DHS 4300A Sensitive Systems Handbook

Attachment F

To Handbook v. 11.0

Incident Response

Version 11.0

April 24, 2015

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
0.1		Draft Baseline Release
0.2	February 9, 2004	Revised Document Title
2.0	March 31, 2004	Undergoing development
2.1	August 31, 2004	Added content
3.0	August 15, 2005	Revision to Section 3.1.4.2 (“Law Enforcement”)
4.0	June 1, 2006	Minor editorial changes. Appendix F2 contact information updated
4.1	March 23, 2007	Update based on SOC CONOPS, March 12, 2007
5.1	April 18, 2007	Update based on SOC CONOPS, Final Version 1.4.1, April 16, 2007; Updates the term, Sensitive But Unclassified to For Official Use Only
5.2	June 1, 2007	Minor editiorial changes.
5.3	October 1, 2007	Updated to focus on incident management and closeout.
6.0	May 14, 2008	Updated Figure F-3, Incident Reporting Process Updated Figure F-4 – DHS ENTERPRISE SOC Organization
6.1	September 23, 2008	Global Replaced “CPO” with “Chief Privacy Officer.” Replaced “CISOs/ISSMs” with “Component CISOs/ISSMs.” Section 1.0 1.4 – Updated title and date of NIST SP 800-53. Section 2.0 2.1.1 – Updated section to reflect changes to the security incident handling section in 4300A Policy. Section 3.0 3.1.4.3 – Updated section based on updated text in 4300A Policy. Section 4.0 4.4, third paragraph – Replaced text with “The DHS ENTERPRISE SOC will coordinate support from Components with appropriate capabilities for support in handling incidents requiring computer forensics.” 4.4.1, first paragraph – Updated text with the most recent policy text. 4.4.3 – Replaced “through coordination among its…” with “the DHS ENTERPRISE SOC will coordinate among the…” Section 6.0 6.6, first paragraph, second sentence – Replace “may inadvertently bring classified information…” with “may inadvertently pass collateral (classified) information…” 6.6, fourth paragraph, first sentence – Replace “…clean up the spillage” with “to perform spillage cleanup.” Appendix F3 Replaced “Minor – Small scale (19 or less users)” with “Minor – Small scale (19 or fewer users)…”

Version	Date	Description
7.0	August 7, 2009	2.1.1 and 4.4.1 Updated policy based on changes to 4300A
11.0	April 24, 2015	Entire document rewritten to align with current standards and directives. Throughout: "DHS Enterprise SOC" replaced by "DHS OneNet SOC."

CONTENTS

TABLES

1.0 INTRODUCTION

1.1 Purpose

This attachment defines and documents requirements, guidance, and procedures that implement security incident management policy as given in Department of Homeland Security (DHS) Sensitive Systems Policy Directive 4300A, within the Department, including Headquarters and all Components. This document is intended to be adaptable and fluid, and will be changed as security requirements and the DHS Information Technology (IT) environment change.

1.2 Scope and Application

Incident response encompasses all actions taken to quickly restore normal IT service and to minimize adverse impacts on business operations. This document provides guidance for handling every category of information systems security incident and applies to DHS Headquarters, all DHS Components, DHS Data Centers, and to any company, consultant, partner, or Government agency that is receiving Federal funds from DHS or performing a Federal function on behalf of, or in cooperation with, DHS.

1.3 Authorities and References

Federal Laws

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899

Privacy Act of 1974 (Privacy Act), as amended Pub L 93-579, 88 Stat 1896, 5 U.S.C. § 552a

Freedom of Information Act of 2002 as amended, Pub L 93-579, 5 U.S.C. 552

Executive Orders and Directives

Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003

Office of Management and Budget (OMB) Publications

OMB Circular A-130, "Management of Federal Information Resources," revised, November 30, 2000

OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006

OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007

Department of Homeland Security Management Directives

MD 140-01, "Information Technology Systems Security," July 31, 2007

MD 11056.1, "Sensitive Security Information (SSI)," November 3, 2006

MD 11060.1, "Operations Security Program," September 25, 2006

Department of Homeland Security Publications

DHS Sensitive Systems Policy Directive 4300A, v9.1, June 2012

DHS 4300A Sensitive Systems Handbook, v9.1, June 2012

DHS Privacy Incident Handling Guidance, v3.0, January 26, 2012. *[Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf*]*

Homeland Secure Data Network (HSDN) Security Plan

Incident Response Plan for Homeland Secure Data Network (HSDN)

Standard Operating Procedures (SOP) for the Operation of the Security Operations Center (SOC)

DHS Security Operations Center Concept of Operations (CONOPS), v1.4.4, September 30, 2007.

United States Secret Service Publications

"Best Practices for Seizing Electronic Evidence," v.3, 2006

National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS)

National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006

National Institute of Standards and Technology (NIST) Special Publications (SP)

NIST SP 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013

NIST SP 800-61, Rev 2, "Computer Security Incident Handling Guide," August 2012

NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response," August 2006

NIST SP 800-126, Rev 1.2, "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP," September 2011

United States Computer Emergency Response Team Publications

US-CERT "Concept of Operations for Federal Cyber Security Incident Handling," v3.2, April 2005

Publications of the Committee on National Security Systems (CNSS)

CNSS-079-07, "Frequently Asked Questions (FAQ) on Incidents and Spills," August 2007

2.0 OVERVIEW OF DHS INCIDENT RESPONSE CAPABILITY

This section provides a basic description and understanding of DHS incident response capability, incident reporting structure, incident priority levels, and provides essential definitions.

2.1 Background

Incident response capability provides a consistently effective means of responding to and reporting on information systems security incidents.

2.2 Definitions

For purposes of classification, DHS incident response procedures use the definitions given below. Additional definitions will be given in the document where needed; all relevant terms and definitions will be found in the glossary, Appendix F-5.

Event: An occurrence, not yet assessed, that may affect the performance of an Information System.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the data the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Minor Incident**:** An incident that due to proper functioning of a security control is not likely to impact the DHS mission or a critical DHS asset. Minor incidents do not require immediate leadership notification.

A minor incident meets one or more of the following criteria:

- The incident impacts the confidentiality, integrity, or availability of a non-critical system or non-sensitive data.
- The incident relates to a minor policy violations.

Personally Identifiable Information (PII): Any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, a visitor to the U.S., or a Department employee or contractor. (See also Sec. 3.10.5 for amplification).

