



National Security Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Physical Hunting Capability

Version 1.1.1

Physical Hunting is employed to detect anomalies in the physical components, and vulnerabilities associated with those components, in the physical infrastructure of the Enterprise. Physical Hunting may involve detection of technical surveillance devices (e.g., keystroke taps, bugs). This Capability provides for hardware forensics and searching for vulnerabilities in the physical Enterprise, including intended emanations and changes to the environment.

07/30/2012



# CGS Physical 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.....	6
6	Organizational Implementation Considerations .....	6
7	Capability Interrelationships.....	6
7.1	Required Interrelationships .....	6
7.2	Core Interrelationships .....	6
7.3	Supporting Interrelationships.....	7
8	Security Controls .....	8
9	Directives, Policies, and Standards .....	9
10	Cost Considerations .....	15
11	Guidance Statements.....	16



# CGS Physical 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 Physical 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.

Physical Hunting is employed to detect anomalies in the physical components, and vulnerabilities associated with those components, in the physical infrastructure of the Enterprise. Physical Hunting may involve detection of technical surveillance devices (e.g., keystroke taps, bugs). This Capability provides for hardware forensics and searching for vulnerabilities in the physical Enterprise, including intended emanations and changes to the environment.

## 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 Enterprise shall have a program, staff, and plan to administer, report, and follow up on assessments and incident investigations. This Capability addresses the ability to detect intentional and unintentional anomalies associated with the physical components of a network and with the facilities in which the network resides. It covers all Physical Hunting activities in security and counterintelligence, and technical security areas including Technical Surveillance Countermeasures (TSCM) and TEMPEST activities. TSCM is employed to seek out intentional anomalies, and TEMPEST activities are employed to determine whether any unintentional anomalies exist. TEMPEST inspections are required for all Sensitive Compartmented Information Facility (SCIF) facilities or spaces.

TSCM-trained personnel are capable of conducting physical and instrumented technical inspections of facilities for the presence of technical surveillance devices and technical security weaknesses. Trained and certified experts are required for performing Physical Hunting activities. All staff conducting TSCM activities receive TSCM training from the Interagency Training Center (ITC).



# CGS Physical Hunting Capability



Version 1.1.1

TEMPEST-trained personnel are capable of conducting physical and instrumented evaluations of facilities for compromising emanations, which may be caused by poor design, installation, maintenance, or component age and degradation that cause sensitive or classified information to emanate from a facility. TEMPEST evaluations also include an assessment of physical security protections and how the protections in place prevent compromising emanations. In addition, TEMPEST evaluations include an assessment of physical controls such as guards and badging. All TEMPEST inspectors shall obtain training at the National TEMPEST School. All TEMPEST teams have one Certified TEMPEST Technical Authority (CTTA) physically present per inspection.

The Enterprise may obtain Physical Hunting technical services from other Organizations, after executing the appropriate Organizational agreements, or it may use its own certified technical staff to conduct the actual sweeps or assessments. For TEMPEST inspections, each Organization may obtain external support for the TEMPEST team, but the CTTA shall be government staff. TEMPEST evaluations are required before any facility processes Sensitive Compartmented Information (SCI). Evaluations are also conducted upon SCIF reaccreditation (see agency-specific policy for frequency, listed in the Directives and Policies Table), when a SCIF facility changes the type of information it is processing, or when a SCIF changes its facility structure. In addition to facility inspections, TEMPEST evaluations are also conducted on new cryptographic equipment that is directly responsible for encryption (currently part of the cryptographic modernization effort). This is conducted during the development phase of the equipment, prior to deployment and operations.

To support forensic investigation and Physical Hunting activities, a strict chain of custody is maintained for any physical evidence that shall be confiscated or modified. The TSCM Team shall have appropriate authority (in agreement with the customer Organization) to conduct/support activities for forensic investigations, and all legal and procedural provisions shall be in place to do so.

The TSCM Team shall complete an out-brief and generate a report of the findings within 5 days of completion (or other alternate timeframe agreed upon by the client Organizations) and findings shall be categorized by severity to indicate vulnerabilities that may require immediate attention. Mitigation of the vulnerabilities falls to the client Organization and is not the responsibility of the TSCM Team, although the team may be asked to support mitigation decisions. The Capability shall communicate with the Vulnerability Assessment and Risk Assessment Capabilities, to determine severity and remediation action to be taken under the Incident Response Capability.



