National Security Agency/Central Support Service

INFORMATION ASSURANCE DIRECTORATE

CGS Host Intrusion Prevention Capability

Version 1.1.1

The Host Intrusion Prevention Capability employs a response to a perceived incident of interference on a host-based system and encompasses mechanisms that reside on a host to react in real-time to block, drop, redirect, and/or quarantine malicious activities. Host Intrusion Prevention is enabled through a host-based system rather than on a network appliance.

07/30/2012

CGS Host Intrusion Prevention Capability

Version 1.1.1

Table of Contents

1 Revisions 2

2 Capability Definition 3

3 Capability Gold Standard Guidance 3

4 Environment Pre-Conditions 5

5 Capability Post-Conditions 6

6 Organizational Implementation Considerations 6

7 Capability Interrelationships 7

7.1 Required Interrelationships 8

7.2 Core Interrelationships 8

7.3 Supporting Interrelationships 9

8 Security Controls 9

9 Directives, Policies, and Standards 10

10 Cost Considerations 13

11 Guidance Statements 14

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

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 Prevention Capability employs a response to a perceived incident of interference on a host-based system and encompasses mechanisms that reside on a host to react in real-time to block, drop, redirect, and/or quarantine malicious activities. Host Intrusion Prevention is enabled through a host-based system rather than on a network appliance.

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 Intrusion Prevention Capability is a host-based node’s first line of protection against intrusive attacks. Host Intrusion Prevention may encompass mechanisms, such as firewalls, intrusion detection systems (IDS), anti-virus, anti-malware, and application controls. The Host Intrusion Prevention Capability shall apply protections to all host components that are configurable, such as file system properties. Host Intrusion Prevention Systems protect hosts from the network layer to the application layer, against known and unknown malicious attacks.

The Host Intrusion Prevention Capability shall react to attacks or perceived attacks, such as reconnaissance against the target system, as they occur, on any of the Capability’s hosts to prevent them from damaging or compromising the host or its information. This Capability shall maintain operational security. This is accomplished by configuring Host Intrusion Prevention on each host on the network.

A host is any device on the network, such as a user workstation, virtual machine, router, server, smart phone, and other wireless devices. Every host on the network shall contain Host Intrusion Prevention Capabilities that need to be configured differently for multiple types of hosts; this addresses smart phones, which may use a subset of Host Intrusion

Prevention technologies. Host Intrusion Prevention also applies to network devices such as routers, where the Network Intrusion Prevention is responsible for the traffic that flows through the device; however, Host Intrusion Prevention is protecting the platform or device itself.

Host Intrusion Prevention shall have the ability to react, in real-time, to Host Intrusion Detection or other capability alerts or signatures. The Host Intrusion Prevention Capability shall be in listen mode and initiate action based on the source and type of threat. Typical responses may be to block all traffic from the source Internet Protocol (IP) address, block incoming traffic on that port, and redirect any packets, stopping a process or blocking system calls that are deemed to be malicious from writing to protected directories to proactively protect the host or network. In addition to an intrusion response, Host Intrusion Prevention shall send an alert notification (e.g., an action alert to the appropriate system administrators within the Organization).

Host Intrusion Prevention enforces policies and rules that prohibit certain types of behavior or activities on or by the host (e.g., limiting user to three failed log-on attempts). In addition, Host Intrusion Prevention can be configured to respond to any traffic that violates the Host Intrusion Prevention regulations. These rules allow Host Intrusion Prevention to react to real-time malicious attacks.

The Host Intrusion Prevention Capability shall be centrally managed. Central management needs to ensure that the administrator can log in from a central location within the enclave (a designated silo within the network). Policy is configured and pushed from the central management console (policy will be defined within the Digital Policy Management, Incident Response/Analysis or Risk Mitigation Capabilities). Host-based intrusion prevention agents shall not communicate between one another. Communications between the individual host-based agents and the central manager shall occur over secure channels to protect its integrity and confidentiality, and to be authenticated and audited (see Communication Protection Capability).

The Host Intrusion Prevention Capability generates alerts using a standard format such as Common Event Expression (CEE™), which enables the correlation of event prevention alerts. This correlation shall occur in the Enterprise Audit Management Capability. In addition to alerts, Host Intrusion Prevention shall have the ability to send data to higher authoritative reporting officials.

For Host Intrusion Prevention to work efficiently, the Capability shall have mechanisms to prevent unauthorized changes to host resources such as memory, registry, files, processes, or anything configurable on the host to ensure unauthorized changes are not made. The proper placement (based on policy) of Host Intrusion Prevention on every host, where technology is available, can be effective at blocking intrusions, or at least containing threats for stopping intrusions and infections at the individual host level. The Organization shall use the technology that is available to perform the Host Intrusion Prevention functionality, even if that means using only a subset of the Capability rather than the overall technology (e.g., using host-based firewalls and other intrusion prevention technologies).