Significant Incident: An incident related to computer security whose impact on the DHS mission or on a critical DHS asset constitutes a meaningful threat to the DHS mission and requires immediate notification of leadership.

A significant incident meets one or more of the following criteria:

- The incident has impacts the confidentiality, integrity, or availability of a critical system or sensitive data (for example PII or FOUO).
- There is a high probability of public disclosure of the incident and consequent embarrassment of the Department.
- The impact of the incident results in DHS users losing access to a critical service (for example, email, network access, Internet access).

***Spillage*:** A security incident that results in the transfer of classified or Sensitive But Unclassified (SBU) information onto an information system or to a medium, person, or location not accredited (i.e., authorized) for the appropriate security level.

***Technical Classified Spill*:** A security incident that results in the spillage of classified information (Confidential, Secret, or Top Secret) to information systems or other digital media not authorized to process data at that level. Examples include e-mailing a classified document from an account authorized to process up to SECRET to another account only authorized to process unclassified material, or saving a SECRET document onto a thumb drive or CD on a secure workstation and uploading it to a sensitive but unclassified (SBU) workstation.

Non-Technical Classified Spillage: A security incident involving spillage of classified information occurring outside of an IT environment.

Sanitization or Wiping: The use of an approved method and utility to decontaminate or disinfect a system, an application, or media to make suitable for re-use, without physically destroying what is disinfected. Wiping usually refers to the use of an approved software utility that writes data over a hard disk multiple times using several different data patterns.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source

Critical System: A system with a FIPS 199 criticality rating of “High”.

Non-Critical System: Any system with a FIPS 199 criticality rating other than “High”.

3.0 DHS, HSDN, AND COMPONENT SECURITY OPERATIONS CENTERS

The DHS CIO established the DHS OneNet Security Operations Center (SOC) and authorized the establishment of subordinate DHS Component SOCs. A separate SOC has been established for the Homeland Secure Data Network (HSDN).

An essential part of the missions of the DHS ONENET SOC and of the HSDN SOC is to ensure that SBU and SECRET IT resources are secure and available for use by the Department in accomplishing its mission; the SOCs are also responsible for validation of compliance with security policy and controls throughout the Department. The descriptions that follow define SOC operations and the interaction between the DHS ONENET SOC, the HSDN SOC, and Component SOCs.

The DHS ONENET SOC works closely with the HSDN SOC, DHS Office of Intelligence and Analysis (I&A), and the DHS Chief Security Officer (CSO) to coordinate security operations.

The HSDN SOC is the central coordinating and reporting authority for all computer security incidents that occur on the HSDN throughout the Department.

Primary focus areas of the DHS ONENET SOC and the HSDN SOC include monitoring the DHS environment for attacks, potential threats or vulnerabilities; providing DHS management with unfettered situational visibility throughout the DHS enterprise; and providing guidance, direction, and support for Component CIOs in building Component SOC capabilities. The DHS and HSDN SOCs also provide operational support for Information Systems Security Managers (ISSM) and IT support staff during incidents, and coordinate with other resources internal and external to DHS to address and investigate incidents that require special handling. SOCs may also be required to perform proactive vulnerability assessment and penetration testing activities if these capabilities do not exist elsewhere within the Component. DHS ONENET SOC and Component SOC personnel are trained to provide SOC services.

Component SOCs are operationally subordinate to the DHS ONENET SOC and keep the DHS ONENET SOC advised of information security posture within their respective Components, including incident and vulnerability management, analysis, remediation, and reporting.

The HSDN SOC is responsible for security operations on the HSDN and works closely with the DHS ONENET SOC to provide threat intelligence and classified information spillage handling.

The DHS ONENET SOC enables computer security situational awareness throughout the Department, and is able to provide additional services to Components through Service Level Agreements (SLA). The DHS ONENET SOC serves as a central data repository and a reporting, and coordinating point for computer security incidents. The DHS ONENET SOC is capable of responding to incidents 24/7, and provides technical assistance to Components.

This document outlines the basic functions in incident response of the DHS ONENET SOC and details how the SOC interfaces with Component SOCs, the National Operations Center, Network Operations Centers, Chief Information Officers (CIO), Chief Information Security Officers (CISO), ISSMs and ISSOs, the DHS Privacy Office, the DHS Chief Security Officer (CSO), the backup SOC, the backup NOC, external organizations, and law enforcement agencies. This document also outlines the basic functions of the HSDN SOC and lays the groundwork for future operational reporting.

In addition, this document includes reporting and coordination requirements from the DHS ONENET SOC to provide guidance and direction to Component SOCs to proactively maintain a strong security posture. The DHS ONENET SOC will also provide detailed procedures that require acknowledgement, reporting, and remediation of security events.

Figure 1 shows the organization of the DHS ONENET SOC and reflects its operational structure. The DHS ONENET SOC reports to the DHS CIO, who, along with the DHS CISO provides senior management guidance and direction to the SOC, which in turn provides guidance to Component SOCs.

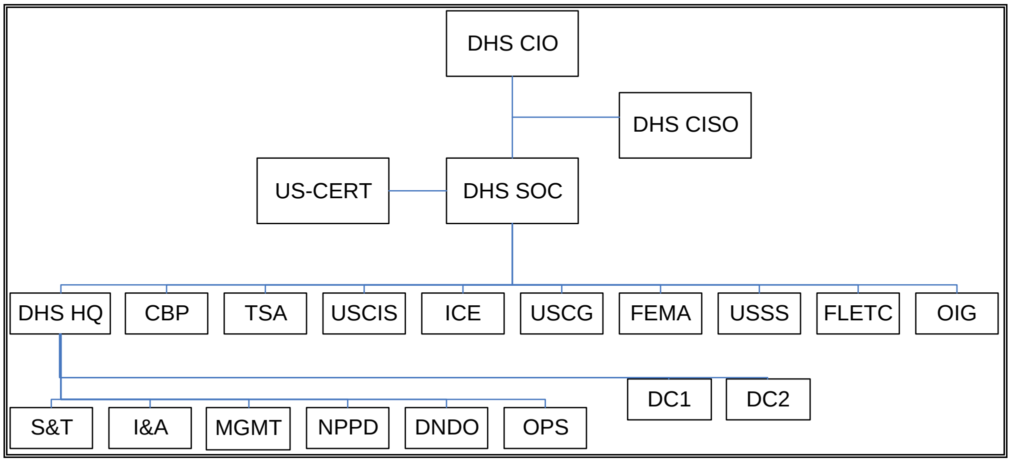

Figure 1: DHS ONENET SOC Organization. (Acronyms defined in Appendix A)

3.1 DHS Security Incidents and Incident Response and Reporting Policy

DHS Sensitive Systems Policy Directive 4300A, Section 4.9, contains the DHS policy elements governing incident response.

