Network Intrusion Detection Capability relies on the Network Security Evaluation Capability to provide feedback on the effectiveness of network intrusion detection activities.
- Network Enterprise Monitoring—The Network Intrusion Detection Capability relies on the Network Enterprise Monitoring Capability to obtain real-time state of the network and networked devices across the Enterprise to make adjustments to its detection and analysis functions. The Network Enterprise Monitoring Capability monitors the status of network intrusion detection devices.
- Incident Response—The Network Intrusion Detection Capability relies on the Incident Response Capability to make adjustments to focus its detection and analysis functions based on steps being taken in reaction to specific incidents.
- Incident Analysis—The Network Intrusion Detection Capability relies on the Incident Analysis Capability to provide information that feeds into situational awareness.
- Risk Monitoring—The Network Intrusion Detection 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; Enhancement/s: (5) The organization monitors for unauthorized remote connections to the information system [Assignment: organization-defined frequency], and takes appropriate action if



CGS Network Intrusion Detection Capability



Version 1.1.1

	an unauthorized connection is discovered.
IR-4 INCIDENT HANDLING	<p>Control: The organization: Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;</p> <p>Enhancement/s: (1) The organization employs automated mechanisms to support the incident handling process.</p>
SI-4 INFORMATION SYSTEM MONITORING	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks; b. Identifies unauthorized use of the information system; 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; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and <p>Enhancement/s: (1) The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols. (2) The organization employs automated tools to support near real-time analysis of events. (3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.</p>



CGS Network Intrusion Detection Capability



Version 1.1.1

	<p>(5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [Assignment: organization-defined list of compromise indicators].</p> <p>(7) The information system notifies [Assignment: organization-defined list of incident response personnel (identified by name and/or by role)] of suspicious events and takes [Assignment: organization-defined list of least-disruptive actions to terminate suspicious events].</p> <p>(8) The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.</p> <p>(9) The organization tests/exercises intrusion-monitoring tools [Assignment: organization-defined time-period].</p> <p>(11) The organization analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.</p> <p>(12) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts].</p> <p>(13) The organization:</p> <p>(a) Analyzes communications traffic/event patterns for the information system;</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 Intrusion Detection Directives and Policies

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



CGS Network Intrusion Detection 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 8110.1, Multinational Information Sharing Networks Implementation, 6 February 2004, Unclassified	Summary: This instruction implements policy and establishes responsibilities in accordance with (IAW) Department of Defense Directive (DoDD) 8100.1, Global Information Grid (GIG) Overarching Policy, 19 September 2002, for multinational information sharing networks using the GIG. Director, Defense Information Systems Agency (DISA) responsibilities include [5.1.12.6] Provide Enterprise Network Intrusion Detection, ...
DoDI 8420.01, Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies, 3 November 2009, Unclassified	Summary: This instruction establishes policy, assigns responsibilities, and provides procedures for the use of commercial wireless local area network (WLAN) devices, systems, and technologies to achieve and increase joint interoperability, appropriately protect Department of Defense (DoD) information, and enhance overall security to sufficiently protect DoD information by embracing open standards for WLAN devices, systems, and technologies. It provides guidance on establishing a wireless Network Intrusion Detection Capability for monitoring local area networks.
DoDD 8500.01E, Information Assurance (IA), 23 April 2007, Unclassified	Summary: This directive establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a Defense-in-Depth approach that integrates the capabilities of personnel, operations, and technology and supports the 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



CGS Network Intrusion Detection Capability



Version 1.1.1

	<p>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 accordance with DoD and component policy and restrictions.</p>
<p>DoDD O-8530.1, Computer Network Defense (CND),</p>	<p>Summary: This directive establishes the Computer Network Defense (CND) policy, definition, and responsibilities necessary to provide the essential structure and support for CND within the Department of Defense information systems and computer networks.</p>
<p>CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified</p>	<p>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 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. Combatant commands/services/agencies and field activities, in employing boundary protection, remote access, and Internet access will ensure boundary defense mechanisms (including firewalls and Network Intrusion Detection systems) are deployed at the enclave boundary of DoD systems....</p>
<p>DISA Enclave Security Technical Implementation Guide (STIG), version 4.2, 10 March 2008, Unclassified</p>	<p>Summary: This Security Technical Implementation Guide (STIG) provides organizations an overview of the applicable policy and additional STIG documents required to implement secure information systems and networks while ensuring interoperability. Minimum enclave requirements to secure the enclave boundary and the information systems that reside within include External Network Intrusion Detection System, anomaly detection, or prevention device; and Internal Network Intrusion Detection System.</p>



CGS Network Intrusion Detection Capability



Version 1.1.1

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. It includes policy that DHS components shall provide appropriate security for their email systems and email clients by ... deploying appropriate network protection mechanisms, such as firewalls, routers, switches, and Intrusion Detection Systems.
DHS 4300A, Sensitive Systems Handbook, version 5.5, 30 September 2007, Unclassified	Summary: This handbook provides specific techniques and procedures for implementing the requirements of the DHS IT Security Program for Sensitive Systems IAW 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 incident to the DHS Security Operations Center. Information System Security Manager (ISSM) network security monitoring responsibilities include establishing policy and implementing and managing a viable Intrusion Detection program within each component.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	



