



National Security Agency/Central Support Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Host Intrusion Detection Capability

Version 1.1.1

The Host Intrusion Detection Capability helps to detect malicious activity by monitoring for anomalies within the system that indicate malicious activity. The Capability is deployed to monitor the internals of a system(s) for threats.



# CGS Host 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.....	4
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 .....	14
11	Guidance Statements.....	15



# CGS Host 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 Host 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 Host Intrusion Detection Capability helps to detect malicious activity by monitoring for anomalies within the system that indicate malicious activity. The Capability is deployed to monitor the internals of a system(s) for threats.

## 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 host is an end point on the network or a stand-alone machine. In the Host Intrusion Detection Capability, the host-based system monitors anomalies, events, incidents, behavioral patterns, and malicious activities; analyzes anything configurable within the host on a network for anomalous modifications; and triggers alerts when an intrusion is detected on the host.

Each Enterprise shall be able to detect anomalies that occur directly on a host so they can be handled in a timely and effective manner before sensitive information is compromised or that host is used as an attack point to other systems. The Host Intrusion Detection Capability resides on every host, where possible. If the Host Intrusion Detection Capability is not implemented on a specific host, the determination not to implement shall be an explicit decision based on identified and prioritized mission needs in accordance with organizational policy. This Capability monitors for anomalies within the host such as in the basic input/output system (BIOS), file system, system log files, process communication, and kernel activity, as applicable for each system.

Alerts shall occur near real-time with the detection of the event (which is real-time). Alerts of anomalies and events shall be machine generated and are human and machine readable. In addition, the Host Intrusion Detection Capability shall produce reports on all the events it monitors, not just the events that generate alerts. Alerts shall include reason



# CGS Host Intrusion Detection Capability



Version 1.1.1

for the event, the signature that was detected, Internet Protocol (IP) addresses (source and destination), protocol and port (if applicable), timestamp (synchronized with a trusted source), and reference to any external relevant data, such as Enterprise policy. External relevant data may vary based on the incident signature. When the Enterprise implements wireless technologies, Host Intrusion Detection technologies for the wireless devices shall be implemented and integrated into the overall Enterprise Host Intrusion Detection Capability.

The Host Intrusion Detection Capability provides mechanisms access to an updated signature repository. The signature repository provides the Host Intrusion Detection mechanisms with attack signatures to identify intrusion activities (see Capability Interrelationships). The priority of signatures is directly related to the threat they represent, and each Host Intrusion Detection device has a specific signature set. When detected, the event will reflect the priority. The signature set is maintained by the Signature Repository Capability and distributed to the Host Intrusion Detection device.

The Host Intrusion Detection Capability shall be centrally managed. Central management ensures the security administrator can log in from a central location within the enclave (a designated silo within the network). The security administrator shall manage Host Intrusion Detection modules so that they are appropriately protected. In instances where Host Intrusion Detection monitors system properties for change, information about any authorized updates to the system shall be obtained from the Configuration Management Capability. In some cases information about the system updated shall be manually entered in the Host Intrusion Detection system to prevent an attacker from taking advantage of an automated change in the system profile.

The Host Intrusion Detection Capability shall be able to detect configuration modifications in the host's internal system activity and generate alerts based on anomalies whose deviation from those patterns is statistically significant. The Configuration Management baseline determines which configuration changes would indicate an anomaly. Basic event information is not always enough to make a determination, so the Enterprise shall employ regular integrity checks of a device (e.g., file systems, BIOS, hardware).

## 4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are



# CGS Host Intrusion Detection Capability



Version 1.1.1

services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. The host can support the added load of the Host Intrusion Detection Capability.
2. Host Intrusion Detection mechanisms receive updates from a signature repository.
3. The host is in an initial secured and stable state.
4. Host Intrusion Detection mechanisms have access to a database for offloading of reports/records.
5. Detection may require knowledge and analysis of multiple components in the Enterprise.

## 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 monitors the host for anomalies and provide alerts.
2. When reporting or making use of centralized management, the Capability consumes additional bandwidth.
3. The Capability does not interfere with host operations.

## 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 the Host Intrusion Detection Capability is implemented correctly, the Organization will possess a capability to effectively detect activities and intrusions on each host. The Host Intrusion Detection Capability will provide useful alerts via multiple means (email, Short Message Service [SMS], or other methods as defined by the Organization) to appropriate security administrators.

The Organization will employ Host Intrusion Detection signatures that will be kept updated by a centrally managed signature repository (see Signature Repository Capability). The Host Intrusion Detection Capability itself will also be kept updated through a centrally managed system. This central management system and its connections with the host systems will be kept secured (see System Protection and Communication Protection



# CGS Host Intrusion Detection Capability



Version 1.1.1

Capabilities). The security administrator will log into the central location console to manage the Host Intrusion Detection implementations. Through the designated console, the administrator will obtain automated reports provided in a standard form. Reporting alerts for the Host Intrusion Detection Capability will be protected in accordance with policy for the information being reported.