3.2 Incident Response Report Flow

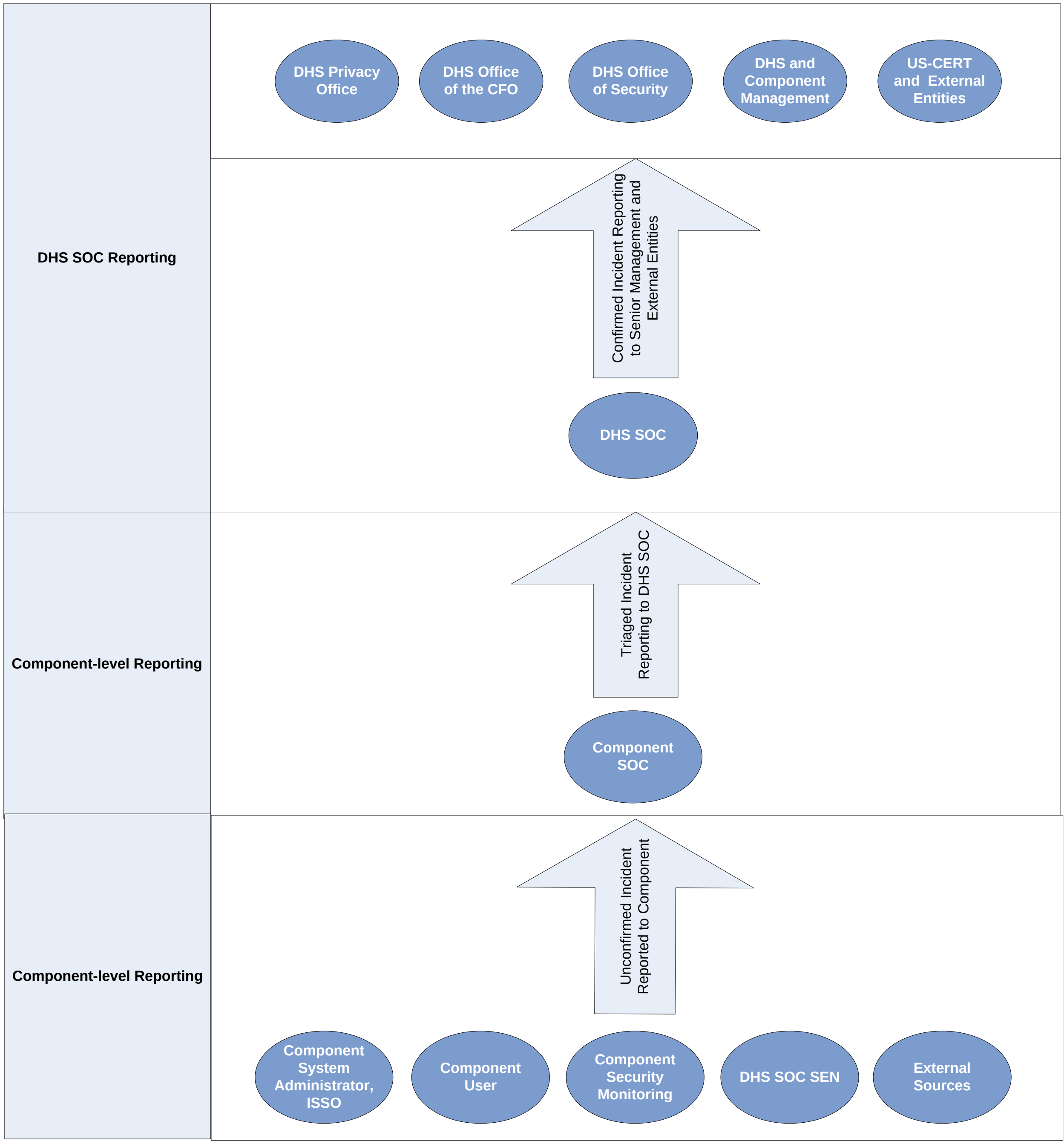
DHS SOC Reporting
DHS Privacy Office
DHS Office of the CFO
DHS Office of Security
DHS and Component Management
US-CERT and External Entities
Confirmed Incident Reporting to Senior Management and External Entities
DHS SOC
Component-level Reporting
Triaged Incident Reporting to DHS SOC
Component SOC
Component-level Reporting
Unconfirmed Incident Reported to Component
Component System Administrator, ISSO
Component User
Component Security Monitoring
DHS SOC SEN
External Sources

