



National Security Agency/Central Support Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Network Hunting Capability

Version 1.1.1

The Network Hunting Capability is employed to proactively look for indicators of an active threat or exploitation of a vulnerability that was previously known or unknown. Network Hunting may involve signature detection and detection of changes in behaviors and normal usage, as well as the ability to detect incidents that are not known to be occurring.



# CGS Network Hunting 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 .....	10
10	Cost Considerations .....	13
11	Guidance Statements.....	13



# CGS Network Hunting 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 Hunting 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 Hunting Capability is employed to proactively look for indicators of an active threat or exploitation of a vulnerability that was previously known or unknown. Network Hunting may involve signature detection and detection of changes in behaviors and normal usage, as well as the ability to detect incidents that are not known to be occurring.

## 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.

Each department or agency shall have a Network Hunting Program, sufficient staff, and a plan to administer, report, and follow up on threat, vulnerability, and hunting evaluations. The Network Hunting Capability addresses the ability to detect known or unknown anomalies associated with the network components and the Enterprise in which the network resides. Network Hunting looks for indicators to identify both known and unknown threats and activities that could indicate an intrusion, or evidence of attack against the network, and take or initiate action to respond to this attack.

The Network Hunting Capability shall take a proactive approach, using known vulnerability or threat indicators. These indicators shall feed into Network Hunting activities so that vulnerabilities or threats that were previously unidentified on the network may be detected. Network hunters shall understand how to exploit vulnerabilities and use that knowledge to conduct searches to determine any indication of malicious activity. The Network Hunting Capability shall use all authoritative data sources to research indicators, such as the National Cyber Investigative Joint Task Force (NCIJTF), or United States Computer Emergency Readiness Team (US-CERT). These sources shall be further analyzed based on priority, time, resources, threat capability and intent, and risk to help Network Hunting Teams focus their hunting activities. A formal process shall be established for determining new indicators (feedback mechanism for new indicators



# CGS Network Hunting Capability



Version 1.1.1

based on current indicators) to feed back into the threat database. Network hunting activities shall use underlying network details to determine which indicators might apply, such as operating system software and hardware, and shall use the appropriate Capabilities to obtain that information.

Network hunting services may be employed as an internal dedicated team or may be provided by external service providers such as the Computer Network Defense Service Provider (CNDSP). When Network Hunting Teams are internal, they shall be in a separate department from the network and system administrators to prevent conflict of interest. When an external team is used, it shall comply with the appropriate agreements that are in place (e.g., Nondisclosure Agreements [NDAs], Memorandums of Understanding [MOUs], and Scope Definition Documents).

Network Hunting Teams shall comply with any Community-established certification standards to ensure the team has the appropriate level of technology knowledge and understanding of the hunting methodology. The teams shall comprise individuals who have demonstrated practical experience with information assurance (IA) principles and practices, system and network administration, and an understanding of system vulnerabilities, computer forensics, and an adversary's operational methodology.

The Network Hunting Team shall be given the authority to have administrators make changes to the network without going through the full-scale change management process. However, the team shall not circumvent change processes. To be effective, the team shall be allowed to execute in accordance with emergency change procedures that are established by the Enterprise. Emergency change procedures shall be developed such that they ensure changes do not create an unacceptable level of risk.

Network hunting reports shall be created based on the threat type and the mission need. The reported findings on threats and vulnerabilities detected shall be shared with other Organizations, such as JTF-Global Network Operations (GNO), Defense Intelligence Agency (DIA), and other authorities where possible. New indicators and techniques shall be shared in a non-attributable manner to feed back into Detection and Mitigation Capabilities (sharing is defined in the agreements with the Organization).

The Network Hunting Capability shall work in cooperation with other Capabilities in a reactive capacity, when necessary, to help identify how an attacker penetrated the network's defenses. An example of this cooperation would be Network Security Evaluations. Network Hunting can provide information to Network Security Evaluations to



# CGS Network Hunting Capability



Version 1.1.1

inform it of previously unidentified vulnerabilities so that this information can be incorporated into the Network Security Evaluations assessment methods.