CGS Network Intrusion Detection Capability



Version 1.1.1

Network Intrusion Detection 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, ...)	
NIST SP 800-36, Guide to Selecting Information Technology Security Products, October 2003, Unclassified	Summary: This special publication describes the characteristics of several categories of IT security products and seeks to help organizations make informed decisions when selecting IT security products. The categories of products listed include operational controls such as Intrusion Detection and technical controls such as firewalls.
NIST SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008, Unclassified	Summary: This special publication provides guidance to organizations in securing their legacy Institute of Electrical and Electronics Engineers (IEEE) 802.11 WLANs that cannot use IEEE 802.11i. A Wireless Intrusion Detection and Prevention System (WIDPS) is an effective tool for determining whether unauthorized users or devices are attempting to access, have already accessed, or have compromised a WLAN.
NIST SP 800-61, Computer Security Incident Handling Guide, March 2008, Unclassified	Summary: This special publication provides practical guidelines on establishing an effective incident response program and responding to incidents effectively and efficiently. Its primary focus is detecting, analyzing, prioritizing, and handling incidents. Continually monitoring threats through Intrusion Detection and Prevention Systems (IDPSs) and other mechanisms is essential. Configuring networks and using Host Intrusion Detection



CGS Network Intrusion Detection Capability



Version 1.1.1

	software to identify activity associated with infections are among the actions to be performed when containing a malicious code incident.
NIST SP 800-83, Guide to Malware Incident Prevention and Handling, November 2005, Unclassified	Summary: This special publication provides recommendations for improving an organization's malware incident prevention measures and gives extensive recommendations for enhancing the existing Incident Response Capability so that it is better prepared to handle malware incidents, particularly widespread ones. Organizations should have a robust Incident Response Process Capability that addresses malware incident handling. During the detection and analysis phase, they should strive to detect and validate malware incidents rapidly by monitoring alerts produced by technical controls (e.g., antivirus software, spyware detection and removal utilities, Intrusion Detection Systems) to identify likely impending malware incidents.
NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007, Unclassified	Summary: This special publication describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them. The types of IDPS technologies are differentiated primarily by the types of events they monitor and the ways in which they are deployed. The guide provides practical, real-world guidance for each of four classes of IDPS products: network-based, wireless, network behavior analysis, and host-based.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Common Vulnerabilities and Exposures (CVE™) MITRE maintains CVE,	Summary: Common Vulnerabilities and Exposures (CVE™) is a dictionary of common names (i.e., CVE Identifiers) for publically known information security



CGS Network Intrusion Detection Capability



Version 1.1.1

<p>manages the compatibility program, maintains the CVE public website, and provides impartial technical guidance to the CVE Editorial Board throughout the process to ensure that CVE serves the public interest. http://cve.mitre.org Unclassified</p>	<p>vulnerabilities and exposures. CVE's common identifiers make it easier to share data across separate network security databases and tools and provide a baseline for evaluating the coverage of an organization's security tools. The report from a security tool that incorporates CVE Identifiers enables information to be quickly and accurately accessed from one or more separate CVE-compatible databases to remediate the problem. CVE use is widespread in many areas including vulnerability management, vulnerability alerting, patch management, and intrusion detection.</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. False positive alerts—This could cause an increase in resources required to analyze the alerts and ensure their accuracy.
2. Time to implement, maintain, and execute—Otherwise productive time can be spent handling false alerts.
3. Storage requirements—Packet captures will need to be stored somewhere.
4. Placement—The locations and number of detection devices that are placed on the network will affect their effectiveness.



CGS Network Intrusion Detection Capability



Version 1.1.1

5. Lifecycle maintenance—Updated signatures need to be incorporated as they are made available.
6. Changing detection patterns—If the number of attacks, events, or patterns change, the existing support/services, including storage, may need to also increase.
7. Manpower to implement, maintain, and execute—Dedicated security personnel may be necessary to manage the detection systems and alerts.

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 Intrusion Detection Capability.

- The Enterprise shall help to detect malicious activity incoming to, outgoing from, and on the network by deploying network intrusion detection systems to inspect all network traffic for malicious activity, including anomalies and incidents. The network traffic shall be examined by passive and in-line computer network defense sensors located within the network.
- The Enterprise shall detect security-relevant anomalies, incidents, and malicious activities on the Enterprise's networks and generate responses.
- The Enterprise shall analyze network traffic at the packet level while maintaining all network availability requirements.
- Each network intrusion detection device shall obtain a signature set from a signature repository through a secure connection.
- Manual distribution of signatures shall occur only when dictated by mission need.
- When an anomaly, incident, or malicious activity is detected, the notification shall reflect the priority of the threat to the Enterprise and mission. Priority levels shall be determined by the Enterprise and can be used to determine the recipient of the alert.
- There shall be, at a minimum, one network intrusion detection device configured just inside each network boundary. For larger networks, the Enterprise shall add additional network intrusion detection devices based on environment and mission needs.
- In addition to traditional signature detection, the Enterprise shall be able to identify patterns in the network's activity in near real-time and generate alerts



CGS Network Intrusion Detection Capability



Version 1.1.1

based on anomalies whose deviation from those patterns is statistically significant.

- The Enterprise shall capture event packet data, when necessary.
- Alerts and event information shall be machine generated and readable by humans or machines.
- Automated alert notifications shall occur in near real-time with the detection of the event and in accordance with Enterprise Policy.
- Event alerts shall include the following information:
 - Reason for the event
 - Signature or anomaly
 - Addresses and ports (source/destination)
 - Protocol
 - Time stamp synchronized with a centralized authoritative and trusted source (trusted is more important in this case than authoritative time source)
 - Capture packet (this could vary based on the incident/signature, and needs to be based on the Enterprise policy).
- Notifications of events shall be sent to the appropriate consumers within the Enterprise, which may include security administrators or other systems.
- Regular reports of intrusion detection activity shall be produced for appropriate consumers within the Enterprise in addition to other Organizations, as determined by Enterprise policy.
- Network intrusion detection systems shall be centrally managed using remote management, where possible, to enable policy changes to be applied to all devices simultaneously.
- Connections between detection systems and the remote management console shall be secure.