Figure 2: Incident response reporting flow

3.3 DHS Incident Response Life Cycle

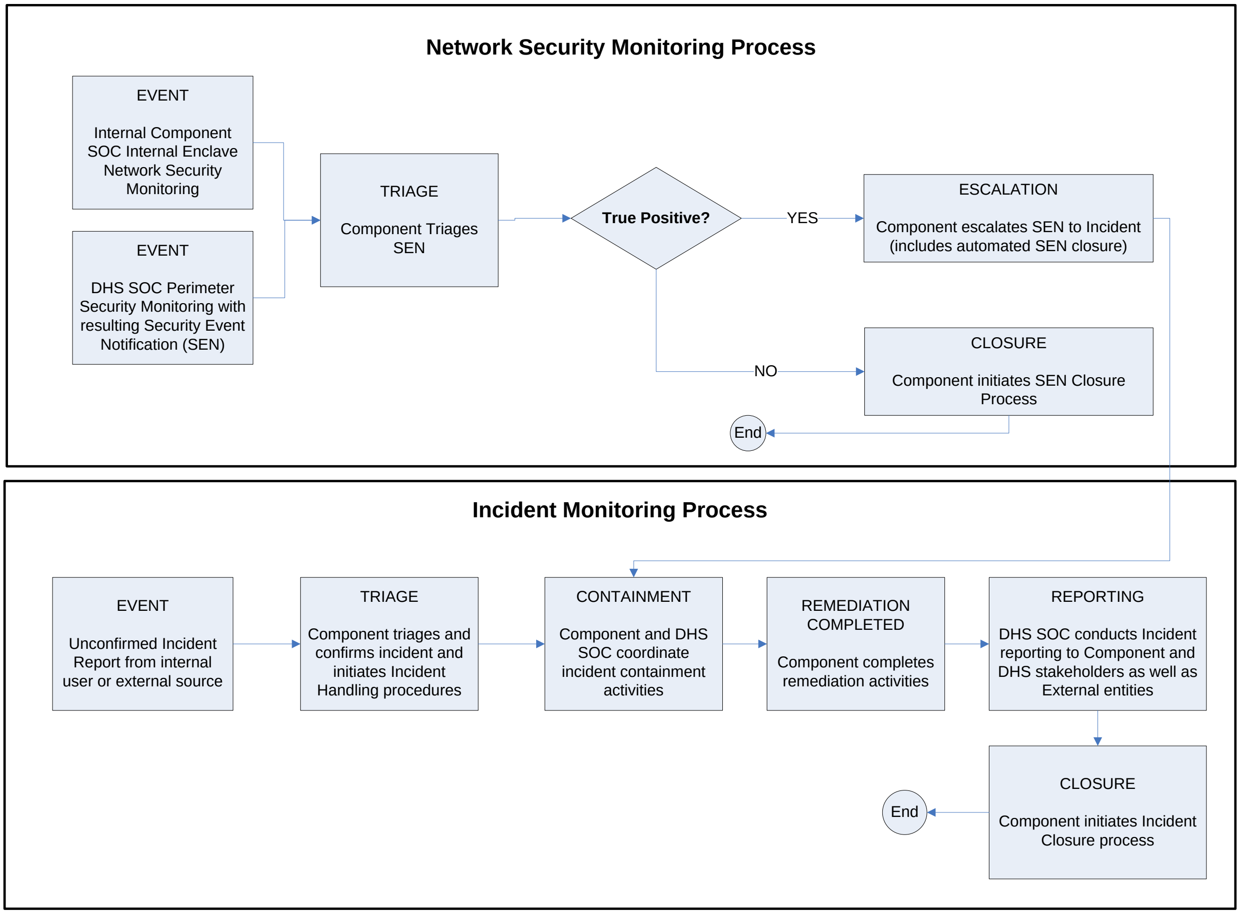
Network Security Monitoring Process
EVENT
Internal Component SOC Internal Enclave Network Security Monitoring
EVENT
DHS SOC Perimeter Security Monitoring with resulting Security Event Notification (SEN)
TRIAGE
Component Triages SEN
True Positive?
YES
NO
ESCALATION
Component escalates SEN to Incident (includes automated SEN closure)
CLOSURE
Component initiates SEN Closure Process
End
Incident Monitoring Process
EVENT
Unconfirmed Incident Report from internal user or external source
TRIAGE
Component triages and confirms incident and initiates Incident Handling procedures
CONTAINMENT
Component and DHS SOC coordinate incident containment activities
REMEDIATION COMPLETED
Component completes remediation activities
REPORTING
DHS SOC conducts Incident reporting to Component and DHS stakeholders as well as External entities
CLOSURE
Component initiates Incident Closure process
End

Figure 3: DHS Incident Response Life Cycle

3.4 Roles and Responsibilities for Incident Response

3.4.1 The DHS Chief Information Officer

The DHS CIO is the principal advocate for DHS computer security incident response activities and is the accreditation authority for the DHS ONENET SOC.

With respect to incident response, the DHS CIO has the following responsibilities:

- Ensure oversight and compliance with DHS policy.
- Establish a Department-level SOC.
- Ensure that all DHS Components maintain or are supported by a primary SOC capability.
- Establish partnering agreements with Federal incident response capabilities outside DHS.
- Establish partnering agreements for law enforcement support for security-related incidents.
- Act as sole authority for public release of security incident information.

3.4.2 DHS Chief Information Security Officer

With respect to incident response, the CISO has the following responsibilities:

- Oversee the SOC, including Government employees and contractor personnel.
- Serve as the primary interface between the DHS ONENET SOC and DHS management.
- Develop and maintain risk-based information security policies and procedures.
- Periodically test and evaluate the effectiveness of information security policies, procedures, and practices.
- Brief the DHS CIO and other senior management officials on significant incidents, providing the status of ongoing investigations and the outcomes of completed investigations.
- Distribute incident reports to the DHS CIO, DHS Component CIOs and DHS Component CISOs.
- Establish and maintain processes for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the Department's information security policies, procedures, and practices.
- Establish and implement tools and processes that support Component SOC policies and procedures that ensure timely reporting of security incidents.
- Develop and maintain incident response procedures and the policy supporting those procedures.
- Ensure that incidents are reported to US-CERT in accordance with federal regulations.
- Approve incident reports prior to their release to external Government entities including US-CERT.
- Approve deployment of SOC incident handling teams to Component locations.
- Ensure that Department employees and contractor personnel receive appropriate information security awareness training.

3.4.3 DHS Chief Security Officer

The DHS CSO is the Secretary's representative in matters related to security, and advises the Secretary on security-related issues that affect DHS personnel, property, facilities, and information.

The DHS CSO supports, guides, and coordinates with the DHS CISO to ensure that DHS IT systems are properly secured.

With respect to incident response, the DHS CSO has the following responsibilities:

- Notify, with advice from the CIO and the DHS ONENET SOC, the appropriate agency of any significant incident that requires law enforcement involvement.
- Coordinate, when criminal activity involving DHS IT infrastructure is suspected, with the DHS ONENET SOC, DHS CIO, DHS CISO, Component CIO, Component CISO, Component SOC, I&A, HSDN, and the Office of Inspector General (OIG) to:
- Isolate, secure, and preserve the state of any equipment suspected of being involved in a crime.
- Notify and coordinate with appropriate law enforcement organizations.
- Provide oversight and guidance to DHS ONENET SOC on incident handling activities relating to matters of national security (e.g., classified spills) and approve incident resolution and closure.

3.4.4 DHS Privacy Office

The DHS Privacy Office develops and oversees the implementation of DHS policies for safeguarding privacy in accordance with applicable Federal laws, regulations, and directives. The DHS Privacy Office establishes and maintains privacy requirements.

With respect to incident response, the DHS Privacy Office has the following responsibilities:

- Oversee management of privacy incidents.
- Provide privacy incident status reports to the DHS CIO as appropriate.
- Receive from Component Privacy Officers and PPOCs, and from the DHS ONENET SOC, reports on the handling of suspected or confirmed privacy incidents or incidents involving PII.
- Work with the DHS CIO and CISO, and Component CIOs and CISOs to prepare for release of information about information security incidents involving PII or other privacy issues.
- Provide oversight and guidance to the DHS ONENET SOC, Component Privacy Offices and PPOCs, and to Component SOCs for incident handling activities that are related to confirmed and suspected privacy incidents.