## 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.
2. Normal network usage and traffic patterns are known.
3. Software and hardware inventories are accurate and available.
4. An accurate network map exists.
5. System configurations have established security baselines.
6. The mission is understood and documented.

## 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 identifies the anomaly but will not provide remediation.
2. Network Hunting Teams will be provided privileged access.
3. Agreements will be in place between the Network Operations Team and the Network Hunting Team to employ changes.

## 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).

Organizations will determine whether it is more efficient for them to maintain this Capability internally or to outsource its functions. The advantages to maintaining these teams internally include greater flexibility in conducting hunting and defining scope, and an increased involvement by the team in detecting vulnerabilities. The Organization will make this decision based on the needs of the missions it supports.



# CGS Network Hunting Capability



Version 1.1.1

Organizations will use all available data sources, such as the NCI JTF or US-CERT, to research vulnerability and threat indicators to determine what indicators require information. These sources will be further analyzed based on priority, time, resources, threat capability and intent, and risk to help a Network Hunting Team focus its hunting activities.

Organizations will establish a formal process for determining new indicators (feedback mechanism for new indicators based on current indicators) to feed back into the threat database. New indicators and techniques will be shared in a non-attributable manner to feed back into Detection and Mitigation Capabilities (sharing is defined in the agreements with the Organization).

Organizations will ensure that an internal Network Hunting Team is a dedicated security-trained team focused specifically on the Enterprise and overseen by an experienced subject matter expert team leader. In addition, Organizations will ensure that when using an external team, the appropriate agreements are in place (e.g., NDAs, MOUs, Scope Definition Documents). They will also ensure that they have an understanding of the external team's processes, and that the external team has the appropriate skill sets, clearance levels, and agreements in place. As with the internal team, the external team will comprise dedicated security-trained individuals with privilege access and access to other resources focused specifically on the Enterprise and overseen by an experienced subject matter expert team leader.

The Organization shall ensure that all network and system administrators cooperate with the Network Hunting Team's efforts. Cooperative information sharing will allow the team to do its job more effectively and provide the best possible results.

The Organization will use the non-attributable findings from the Network Hunting of other members of the Community to assess its network security posture. These findings will feed into the Organization's Vulnerability Assessment Capability and Network Security Evaluation Capability.

Organizations will ensure that vetted and tested tools are available for searching and parsing beaconing capabilities; extracting Internet Protocol (IP) data and parsing and normalizing the data; checking integrity; dumping memory; performing string searches; and performing binary analysis, static data analysis, user modeling, and behavior analysis. The tools will need to be accredited, address best practices, collect security and intrusion-related activities, and be associated with the Organization's technology focus.



# CGS Network Hunting Capability



Version 1.1.1

## 7 Capability Interrelationships

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

### 7.1 Required Interrelationships

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

- Network Mapping—The Network Hunting Capability relies on the Network Mapping Capability to provide a visual representation of the network and the location of its components.
- Utilization and Performance Management—The Network Hunting Capability relies on the Utilization and Performance Management Capability for information and baseline statistics analysis to help determine adversary activity.
- Understand Mission Flows—The Network Hunting Capability relies on the Understand Mission Flows Capability to identify key components such as normal traffic patterns to fulfill the mission, which enables the Network Hunting Capability to detect and understand anomalies in normal traffic patterns that indicate an attack and identify vulnerabilities in operational systems to ultimately improve the security posture.
- Vulnerability Assessment—The Network Hunting Capability relies on Vulnerability Assessment for information to ensure hunting activities remain current with emerging vulnerabilities.
- Threat Assessments—The Network Hunting Capability relies on the Threat Assessment Capability to provide information about the capabilities that a threat source may possess.
- Network Enterprise Monitoring—The Network Hunting Capability relies on the Network Enterprise Monitoring Capability to provide aggregated analysis and situational awareness information to help determine adversary activity.
- Network Intrusion Detection—The Network Hunting Capability relies on the Network Intrusion Detection Capability to provide information to focus its activities on detecting anomalies, events, incidents, and malicious activities.
- Host Intrusion Detection—The Network Hunting Capability relies on the Host Intrusion Detection Capability to provide information to focus its activities on detecting anomalies, events, incidents, and malicious activities.