# CGS Physical Hunting Capability



Version 1.1.1

The TEMPEST Team provides a findings and requirements report upon completion of the evaluation. Mitigation of the vulnerabilities falls to the client Organization and is not the responsibility of the TEMPEST Team, although the team may be asked to support mitigation decisions. The CTTA shall determine the appropriate amount of time for the facility to apply the mitigations/corrections to maintain the SCIF accreditation. The CTTA present has the authority to order the facility to stop processing SCI information if he or she finds the severity of emanation leakage to be too high. Severity shall be determined by the CTTA based on the facility's risk posture.

The department or agency shall participate in TSCM community working groups, information sharing, community-sponsored training, and forums and be linked to provided input to and receive reporting from the community research and development (R&D) activities for physical anomaly detection. The R&D component is necessary to ensure the Capability is kept apprised of the latest technology and methods in TSCM and TEMPEST detections. Communications with the TEMPEST Advisory Group (TAG) are maintained for CTTA approvals and community coordination.

For additional Capability Gold Standard Guidance please see the CGS Classified Annex.

## 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 facility employs guards who check for obvious facility anomalies.
2. Users all are authenticated before gaining access to the facilities or network resources.
3. Physical security controls and TEMPEST-related protections are in place for network components, other technology devices, and the facility itself.
4. Equipment from outside sources is inspected by the client Organization prior to being introduced to the facility or network.
5. The Enterprise provides the appropriately trained local resources for the TSCM/TEMPEST Team.
6. The physical protection components can be defeated.



# CGS Physical Hunting Capability



Version 1.1.1

## 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 enables the assessment of any problem areas identified but does not apply corrections.
2. The Capability provides inspection of network components to prevent the connection of unauthorized devices to system resources.
3. This Capability acts as a deterrent for attacks on the physical components.
4. The Capability enables the TEMPEST CTTA to order the facility to cease processing if findings are severe enough.
5. The Capability provides a physical TEMPEST evaluation of the facility protections in place to ensure that they do not enable compromising emanations.

## 6 Organizational Implementation Considerations

For Organizational Implementation Considerations please see the CGS Classified Annex.

## 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.

- Threat Assessments–The Physical Hunting Capability relies on the Threat Assessment Capability to provide information about the capabilities that a threat source may possess.

### 7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.



# CGS Physical Hunting Capability



Version 1.1.1

- Portfolio Management—The Physical 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 Physical 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 Physical Hunting Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Physical 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 Physical 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.

- Vulnerability Assessment—The Physical Hunting Capability relies on the Vulnerability Assessment Capability for information so that hunting activities remain current with emerging vulnerabilities.
- Physical Enterprise Monitoring—The Physical Hunting Capability relies on the Physical Enterprise Monitoring Capability to provide monitoring of events that may trigger hunting activities.
- Incident Response—The Physical Hunting Capability relies on the Incident Response Capability for information that can be used to initiate and adjust hunting activities.
- Risk Monitoring—The Physical Hunting Capability relies on the Risk Monitoring Capability to make adjustments to its functions as the Enterprise risk posture changes over time.



# CGS Physical Hunting Capability



Version 1.1.1

## 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-19 ACCESS CONTROL FOR MOBILE DEVICES	<p>c. Monitors for unauthorized connections of mobile devices to organizational information systems.</p> <p>h. Applies [Assignment: organization-defined inspection and preventative measures] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.</p> <p>Enhancement/s:</p> <p>(4) The organization:</p> <p>(b) Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information: Connection of unclassified mobile devices to classified information systems is prohibited; Connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s); Use of internal or external modems or wireless interfaces within the mobile devices is prohibited; and Mobile devices and the information stored on those devices are subject to random reviews/inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed.</p> <p>Supplemental Guidance: Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed.</p> <p>Specially configured mobile devices include, for example,</p>