3.4.5 Component Chief Information Officer

Component CIOs are the principal advocates for their Components' computer security incident response activities.

With respect to incident response, Component CIOs have the following responsibilities:

- Establish a Component SOC to serve as primary incident response, investigation, and reporting capability for that Component.
- Develop and maintain Component SOC policies and procedures.
- Ensure use of DHS incident handling processes and procedures.
- Ensure compliance with DHS IT policies.
- Advise the DHS CIO of any issues regarding infrastructure protection and vulnerabilities, or that may cause public concern or loss of credibility.
- Ensure that incidents are reported to the DHS ONENET SOC within reporting time requirements.
- Work with the DHS CIO and Public Affairs Office to prepare for public release of security incident information. The DHS CIO or designated representative has sole responsibility for public release of security incident information.

3.4.6 Component Chief Information Security Officer

With respect to incident response, Component CISOs have the following responsibilities:

- Ensure that annual Incident Response training exercises and testing are conducted, coordinating them with the DHS CISO.
- Ensure that annual training includes rapid response, containment, and establishment and maintenance of chain of custody. In planning training, use the DHS ONENET SOC CONOPS and the guidelines in this Attachment as references.

- Coordinate closely with the IT support staff in response to confirmed incidents that require immediate establishment of containment and chain of custody.
- Work with the DHS PO, Component PO/PPOC, Component SOC, and Component CIO to prepare for release of computer security incident information that involves PII or other privacy issues.

3.4.7 Component Privacy Offices and Privacy Points of Contact

Component Privacy Officers and PPOCs are responsible for compliance at the Component level with Federal privacy law, directives, and regulations, and with DHS privacy policy.

With respect to incident response, Component POs and PPOCs have the following responsibilities:

- Receive and evaluate reports of suspected or confirmed privacy incidents that impact DHS.
- Coordinate with program managers, Component ISSMs and ISSOs, and the Component SOC in evaluating, mitigating, and reporting suspected or confirmed incidents involving PII.
- Inform the DHS Privacy Office of the status of ongoing and closed privacy incidents in a timely manner.
- Advise the DHS Privacy Office on handling of reported privacy Incidents.
- Provide privacy incident updates to the Component and DHS ONENET SOCs as information is obtained.
- Work with the DHS Privacy Office, the Component CIO, and the Component CISO in preparation for the release of information regarding computer security incidents involving PII or other privacy issues.
- Provide oversight and guidance to Component SOCs on incident handling activities relating to confirmed and suspected privacy incidents.

3.4.8 Users, System and Network Administrators, and Information Systems Security Officers

All users of DHS information systems, including system and network administrators and security officers, have the following responsibilities:

- Report incidents to Component SOCs immediately upon suspicion or recognition.
- Comply with Department incident response policy.
- Comply with Component-specific incident response policy.
- Support Component incident handling capability.

3.4.9 DHS Security Operation Center

- Review all reported incidents and verify that all pertinent information is recorded, confirmed, and that closure occurs only after all remediation and reporting activities have occurred in accordance with this SSPD 4300A.
- Focus 24x7 monitoring efforts on shared DHS infrastructure such as the Trusted Internet Connections (TIC), Policy Enforcement Points (PEP), E-mail Security Gateway (EMSG), Demilitarized Zones (DMZ), Virtual Private Networks (VPN) and other systems as required by DHS

CISOs to identify security events of interest that require confirmation, escalation, or declaration as a false positive.

- Create SENs based on monitoring and analysis activities when events of interest are identified that require further investigation.
- Provide oversight on investigational activities and review SENs prior to escalation. SENs will be escalated when Components have sufficiently demonstrated that adequate investigation has been performed and that the event is a verified incident. The Component must provide necessary information regarding the event in accordance with the escalation criteria outlined in Appendix F3, "Response Guidelines".
- Review all SENs for closure and close SENs after all reasonable investigational activities have been completed.
- Conduct operations and maintenance and approve changes on all security monitoring devices associated with shared DHS infrastructure (such as Intrusion Detection System (IDS), Data Loss Prevention (DLP)).
- Provide oversight and guidance for all incidents to ensure adherence to DHS Sensitive Systems Policy Directive 4300A.
- Serve as the primary clearinghouse and collection point for information related to incidents involving DHS systems or networks.
- Coordinate privacy and security incident handling activities with DHS entities such as the DHS Office of the Chief Security Officer and the DHS Privacy Office.
- Ensure that remediation and all necessary coordination activities are completed before incident closure.
- Analyze incidents, identifying and notifying other stakeholders and DHS Components that may be affected.
- Provide technical and investigative assistance to Components as needed.
- Provide accurate and timely reports to the DHS CISO on significant incidents and on the status of DHS enterprise computer security.
- Develop and maintain an incident database that contains information on all discovered and reported incidents.
- Provide automated incident notification and reporting to senior DHS and Component leadership and stakeholders such as the DHS Privacy Office and the DHS Office of the Chief Security Officer, as well as external reporting entities such as US-CERT.
- Update US-CERT on incident status as required.
- Facilitate communications between DHS Components for those incidents involving more than one Component (for example, Master incidents).
- Provide ad hoc incident trending reports as requested by the DHS CISO.

3.4.10 Component SOCs

- Focus security monitoring efforts on the Component network and systems.

- Compile and maintain a list of mission-critical systems, financial systems, and applications. The list will assist in determining the classification of the Component's systems, and in prioritization of security incidents.
- Component SOCs shall develop and publish internal computer security incident response plans and incident handling procedures, with copies provided to the DHS ONENET SOC upon request.
- Investigate SENS created by the DHS ONENET SOC and comply with reporting timelines and escalation criteria outlined in Appendix F3, "Response Guidelines" to either escalate the SEN or close it.
- Monitor internal network enclave traffic such as firewall logs, network IDS) and host-based security events (e.g. audit logs, host-based IDS/IPS).
- Request SEN escalation by the DHS ONENET SOC, within the reporting timeframes and meeting the escalation criteria outlined in Appendix F3, "Response Guidelines".
- Conduct SEN investigation and trace activity back to the originating host.
- Request closure when a SEN has been identified as inconclusive or as a false positive after providing adequate explanation of investigational activities via EOC Online.
- Respond to the DHS ONENET SOC on SEN investigation activities based on the escalation criteria in Appendix F3, "Response Guidelines".
- Ensure 24x7 incident handling function exists for the Component.
- Act as lead in the Component's incident handling and response activities, including identification, investigation, containment, eradication, and recovery.
- Coordinate incident response efforts, investigations, and reporting to the DHS ONENET SOC. Reporting should include all significant data such as the who, what, when, where, why and how of a given incident.
- Coordinate incident handling activities with internal Component entities such as the Component Office of Security, Component Privacy Office, and Internal Affairs.
- Coordinate Component-level remediation efforts as mandated by DHS security policies and communicate remediation activity to DHS ONENET SOC through EOC Online log entries.
- Share applicable information Department-wide or Component-wide. For example, by providing network and host-based indicators for malicious logic incidents, that will facilitate implementation of proactive measures to prevent future incidents.
- Provide updates to the DHS ONENET SOC for significant incidents whenever additional information becomes available.
- Provide system images, volatile memory images, and other malicious logic or intrusion related artifacts to the DHS OneNet SOC upon request.
- Request closure of incidents when Component remediation and mitigation actions have concluded.
- Assist other Components with technical or investigation assistance as requested by the DHS ONENET SOC.