# CGS Network Hunting Capability



Version 1.1.1

## 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 Hunting 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 Hunting 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 Hunting Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Network Hunting 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 Hunting 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.

- Hardware Device Inventory–The Network Hunting Capability relies on the Hardware Device Inventory Capability to provide a complete, accurate, and up-to-date database of all hardware components.
- Software Inventory–The Network Hunting Capability relies on the Software Inventory Capability to provide an inventory of each software component pertaining to IA operating networks, systems, and applications.
- Network Security Evaluations–The Network Hunting Capability relies on the Network Security Evaluations Capability to identify vulnerabilities in operational systems, and to demonstrate impact of network vulnerabilities when an attack is launched against the network.



# CGS Network Hunting Capability



Version 1.1.1

- Risk Monitoring–The Network Hunting Capability relies on the Risk Monitoring Capability to provide information used 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>	
SI-4 INFORMATION SYSTEM MONITORING	Control: The organization: <ol style="list-style-type: none"> <li>Monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks;</li> <li>Identifies unauthorized use of the information system;</li> <li>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</li> <li>Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.</li> </ol>
SI-7 SOFTWARE AND INFORMATION INTEGRITY	Control: The information system detects unauthorized changes to software and information. Enhancement/s: <ol style="list-style-type: none"> <li>The organization reassesses the integrity of software and information by performing [Assignment: organization-defined frequency] integrity scans of the information system.</li> <li>The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.</li> <li>The organization employs centrally managed integrity verification tools.</li> </ol>



# CGS Network Hunting Capability



Version 1.1.1

## 9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

### Network Hunting Directives and Policies

Title, Date, Status	Excerpt / Summary
<b>Intelligence Community (IC)</b>	
ICD 702, Technical Surveillance Countermeasures, 18 February 2008, Unclassified	Summary: This directive establishes Director of National Intelligence (DNI) policy and assigns responsibilities for the oversight of the Technical Surveillance Countermeasures (TSCM) programs, in support of the National Intelligence Strategy for the protection of national intelligence and intelligence sources and methods. Representing the convergence of counterintelligence (CI) and security countermeasures, TSCM techniques and countermeasures are designed to detect and nullify a wide variety of technologies used to gain unauthorized access to classified national security information, restricted data, or otherwise sensitive information.
<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
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.
<b>Department of Defense (DoD)</b>	
DoDD O-5240.02, Counterintelligence, 20 December 2007, Classified	Summary: This directive establishes and maintains a comprehensive, integrated, and coordinated Department of Defense (DoD) Counterintelligence (CI) effort under the authority and responsibility of the Under Secretary of Defense for Intelligence (USD (I)). It updates policy and assigns responsibilities for direction, management, coordination, and control of Defense CI activities. These activities consist of integrated DoD and national efforts to



# CGS Network Hunting Capability



Version 1.1.1

	<p>detect, identify, assess, exploit, penetrate, degrade, and counter or neutralize intelligence collection efforts, other intelligence activities, sabotage, espionage, sedition, subversion, assassination, and terrorist activities directed against the DoD, its personnel, information, materiel, facilities, and activities, or against U.S. national security.</p>
<p>DoDI 5240.16, DoD Counterintelligence Functional Services, 21 May 2005, Unclassified</p>	<p>Summary: This instruction assigns responsibilities and prescribes procedures pursuant to DoD Directive (DoDD) 5240.2, DoD CI, 22 May 1997 (reissued as DoDD O-5240.02, CI, 20 December 2007) for the conduct of CI functional services within the DoD. Among the CI functional services DoD component CI organizations are authorized to conduct are specialized CI services such as TSCM and related technical services; and cyber services, including but not limited to, digital forensics and cyber vulnerability assessments.</p>
<p>Defense Reform Initiative Directive (DRID) #27, DoD Computer Forensics Laboratory and Training Program, 10 February 1998, Unclassified</p>	<p>Summary: This document directed the Air Force to establish a joint DoD Computer Forensics Laboratory and Training Program. Its responsibilities include CI and criminal and fraud computer evidence processing, analysis, and diagnostics. It also directed the creation of a training program responsible for providing computer investigation training to individuals and DoD elements that must ensure Defense information systems are secure from unauthorized use, CI, and criminal and fraudulent activities.</p>
<p>DEPSECDEF Memo, DoD Computer Forensics Laboratory (DCFL), and DoD Computer Investigations Training Program (DCITP), 17 August 2001</p>	<p>Summary: This memo ratified the direction set out in Defense Reform Initiative Directive (DRID) #27, dated 10 February 1998, and acknowledged the DoD Computer Forensics Laboratory (DCFL) and DoD Computer Investigations Training Program (DCITP) as fully operational. In addition, it authorized the DCFL to support any DoD investigation (including safety investigations, Inspector General- directed inquiries, and commander inquiries) that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. The DCFL and DCITP should integrate their activities to support infrastructure protection and information operations for ongoing programs and initiatives including the Critical</p>