# CGS Physical Hunting Capability



Version 1.1.1

	computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive.
PE-3 <i>PHYSICAL ACCESS CONTROL</i>	Enhancement/s: (2) The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components. (5) The information system detects/prevents physical tampering or alteration of hardware components within the system.
PE-19 <i>INFORMATION LEAKAGE</i>	Control: The organization protects the information system from information leakage due to electromagnetic signals emanations. Enhancement/s: (1) The organization ensures that information system components, associated data communications, and networks are protected in accordance with: (i) national emissions and TEMPEST policies and procedures; and (ii) the sensitivity of the information being transmitted.
SI-4 <i>INFORMATION SYSTEM MONITORING</i>	Enhancement/s: (14) The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

## 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.

### Physical Hunting Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 702, Technical	Summary: This directive establishes Director of National



# CGS Physical Hunting Capability



Version 1.1.1

<p>Surveillance Countermeasures, 18 February 2008, Unclassified</p>	<p>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 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. These activities are applicable to Physical Hunting.</p>
<p>ICD 705, Sensitive Compartmented Information Facilities, 26 May 2010, Unclassified</p>	<p>Summary: 1. This directive establishes that all Intelligence Community (IC) Sensitive Compartmented Information Facilities (SCIF) shall comply with uniform IC physical and technical security requirements (hereinafter “uniform security requirements”). This mandate is designed to ensure the protection of information and foster efficient, consistent, and reciprocal use of SCIFs in the IC. This directive applies to all facilities accredited by IC elements where Sensitive Compartmented Information (SCI) is processed, stored, or discussed. This directive rescinds Director of Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, including the Manual for Physical Security Standards for Sensitive Compartmented Information Facilities, and all DCID 6/9 Annexes. This Directive also rescinds IC Policy Memorandum (ICPM) 2005-700-1, Intelligence Community Update to Director of Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs); ICPM 2006-700-7, Intelligence Community Modifications to DCID 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)””; and ICPM 2007-700-2, Intelligence Community Modifications to Annex C of Director of Central Intelligence Directive 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs).”</p>



# CGS Physical Hunting Capability



Version 1.1.1

<p>NSTISSAM TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements Electromagnetics, Classified</p>	<p>Summary: This document specifies test procedures for identifying the conducted and electromagnetic radiation emanations characteristics of individual equipment in a laboratory environment. The actual document is classified.</p>
<p>NSTISS TEMPEST/1-93, Compromising Emanations Field Test Requirements, Electromagnetics, 30 August 1993, Classified</p>	<p>Summary: This document specifies test procedures for conducting an instrumented TEMPEST test in a field environment. The actual document is classified.</p>
<p>NSTISS TEMPEST/1-95, Shielded Enclosures, 30 January 1995, Classified</p>	<p>Summary: This document describes the types and characteristics of shielded enclosures and shielding methods to be applied by U.S. government departments and agencies as a TEMPEST countermeasure.</p>
<p>NSTISS TEMPEST/2-91, Compromising Emanations Analysis Handbook, 20 December 1991, Classified</p>	<p>Summary: This handbook describes analysis concepts and techniques currently in use for signals analysis before, during, and after TEMPEST testing. The actual document is classified.</p>
<p>NSTISS TEMPEST/2-92, Procedures for TEMPEST Zoning, 20 December 1992, Classified</p>	<p>Summary: This document specifies test procedures for identifying the attenuation characteristics of facilities and assigning TEMPEST Zone designations based on these characteristics. The actual document is classified.</p>
<p><b>Comprehensive National Cybersecurity Initiative (CNCI)</b></p>	
<p>NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified</p>	<p>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.</p>
<p><b>Department of Defense (DoD)</b></p>	
<p>DoDD O-5240.02, Counterintelligence, 20 December 2007,</p>	<p>Summary: This directive establishes and maintains a comprehensive, integrated, and coordinated DoD Counterintelligence (CI) effort under the authority and</p>