3.4.11 HSDN SOC

- Respond to all incidents that are contained within HSDN (also known as “LAN B”).
- Document all HSDN incidents and report them to the HSDN Government Watch Officer and to DHS ONENET SOC via agreed-upon methods of communication.
- Collaborate with DHS ONENET SOC on any incident that crosses into the unclassified DHS network (also known as “LAN A”).

3.5 DHS Incident Response Capability Structure

Each DHS Component and Departmental Office must establish and maintain a SOC for a primary incident response capability, or develop a memorandum of agreement that will ensure this capability.

The DHS ONENET SOC is the focal point for computer security incident response activities and operates 24/7 as escalated support. All computer security incidents are reported to the SOC (through the Component SOC). External incident reporting to US-CERT is the responsibility of the DHS SOC.

3.6 DHS ONENET SOC Functions

The DHS ONENET SOC provides security incident handling services, including:

- **Off-site Support:** DHS ONENET SOC escalated support provides security incident management support including incident coordination, technical advice, and mitigation strategies as required.
- **On-site Support:** When requested by an affected Component, and where warranted, the DHS OneNet SOC participates in on-site incident handling efforts.
- **Advisories and Vulnerabilities:** DHS ONENET SOC is responsible for providing timely dissemination of security-related advisories and countermeasures to the Components SOCs.
- **Incident Reports:** DHS ONENET SOC is responsible for facilitating incident reporting to senior DHS and Component leadership and to US-CERT; for maintaining information on reported incidents; and for compiling both sanitized and unsanitized reports as directed.
- **Network Security Monitoring:** DHS ONENET SOC is responsible for proactive monitoring of shared DHS infrastructure such as the Trusted Internet Connection (TIC), Policy Enforcement Points (PEP), E-mail Security Gateway (EMSG) for anomalous activity indicative of a significant or minor incident.
- **Digital Media Analysis (DMA):** DHS ONENET SOC is responsible for providing forensic analysis capability of digital media in support of incident response activities for the Department as well as Components as needed.
- **Focused Operations (FO):** DHS ONENET SOC is responsible for supporting the DHS Cyber Threat Division (CTD) in detecting, preventing, and investigating advanced persistent threat activity.

3.7 Incident Reporting Process Flow

Incidents are identified by a number of methods resulting in different workflows. The overall incident handling process is shown in detail in Figure F-3. Incidents can be detected or reported in various ways:

- Reported by the Component SOC through the user community
- Detected by the Component SOC through internal Component enclave security monitoring activities

- Detected by the DHS ONENET SOC through monitoring activities of shared DHS infrastructure (e.g., TIC, PEP, EMSG)
- Reported from a trusted external entity such as US-CERT (usually via the DHS ONENET SOC)

User Reporting: User reporting occurs through a Component end-user, system administrator, or Information Systems Security Officer observing activity that violates the Components or DHS's security policy. Component-level reporting procedures are established by the Component. Component SOCs must triage and report all incidents to DHS ONENET SOC.

Component Detection: Component SOCs must monitor internal network enclave traffic (e.g. firewall logs, network IDS) and host-based security events (e.g. audit logs, host-based IDS/IPS). When identifying an event that is triaged and deemed likely to result in a security incident (reference Appendix F3, response guidelines for various categories), Component SOCs should track the investigation of the event using the EOC Online portal via the SEN process. Events can be triaged in the draft stage for SENs, triaging should be completed within 24 hours. If there is uncertainty, caution should prevail, and the Component should report the event/suspected incidents to DHS ONENET SOC via EOC Online. Once a SEN has been determined to be an actionable event, requiring remediation, Components are to escalate to an Incident and take necessary actions for closure.

DHS ONENET SOC Detection: DHS ONENET SOCs must monitor infrastructure such as the Trusted Internet Connection (TIC), Policy Enforcement Point (PEP), E-mail Security Gateway (EMSG), Demilitarized Zones (DMZ), Virtual Private Networks (VPN) and other devices as required by the DHS CISO's office.). When identifying an event that is triaged and deemed likely to result in a security incident (reference Appendix F3, response guidelines for various categories), DHS ONENET SOC must track the investigation of the event using the EOC Online security portal via the SEN process, assign it to the applicable Component(s). Events are triaged in the draft stage for SENs by DHS ONENET SOC and the triage process should be completed within 24 hours. Once a SEN has been determined to be an actionable event, requiring remediation, Components are to escalate to an Incident and take necessary actions for closure.

External entity reporting: An external source such as a private citizen, a news report, or another government agency, may be the first notification of an incident. In this case, a SEN must be created by DHS ONENET SOC as the primary notification mechanism to the Component. These SENs can be escalated to incidents upon confirmation.

Note: Timeframes for all incident reporting to the DHS ONENET SOC and escalation criteria are outlined in Appendix F3, "Response Guidelines". All incidents must be reported to Component and DHS ONENET SOC, even those that have been resolved prior to reporting.