The Organization will implement maintenance and administration for Host Intrusion Detection Capabilities on different hosts on multiple enclaves on a network. The placement of Host Intrusion Detection devices and signatures applied will depend on a number of factors, including how often files change, what activities occur on that host, and the operating system. An effective Host Intrusion Detection Capability will combine multiple types of detection throughout the Enterprise.

The Organization will employ file system detection for Host Intrusion Detection. File system detection is useful and effective when detecting files and directories that change infrequently. Directories that contain system binaries and libraries that are unlikely to change often are good candidates for file system detection. An Organization will regularly check the integrity of these files to make sure that they comply with the internal configuration of a host, because they tend to be targets of attacks upon intrusion. Directories that store temporary files, while difficult to monitor because their contents tend to change so frequently, can be popular locations for attackers to store their working data and so will also be monitored if possible.

The Organization's Host Intrusion Detection Capability will analyze log files to ensure that their size and contents have not unexpectedly changed since the last check by the security administrator. System log files are obvious targets of attackers because they often contain the details of how the attacker gained access to the system. The Organization is aware of which logs tend to be dynamic in size and which are more static.

An Organization's process communication for its Host Intrusion Detection Capability detects unauthorized use of inter-process communications, running services, and unauthorized open ports on the host. Organizations will protect extremely critical/sensitive information data by deploying Host Intrusion Detection within the host. The Organization will ensure Host Intrusion Detection monitors whether a critical system service has been disabled to ensure that attackers' tactics are detected through system logging services.

An Organization will employ a powerful mechanism that hardens a system and detects intruders that are able to gain access, such as a kernel-based detection for Host Intrusion



# CGS Host Intrusion Detection Capability



Version 1.1.1

Detection. However, this Host Intrusion Detection function can also be very difficult to maintain, especially by an Enterprise-wide detection utility.

## 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.

- Configuration Management—The Host Intrusion Detection Capability relies on the Configuration Management Capability to provide information about authorized configuration updates to systems.
- Vulnerability Assessment—The Host Intrusion Detection Capability relies on the Vulnerability Assessment Capability for information so that host-based intrusion detection techniques remain cognizant of emerging vulnerabilities.
- Threat Assessment—The Host Intrusion Detection Capability relies on the Threat Assessment Capability to provide threat information that feeds into detection patterns.
- Signature Repository—The Host 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 Host 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 Host 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 Host Intrusion Detection Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.



# CGS Host Intrusion Detection Capability



Version 1.1.1

- IA Training–The Host 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 Host 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 Host Intrusion Detection Capability relies on the System Protection Capability to secure the host intrusion detection central management console.
- Communication Protection–The Host Intrusion Detection Capability relies on the Communication Protection Capability to secure the connections between the host-based intrusion detection agents and the central management console.
- Network Security Evaluations–The Host Intrusion Detection Capability relies on the Network Security Evaluation Capability to provide feedback on the effectiveness of host intrusion detection activities.
- Incident Response–The Host Intrusion Detection Capability relies on information from the Incident Response Capability to make adjustments to focus its detection and analysis functions based on steps being taken in reaction to specific incidents.
- Risk Monitoring–The Host 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>	
CM-7 LEAST FUNCTIONALITY	Enhancement/s: (1) The organization reviews the information system



# CGS Host Intrusion Detection Capability



Version 1.1.1

	<p>[Assignment: organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services.</p>
<p><b>IR-4 INCIDENT HANDLING</b></p>	<p>Control: The organization:          Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;          Enhancement/s:          (1) The organization employs automated mechanisms to support the incident handling process.</p>
<p><b>SI-4 INFORMATION SYSTEM MONITORING</b></p>	<p>Control: The organization:          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          e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.          Enhancement/s:          (1) The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.          (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</p>



# CGS Host Intrusion Detection Capability



Version 1.1.1

	<p>communications for unusual or unauthorized activities or conditions.</p> <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>(9) The organization tests/exercises intrusion-monitoring tools [Assignment: organization-defined time-period].</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>
--	---

## 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.

### Host Intrusion Detection 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.



# CGS Host Intrusion Detection Capability



Version 1.1.1

Department of Defense (DoD)	
DoDD O-8530.1, Computer Network Defense (CND), 8 January 2001, Classified	Summary: This directive establishes the computer network defense policy, definition, and responsibilities within the Department of Defense (DoD).
AFI 33-115, Network Operations (NETOPS), 24 May 2006, Unclassified	Summary: This instruction provides the overarching policy, direction, and structure for the Air Force-Global Information Grid (AF-GIG). Network Operations (NetOps) provide effective, efficient, secure, and reliable information network services used in critical DoD and Air Force communications and information processes. The extensive list of enumerated operational roles and responsibilities includes the following directive: Equip all servers within the Combat Information Transport System (CITS) Network Battle Management/Network Defense (NBM/ND) boundary with host-based intrusion detection and network security analysis and scanning tools.
DISA Enclave Security Technical Implementation Guide (STIG), version 4.2, 10 March 2008, Unclassified	Summary: This guide provides organizations an overview of the applicable policy and additional Security Technical Implementation Guidance (STIG) documents required to implement secure information systems and networks while ensuring interoperability. Computing environment security mechanisms are implemented on the actual end systems (hosts) including workstations, servers, mainframes, and the applications they host. Computing environment security mechanisms are described, including the employment of host-based intrusion detection systems (IDS) on all servers.
DISA Instant Messaging Security Technical Implementation Guide (STIG), version 1.2, 15 February 2008, Unclassified	Summary: This guide provides DoD-approved security configuration guidelines for secure instant messaging systems. The document will assist sites in meeting the minimum requirements, standards, controls, and options that must be in place for secure instant messaging environments. Mitigating the vulnerabilities in instant messaging operating systems and applications is achieved through building servers and applications with the appropriate STIGs and checklists, and protecting servers and data from unauthorized access. All instant messaging servers and workstations will have up-to-date, properly configured virus