# CGS Network Hunting Capability



Version 1.1.1

	Infrastructure Protection (CIP) program.
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	

## Network Hunting Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	



# CGS Network Hunting Capability



Version 1.1.1

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. Solution used for implementation—This Capability will require specialized tools (hardware and software) to carry out its functions.
2. Manpower to implement, maintain, and execute—Personnel will be required to respond to requests and carry out Capability functions. Use of an internal versus external team will affect costs, motivations, and response time.

## 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 Hunting Capability.

- The Enterprise shall look for indicators of an active threat or exploitation of a vulnerability that was previously known or unknown. Network hunting may involve



# CGS Network Hunting Capability



Version 1.1.1

signature detection and detection of changes in behaviors and normal usage, as well as the ability to detect incidents that are not known to be occurring.

- The Enterprise shall have a Network Hunting Program, sufficient staff, and a plan to administer, report, and follow up on threat, vulnerability, and hunting evaluations.
- The Enterprise shall detect known or unknown anomalies associated with the network components and the Enterprise in which the network resides.
- The Enterprise shall look for indicators to identify both known and unknown threats and activities that could indicate an intrusion, or evidence of attack against the network and take or initiate action to respond to this attack.
- The Enterprise shall take a proactive approach, using known vulnerability or threat indicators to feed into network hunting activities to detect previously unidentified vulnerabilities or threats.
- Network hunters shall understand how to exploit a vulnerability and use that knowledge to conduct searches to determine any indication of malicious activity.
- The Enterprise shall use all authoritative data sources to research indicators. These sources shall be further analyzed based on priority, time, resources, threat capability and intent, and risk to help network hunting teams focus their hunting activities.
- A formal process shall be established for determining new indicators to feed back into the threat database using underlying network details to determine which indicators might apply, such as operating system software and hardware.
- When network hunting teams are internal, they shall be a dedicated team in a separate department from the network and system administrators to prevent conflict of interest.
- When an external team is used for network hunting services, the service provider shall comply with the appropriate agreements that are in place (e.g., NDAs, MOUs, and Scope Definition Documents).
- Network hunting teams shall comply with any Community-established certification standards to ensure the team has the appropriate level of technology knowledge and understanding of the hunting methodology.
- Network hunting teams shall comprise individuals who have demonstrated practical experience with IA principles and practices, system and network administration, and an understanding of system vulnerabilities, computer forensics, and an adversary's operational methodology.
- The network hunting team shall be given the authority to have administrators make changes to the network without going through the full-scale change management process (e.g., emergency change procedures); however, the team shall not



# CGS Network Hunting Capability



Version 1.1.1

circumvent change processes but shall be allowed to execute in accordance with emergency change procedures that are established by the Enterprise but that ensure changes do not create an unacceptable level of risk.

- Network hunting reports shall be created based on the threat type and the mission need.
- The reported findings on threats and vulnerabilities detected shall be shared with other Organizations, such as Joint Task Force-Global Network Operations (JTF-GNO), DIA, and other authorities, where possible. New indicators and techniques shall be shared in a non-attributable manner.