Host Intrusion Prevention reacts based on alerts provided from Host Intrusion Detection; however, false positives may occur. Host Intrusion Prevention is responsible for reacting to alerts while relying on another Capability to determine whether it was a false positive (see Incident Response/Analysis Capability). All alerts are sent to the central management console.

An Enterprise shall employ only technologies and products that have been approved by the Organization for use on its hosts. An Enterprise shall be able to write and implement rules for use of products and technologies for its Host Intrusion Prevention 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. System availability requirements are clearly known to ensure proper placement of Host Intrusion Prevention and their communications.
2. Access to a database exists for exporting reports.
3. There are reliable communications between the Host Intrusion Prevention and central manager.
4. Detection capabilities exist that provide alerts to react to.
5. Detection capabilities have the ability to automatically send policy updates to Host Intrusion Prevention.
6. Hosts have the necessary resources to support the Host Intrusion Prevention.
7. The central management console can keep track of the Host Intrusion Prevention Capability it is managing and the hosts with which the Capabilities are associated.

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 reacts to alerts as they are provided.
2. The Capability generates useful notifications of its actions.
3. The Capability sends useful alerts to the central management console.
4. The Capability will minimally disrupt host operations under normal operating conditions unless directed to prevent a host action.
5. A single network may implement multiple Host Intrusion Prevention devices.

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 Host Intrusion Prevention is implemented correctly, the Organization will have a Capability to respond to intrusions on each host in a timely, reliable, and secure manner, as they occur, with little or no human interaction. Each host will have its own Host Intrusion Prevention Capability installed and centrally managed. Long-term sustainability will require human interaction for system maintenance and to verify that responses correspond with actual threats and not false positives.

The Organization will employ only technologies and products that have been approved by the Organization for use on its hosts. This will be done in accordance with the Organization's risk analysis process.

The Host Intrusion Prevention Capability can be a target for attackers looking to perform a series of attacks, such as a denial-of-service to a host. Because Host Intrusion Prevention is designed to perform a prevention action, such as block ports, protocols, and IP addresses, attackers can use these actions to their advantage by causing misconfigurations in the systems that implement the Host Intrusion Prevention Capability. Therefore, the Organization will maintain secure communications, including integrity controls, and ensure the proper authentication occurs between the host-based Capability and the central manager that provides configurations and controls access to the Host

Intrusion Prevention Capability mechanisms (e.g., use of one-time passwords for managers and administrators). This will ensure that the Host Intrusion Detection Capability knows when a configuration change is authorized and therefore will not trigger the Host Intrusion Prevention Capability.

Attacks are continually evolving, with new exploit techniques and malicious code being developed. To stay abreast of the latest threats and how to address them, the Host Intrusion Prevention Capability has its attack signatures kept current using a centrally managed signature repository (see Signature Repository Capability). The Organization will provide centralized management to obtain information from the Signature Repository, which will provide definitions, patterns, and behaviors of malicious activity for Host Intrusion Prevention. These signatures will be used by Host Intrusion Prevention to determine which response actions are to be executed. The end result will be pushed out by digital policy (See Digital Policy Management Capability) to the host-based system.

The Organization will employ a Host Intrusion Prevention solution that provides centralized management. Centralized management will facilitate Enterprise-wide configuration changes to the Host Intrusion Prevention Capability on all hosts from one location. The Organization may need to perform the initial baseline manually (per host) to ensure that the configuration does not inhibit the operations of the host. Other than this instance, central management is structured such that manual configuration will not occur, and the Digital Policy Management Capability will provide the necessary information to the Configuration Management Capability for distribution to the hosts.

The Enterprise will benefit from a trial and error test for indications of how its Host Intrusion Prevention Capability will operate on its network. The Organization will determine the services of Host Intrusion Prevention mechanisms for host functionality by using a test environment. The test environment itself may choose not employ Host Intrusion Prevention devices for mission reasons. If so, risk decisions will be made by the test environment's Designated Approval Authority (DAA). Once the Host Intrusion Prevention has been tested, the Organization will deploy the approved Host Intrusion Prevention configuration for use on the host.

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 Host Intrusion Prevention Capability relies on the Network Mapping Capability to provide visualization of the network to determine placement of intrusion prevention devices.
- Configuration Management-The Host Intrusion Prevention Capability relies on the Configuration Management Capability to manage the hardware, software, and firmware on host-based systems and the intrusion prevention agents that operate on them.
- Access Management-The Host Intrusion Prevention Capability relies on the Access Management Capability to enforce policies for authorized logical and physical access to the intrusion prevention management console and modules.
- Digital Policy Management-The Host Intrusion Prevention Capability relies on the Digital Policy Management Capability to provide machine-readable policies that determine the appropriate course of action for the intrusion prevention modules.
- Signature Repository-The Host Intrusion Prevention Capability relies on the Signature Repository Capability to obtain signatures that define known attack patterns to take preventative actions.
- Host Intrusion Detection-The Host Intrusion Prevention Capability relies on the Host Intrusion Detection Capability to discover malicious activity within a host-based system, which the intrusion prevention modules can respond to.
- Incident Response-The Host Intrusion Prevention Capability relies on the Incident Response Capability to define the procedures to report an intrusive risk on a host-based system, which the intrusion prevention modules will respond to appropriately.
- Contingency Planning-The Host Intrusion Prevention Capability relies on the Contingency Planning Capability to provide mission disruption and recovery information to inform decision-making processes and the formulation of possible courses of action.