# CGS Physical Hunting Capability



Version 1.1.1

<p>Unclassified</p>	<p>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 Department of Defense (DoD) and national efforts to 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. CI is useful in the pursuit of Physical Hunting. This directive specifies certification requirements for team members.</p>
<p>DoDI 5240.05, Technical Surveillance Countermeasures (TSCM) Program, 22 February 2006, Unclassified</p>	<p>Summary: This instruction reissues DoD Instruction 5240.5 dated May 23, 1984, and implements DoD Directive 5240.2 as it pertains to the DoD TSCM program. It also defines the role of TSCM as one of the CI functional services and the responsibilities of the Director, DoD Counterintelligence Field Activity (DoD CIFA) and the Director, National Security Agency (NSA)/Central Security Service (CSS) in the DoD TSCM program.</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 Counterintelligence (CI), 22 May 1997 (reissued as DoDD O-5240.02, Counterintelligence, 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 specialized CI services such as TSCM and related technical services and cyber services, including but not limited to, digital forensics and cyber vulnerability assessments. These activities are closely related to Physical Hunting.</p>
<p>Defense Reform Initiative Directive (DRID) #27, DoD Computer Forensics Laboratory and Training</p>	<p>Summary: This document directed the Air Force to establish a joint DoD Computer Forensics Laboratory and Training Program. Its responsibilities include CI, criminal, and fraud computer evidence processing, analysis, and</p>



# CGS Physical Hunting Capability



Version 1.1.1

<p>Program, 10 February 1998, Unclassified</p>	<p>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. These activities fall within the scope of Physical Hunting.</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 #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 Infrastructure Protection (CIP) program. This falls within the scope of Physical Hunting.</p>
<p>Committee for National Security Systems (CNSS)</p>	
<p>CNSSP 300 National Policy on Control of Compromising Emanations, 01 April 2004, Classified</p>	<p>Summary: This document establishes national TEMPEST policy for national security systems and supersedes National Security Telecommunications and Information Systems Security Policy (NSTISSP) 300, "National Policy on Control of Compromising Emanations," dated 29 November 1993.</p>
<p>CNSSI 7000, TEMPEST Countermeasures for Facilities, 13 March 1995, Classified</p>	<p>Summary: This document establishes guidelines and procedures that shall be used by departments and agencies to determine the applicable TEMPEST countermeasures for national security systems. The document is classified.</p>
<p>Other Federal (OMB, NIST, ...)</p>	
<p>Nothing found</p>	



# CGS Physical Hunting Capability



Version 1.1.1

Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

## Physical Hunting Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
DoD S-5240.05-M-1, The Conduct of Technical Surveillance Countermeasures volume I, 14 May 2007, Classified	Summary: This manual addresses the conduct of technical surveillance countermeasures. The actual document is classified.
DoD S-5240.05-M-2, The Conduct of Technical Surveillance Countermeasures volume II, 13 November 2007, Classified	Summary: This manual addresses the conduct of technical surveillance countermeasures. The actual document is classified.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	



# CGS Physical Hunting Capability



Version 1.1.1

Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
NSTISSAM Level I – Compromising Emanations Laboratory Test Standard, Classified	Summary: This is the strictest standard for devices that will be operated in North Atlantic Treaty Organization (NATO) Zone 0 environments, where it is assumed that an attacker has almost immediate access (e.g., neighbor room, 1 m distance). The actual document is classified.
NSTISSAM Level II – Laboratory Test Standard for Protected Facility Equipment, Classified	Summary: This is a slightly relaxed standard for devices that are operated in NATO Zone 1 environments, where it is assumed that an attacker cannot get closer that about 20m (or where building materials ensure an attenuation equivalent to the free-space attenuation of this distance). The actual document is classified.
NSTISSAM Level III – Laboratory Tested Standard for Tactical Mobile Equipment/Systems, Classified	Summary: This is an even more relaxed standard for devices operated in NATO Zone 2 environments, where attackers have to deal with about 100 m worth of free-space attenuation (or equivalent attenuation through building materials). The actual document is classified.
NATO SDIP-29 – Installation of Electrical Equipment for Processing of Classified Information, Classified	Summary: This standard defines installation requirements, for example, with respect to grounding and cable distances. The actual document is classified.
AMSG 799B – NATO Zoning Procedures, Classified	Summary: This document defines attenuation measurement procedures, according to which individual rooms within a security perimeter can be classified into Zone 0, Zone 1, Zone 2, or Zone 3, which then determines what shielding standard is required for equipment that processes Secret data in these rooms. The actual document is classified.