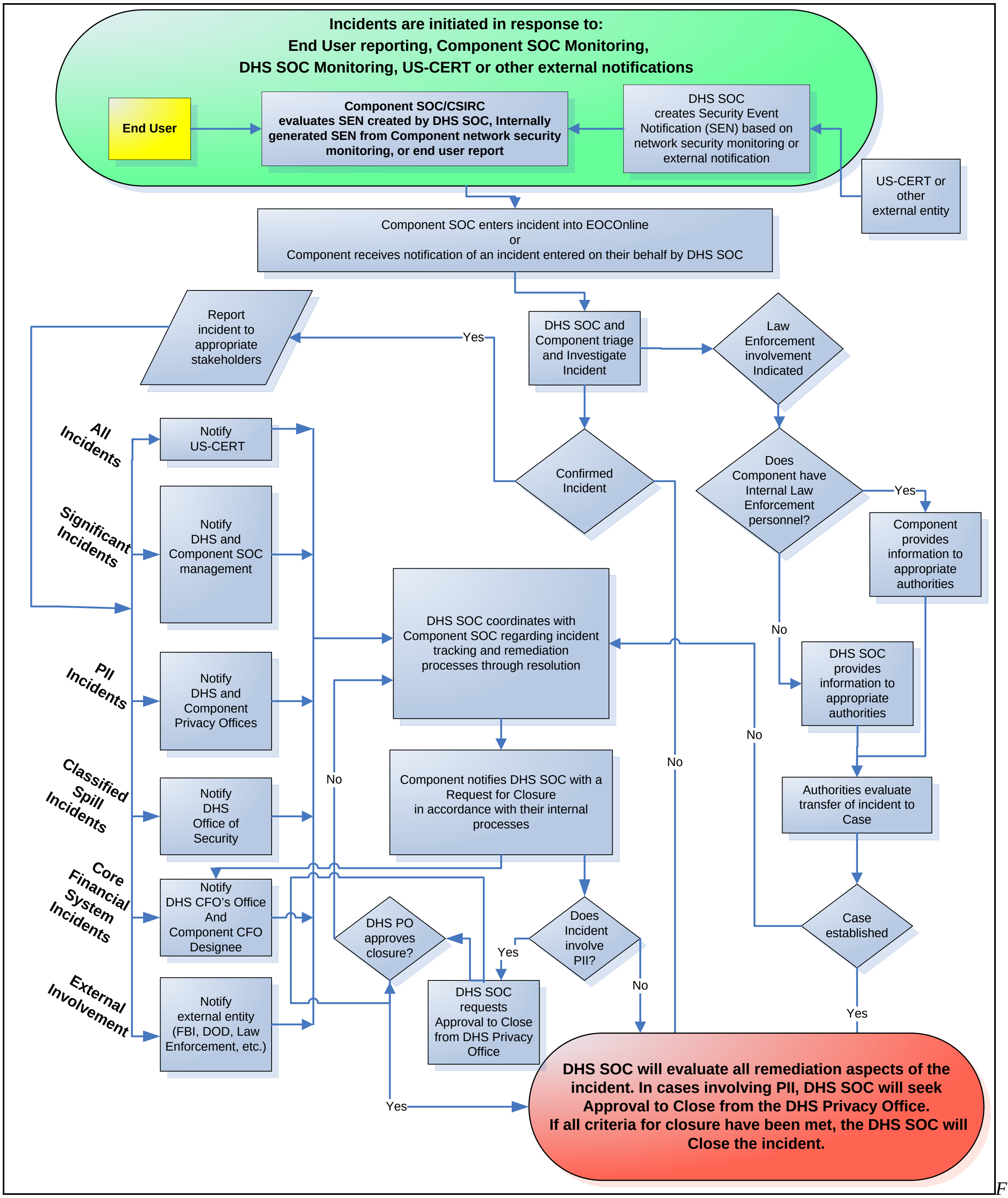
Incidents are initiated in response to:
End User reporting, Component SOC Monitoring,
DHS SOC Monitoring, US-CERT or other external notifications
End User
Component SOC/CSIRC evaluates SEN created by DHS SOC, Internally generated SEN from Component network security monitoring, or end user report
DHS SOC creates Security Event Notification (SEN) based on network security monitoring or external notification
US-CERT or other external entity
Component SOC enters incident into EOCOnline or Component receives notification of an incident entered on their behalf by DHS SOC
Report incident to appropriate stakeholders
Yes
DHS SOC and Component triage and Investigate Incident
Law Enforcement involvement Indicated
All Incidents
Notify US-CERT
Confirmed Incident
Does Component have Internal Law Enforcement personnel?
Yes
Component provides information to appropriate authorities
Significant Incidents
Notify DHS and Component SOC management
DHS SOC coordinates with Component SOC regarding incident tracking and remediation processes through resolution
No
DHS SOC provides information to appropriate authorities
PII Incidents
Notify DHS and Component Privacy Offices
No
Component notifies DHS SOC with a Request for Closure in accordance with their internal processes
No
No
Authorities evaluate transfer of incident to Case
Classified Spill Incidents
Notify DHS Office of Security
Core Financial System Incidents
Notify DHS CFO's Office And Component CFO Designee
DHS PO approves closure?
Does Incident involve PII?
Yes
Case established
No
External Involvement
Notify external entity (FBI, DOD, Law Enforcement, etc.)
DHS SOC requests Approval to Close from DHS Privacy Office
Yes
Yes
DHS SOC will evaluate all remediation aspects of the incident. In cases involving PII, DHS SOC will seek Approval to Close from the DHS Privacy Office.
If all criteria for closure have been met, the DHS SOC will Close the incident.

Figure 4: Functional diagram of DHS Incident Response

3.7.1 Component-level Security Operations Center

Each Component SOC will compile and maintain a list of mission-critical systems, financial systems, and applications. The list will assist in determining the classification of the Component's systems, the prioritization of security and financial incidents

Component SOCs provide primary security monitoring, incident response, and vulnerability management for the Component information assets. The SOCs administer, monitor, respond to, and report on security events, and incidents that involve networks or devices in their watch areas.

DHS Sensitive Systems Policy Directive 4300A requires Components to develop and publish internal computer security incident response plans and incident handling procedures. Copies of these plans and procedures are furnished to to the DHS ONENET SOC upon request.

DHS Component SOCs act as intake centers for receiving Component-level incident reports and are capable of identifying many incidents. The Component SOC performs an initial investigation and determines whether or not the event is a security or privacy incident. If the event is not a computer security or privacy incident, the Component manages the event according to its internal procedures for events that are not validated as incidents and notifies DHS ONENET SOC through EOC Online. If the event is a computer security or privacy incident, the DHS Incident Handling Checklist in Appendix F7 may be used to assist in incident management.

When any Component detects within its monitoring scope an event that has high probability of being an incident, the Component must create a SEN and enter it in EOC Online to initiate tracking during Component SOC triage and investigation of the event. A SEN may also be entered on behalf of a Component by the DHS ONENET SOC. The Component must investigate any SEN within its monitoring scope.