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 Prevention 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 Prevention 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 Prevention Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training-The Host Intrusion Prevention 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 Prevention 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.

- Communication Protection-The Host Intrusion Prevention Capability relies on the Communication Protection Capability to enable the secure transmission of responses, logs, and communications for intrusion prevention modules.
- Threat Assessment-The Host Intrusion Prevention Capability relies on the Threat Assessment Capability to provide insight on current and evolving system threats that will impact a host-based system.

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, *Recommended Security Controls for Federal Information Systems and Organizations*	
CM-7 *LEAST*	Control: The organization configures the information system to

FUNCTIONALITY	provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services]. Supplemental Guidance: Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Enhancement/s: (2) The organization employs automated mechanisms to prevent program execution in accordance with [Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage.
SC-7 *BOUNDARY PROTECTION*	Enhancement/s: (12) The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.

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 Prevention 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	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

January 2008, Classified	networks.
Department of Defense (DoD)	
DoDI 8410.02 NetOps for the Global Information Grid (GIG), 19 December 2008, Unclassified	It is DoD policy that: c. GIG Enterprise Management (GEM), GIG Net, and GIG Content Management (GCM) functions shall be operationally and technically integrated to ensure simultaneous and effective monitoring, management, and security of the Enterprise. d. As information systems capabilities mature, they shall be capable of reporting their system status to include fault, configuration, performance, and security to facilitate GIG health and mission readiness assessments. In the section for Responsibilities of Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/Department of Defense Chief Information Officer (DoD CIO): e. Develop NetOps capability increments in collaboration with functional owners and Capability Portfolio Managers to ensure efficient and secure GIG operations.
DISA Anti-Spyware Security Technical Implementation Guide (STIG), version 4.1, 3 December 2009, Unclassified	Summary: This guide provides the technical security policies, requirements, and implementation details for applying desktop anti-spyware security concepts to commercial off-the-shelf (COTS) applications.
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	

Host Intrusion Prevention 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 (SP) describes the characteristics of several categories of information technology (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 prevention for both hosts and networks.
NIST SP 800-61, Rev 1, Computer Security Incident Handling Guide, March 2008, Unclassified	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 Intrusion Detection and Prevention Systems (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.
NIST SP 800-83, Guide to Malware Incident	Summary: This SP provides recommendations for improving an Organization's malware incident prevention measures

Prevention and Handling, November 2005, Unclassified	and gives extensive recommendations for enhancing 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. As part of their threat mitigation effort, Organizations should perform threat mitigation to detect and stop malware before it can affect its targets. Intrusion prevention systems are one tool to assist in this effort.
NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007, Unclassified	Summary: This SP 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 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, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)

4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

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

1. Availability requirements–There is the possibility that the prevention system could lock out authorized systems or data unintentionally. This could violate system availability requirements and mission objectives, and require additional time and manpower to fix.
2. Host resources–The host-based intrusion prevention agent will consume individual system resources that may need to be reallocated from another function.
3. Solution used for implementation–The solution needs to be able to scale as necessary to reflect the number of hosts on the network and must have a function that enables centralized management.
4. Necessary training–Personnel need to be trained in the proper use, administration, and management of the intrusion prevention solution.

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 Prevention Capability.

- Host-based intrusion prevention agents shall apply protections to the host that prevent unauthorized changes to host resources, including memory, registry, files, processes, and components that are configurable.
- Host-based intrusion prevention agents shall react to attacks and perceived attacks as they occur.
- Host-based intrusion prevention agents shall be installed and configured on every host in the Enterprise.

- Host-based intrusion prevention agents shall produce alerts in a standard format that will be sent to appropriate security administrators when an intrusion is prevented.
- Host-based intrusion prevention agents shall enforce policies and rules that prohibit certain types of behavior or activities on or by the host (e.g., limiting the user to three failed log-on attempts). These policies and rules shall be configured to respond to any traffic that violates the host intrusion prevention regulations.
- The host intrusion prevention system shall be centrally managed.
- Host-based intrusion prevention agents shall not communicate between one another. Communications between the individual host-based agents and the central manager shall occur over secure channels to maintain their integrity and confidentiality, and to be authenticated and audited.