# CGS Physical Hunting Capability



Version 1.1.1

## 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 may incur travel expenses and other costs associated with research.
2. Necessary training—Investigators need to understand policies and procedures as well as investigation techniques.
3. Manpower to implement, maintain, and execute—Use of an internal versus external team will affect costs, motivations, and response time.
4. Time to implement, maintain, and execute—Investigations can be time-consuming.

## 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 Physical Hunting Capability.

- The Enterprise shall use Physical Hunting to detect anomalies in the physical components, and vulnerabilities associated with those components, in the physical infrastructure and Enterprise. Physical hunting shall involve detection of technical surveillance devices (keystroke taps, bugs, etc.) along with searching



# CGS Physical Hunting Capability



Version 1.1.1

for vulnerabilities in the physical Enterprise, including intended emanations and changes to the environment and hardware forensics.

- Each Enterprise shall have a program, staff, and plan to administer, report, and follow up on assessments and incident investigations.
- The Enterprise shall detect intentional and unintentional anomalies associated with the physical components of a network and with the facilities in which the network resides, including hunting activities in security and counterintelligence and in technical security areas.
- TSCM shall be employed to seek out intentional anomalies.
- TEMPEST activities shall be employed to determine whether any unintentional anomalies exist.
- TEMPEST inspections shall be required for all SCIF facilities or spaces.
- TSCM-trained and certified experts shall perform physical hunting activities. All staff conducting TSCM activities shall receive TSCM training from the ITC.
- All TEMPEST inspectors shall obtain training at the National TEMPEST School and be capable of conducting physical and instrumented evaluations of facilities for compromising emanations.
- TEMPEST evaluations shall include an assessment of physical security protections and how the protections in place prevent compromising emanations. In addition, TEMPEST evaluations shall include an assessment of physical controls such as guards and badging.
- All TEMPEST teams shall have one CTTA physically present per inspection.
- If the Enterprise obtains physical hunting technical services from an external Organization, the appropriate Organizational agreements shall be executed.
- Each Organization may obtain external support for the TEMPEST team performing inspections; however, the CTTA shall be government staff.
- Sweeps or inspections shall be conducted frequently and shall not always require a severe trigger or case to be made to conduct a sweep. Indicators and trend analysis from monitoring activities shall be used to determine what inspections shall occur.
- Scans performed as a result of a trigger shall use the latest hardware forensics techniques to identify any anomalies. Unauthorized devices and anomalies shall be reported.
- Tempest evaluations shall be conducted before any facility processes SCI, upon SCIF reaccreditation (see agency-specific policy for frequency), when a SCIF facility changes the type of information it is processing, or when a SCIF changes its facility structure.



# CGS Physical Hunting Capability



Version 1.1.1

- TEMPEST evaluations shall be conducted on new cryptographic equipment that is directly responsible for encryption during the development phase of the equipment.
- The Technical Surveillance Countermeasures team shall have appropriate authority (in agreement with the customer Organization) to conduct/support activities for forensic investigations, and all legal and procedural provisions shall be in place to do so.
- A strict chain of custody shall be maintained for any physical evidence that shall be confiscated or modified to support forensic investigation and physical hunting activities.
- The TSCM team shall complete an out-brief and generate a report of the findings within 5 days of completion (or other alternate timeframe agreed upon by the client Organizations) and findings shall be categorized by severity to indicate vulnerabilities that may require immediate attention.
- The TSCM team shall support the client Organization with the mitigation of vulnerabilities as needed and assist in determining severity and remediation action to be taken under incident response.
- The TEMPEST team shall provide a findings and requirements report upon completion of the evaluation.
- The CTTA shall determine the appropriate amount of time for the facility to apply the mitigations/corrections to maintain the SCIF accreditation. The CTTA present shall have the authority to order the facility to stop processing SCI information if the severity of emanation leakage is too high, based on the facility's risk posture.
- The Enterprise shall participate in TSCM community working groups, information sharing, community-sponsored training, and forums and be linked to provided input to and receive reporting from the community research and development (R&D) activities for physical anomaly detection.