# CGS Host Intrusion Detection Capability



Version 1.1.1

	protection and host-based IDS.
<b>Committee for National Security Systems (CNSS)</b>	
Nothing found	
<b>Other Federal (OMB, NIST, ...)</b>	
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 information technology (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 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 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. [Handbook refers to both host-based IDS and network IDS.]
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
Nothing found	
<b>Legislative</b>	
Nothing found	



# CGS Host Intrusion Detection Capability



Version 1.1.1

## Host Intrusion Detection Standards

Title, Date, Status	Excerpt / Summary
<b>Intelligence Community (IC)</b>	
Nothing found	
<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
Nothing found	
<b>Department of Defense (DoD)</b>	
Nothing found	
<b>Committee for National Security Systems (CNSS)</b>	
Nothing found	
<b>Other Federal (OMB, NIST, ...)</b>	
NIST SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008, Unclassified	<p>Summary: This special publication (SP) provides guidance to organizations in securing their legacy Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless local area networks (WLAN) that cannot use IEEE 802.11i.</p> <p>Organizations should properly secure their legacy IEEE 802.11 client devices to enhance the WLAN's security posture by using personal firewalls, host-based intrusion detection and prevention systems (IDPS), and antivirus software on client devices.</p>
NIST SP 800-61 Rev 1, Computer Security Incident Handling Guide, March 2008, Unclassified	<p>Summary: This SP 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 IDPSs and other mechanisms is essential. Configuring network and host intrusion detection software to identify activity associated with infections is among the actions to be performed when containing a malicious code incident.</p>
NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems	<p>Summary: This SP describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and</p>



# CGS Host Intrusion Detection Capability



Version 1.1.1

(IDPS), February 2007, Unclassified	maintaining them. The types of IDPS technologies are differentiated primarily by the types of events that 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 (CVETM). MITRE maintains CVE, 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. <a href="http://cve.mitre.org">http://cve.mitre.org</a> Unclassified	Summary: Common Vulnerabilities and Exposures (CVE) is a dictionary of common names (i.e., CVE Identifiers) for publically known information security 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's use is widespread in many areas including vulnerability management, vulnerability alerting, patch management, and intrusion detection

## 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)



# CGS Host Intrusion Detection Capability



Version 1.1.1

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. System resources—The solution will consume resources on the individual hosts.
2. Solution used for implementation—The Enterprise will need to consider the number of hosts to monitor, the capabilities of the different solutions, the host platforms, and redundancy requirements.
3. Necessary training—Personnel will require training on topics including the use, configuration, and administration of the solution.
4. Impact/dependency on existing services—Some hosts are more mission critical than others and may not be able to afford sacrificing resources for a host-based detection agent.
5. Network bandwidth availability and consumption—A central management console that monitors the host-based agents will consume network resources. Detected events must be pushed to the notification system.

## 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 Host Intrusion Detection Capability.

- The host intrusion detection system shall monitor anomalies, events, incidents, behavioral patterns, and malicious activities; analyze anything configurable within the host on a network for anomalous modifications; and trigger alerts when an intrusion is detected on the host.
- The host intrusion detection system shall monitor for anomalies, such as in the BIOS, file system, system log files, process communication, and kernel activity, as applicable for each system.



# CGS Host Intrusion Detection Capability



Version 1.1.1

- The host intrusion detection system shall analyze configurable items within the host for anomalous modifications.
- Anomalies occurring on a host shall be detected and reported in a timely manner, as determined by the Enterprise.
- Alerts shall occur in near real-time (as they occur) with the detection of the event.
- Alerts of anomalies and events shall be machine generated and human and machine readable.
- A host-based intrusion detection system shall be installed on every host, where possible.
- Wireless devices shall be implemented and integrated into the overall Enterprise host intrusion detection system.
- The host-based intrusion detection system shall produce reports on all the activity it monitors, not just the events that generate alerts.
- The host-based intrusion detection agents shall obtain definitions updates from a designated signature repository.
- Host intrusion detection agents deployed on systems across the Enterprise shall be centrally managed.
- The host intrusion detection system shall be managed by a security administrator.
- Authorized configuration updates to systems shall be entered into the host intrusion detection management system. Support for manual entry of updates into the host intrusion detection management system will be included, when necessary.
- The host-based intrusion detection system shall be able to detect configuration modifications in the host's internal system activity and generate alerts based on anomalies whose deviation from those patterns is statistically significant.
- The host-based intrusion detection agent shall employ integrity checks of the device/system it is installed on.