During its investigation, the Component must enter updates to EOC Online, reporting all relevant information discovered. If there is uncertainty, caution should prevail, and the Component should report the event to DHS ONENET SOC via the EOC Online portal at https://eoconline.dhs.gov, accessible only via the DHS Intranet. The overall incident handling process is shown in detail in Figure 4.

When SENS are created by the DHS ONENET SOC, Component SOCs will investigate within their monitoring scope and report their findings in EOC Online.

SEN levels, and the criteria for each, are given in Table 1.

SEN Level	Criteria
INFORMATIONAL	Informational Security Event Notifications (SENs) are derived from security alerts which may or may not pose a threat to the Component infrastructure and situational awareness.
LOW	Low Security Event Notifications (SENs) are derived from security alerts that pose little threat to the Component Infrastructure and may be categorized as such if they are outbound alerts or if the target system is not susceptible to the attack.
MODERATE	Moderate Security Event Notifications (SENs) are derived from security alerts that could pose a moderate threat to the Component Infrastructure. These may include suspected malicious activity aimed at Component non-critical systems or targeted fingerprinting activities. With the exception of a confirmed infection, all other malware events should be considered “suspected” as opposed to “confirmed” and will fall within this category.
CRITICAL	Critical Security Event Notifications (SENs) are derived from security alerts that could pose an immediate threat to the Component Infrastructure. These may include confirmed DoS attacks; suspected malicious activity aimed at a CBP critical system, or confirmed successful malicious activity to or from a Component system. With the exception of a confirmed infection via Symantec or Focused Operations (FO), all other malware events should be considered “suspected” as opposed to “confirmed” and will fall within this category.

Table 1: The criteria for each SEN level

Functional responsibilities and reporting requirements (with required timeframes, are given in Table 2.

Functional Responsibilities of DHS ONENET SOC and Component SOC		
Responsibility	**DHS ONENET SOC**	**Component SOC**
Monitoring and Analysis	• Focus 24x7 monitoring efforts on the DHS TIC, PEPs, the EMSG, DMZ, VPN, and legacy DHS OneNet architecture to identify security events of interest requiring confirmation, escalation, or declaration of false positive. • Create and provide SENs to Components when events of interest are identified. • Provide oversight on investigational activities. • Review all SENs for closure. • Escalate SENs to incidents if required, or close SEN.	• Focus 24/7 monitoring efforts on Component network. • Administer and monitor security tools on Component network. • Conduct SEN investigation and traceback to host. • Escalate SENs to incidents upon confirmation of SEN. • Request closure when a SEN has been identified as inconclusive or as a false positive, after providing adequate explanation of investigational activities within EOC Online.
		Reporting Requirements per SEN Level: INFORMATIONAL • No response required. LOW • Acknowledge receipt within 24 hours. • Respond with investigational activities within one week. • Provide updates weekly until SEN can be closed or escalated to an incident until SEN can be closed or escalated to an incident. MODERATE • Acknowledge receipt within 8 hours. • Respond with investigational activities within 24 hours. • Provide updates every 72 hours CRITICAL • Acknowledge receipt and respond with investigational activities within one hour. • Provide updates every 24 hours until SEN can be closed or escalated to an incident until SEN can be closed or escalated to an incident.

Functional Responsibilities of DHS ONENET SOC and Component SOC		
Responsibility	**DHS ONENET SOC**	**Component SOC**
Incident Response and Investigation Assistance	• Provide oversight and guidance for all incidents to ensure adherence to DHS Sensitive Systems Policy Directive 4300A. • Coordinate privacy and security incident handling activities with DHS entities such as the DHS Office of Security and DHS Privacy Office. • Ensure remediation and all necessary coordination activities are complete before incident closure. • Provide technical and investigative assistance to Components, as needed. • Develop and maintain an incident database that contains information on all discovered and reported incidents. • Provide automated incident notification and reporting to external reporting entities, US-CERT, the DHS Privacy Office, and the DHS Office of Security. • Update US-CERT on incident status as required. • Facilitate communications between DHS Components for those incidents involving more than one Component (i.e., Master incidents)	• Ensure 24x7 Incident Handling function exists for Component. • Act as lead for incident handling and response activities within Component including identification, investigation, containment, eradication, and recovery. • Report all pertinent incident information and updates in a timely manner to DHS ONENET SOC. • Coordinate incident handling activities with internal Component entities such as the Component Office of Security, Component Privacy Office, and Internal Affairs. • Coordinate Component-level remediation efforts as mandated by DHS security policies and communicate activity to DHS ONENET SOC through EOC Online log entries. • Share applicable information to facilitate the implementation of proactive measures to prevent future incidents Department-wide or Component-wide (e.g.,. provide network and host-based indicators for Malicious Logic incidents). • Request closure of incidents when Component remediation and mitigation actions have concluded. • Assist other Components with technical or investigation assistance as requested by the DHS ONENET SOC.
Security Awareness	• Provide an incident response framework and make incident response SOP available to support Components' training efforts as requested. • Provide input as necessary to Component-level capability training. • Identify new training topics and subjects for augmentation of Component-level training.	• Provide internal training at the Component level for system administrators and security officers on Component-level capability procedures and topics. • Adapt training to reflect the evolving and changing nature of threats and incident response.

Table 2: Functional responsibilities of the DHS ONENET SOC and of Component SOCCs

A Component SOC will initiate incident evaluation processes in accordance with its incident response plan. The Component SOC reports incidents to the DHS ONENET SOC in accordance with the Component's incident response plan via the DHS OneNet SOC portal (https://eoconline.dhs.gov). Components report incidents only to the DHS ONENET SOC, and not to any other agency. For events involving devices on other local area networks (LAN), the Component will be responsible for notifying all Component stakeholders and the DHS ONENET SOC.

Each Component SOC shall have the ability to respond 24/7. Each Component will maintain an accurate list of its key POCs and provide the list to the DHS ONENET SOC. POC changes will be reported as soon as possible. Specific responsibilities are outlined in Table 2.

Component SOCs shall catalog their component's capabilities (e.g., forensic, malware, analytical) so that these resources can be employed in response to a national-level cyber incident. Incident response personnel shall have security clearances equal to the classification level of the information they are working with.

Responsibilities of the DHS ONENET SOC and Component SOCs for each function are given in Table 2.

3.7.1 Involvement of Law Enforcement in Incident Response

Law enforcement organizations include the DHS Office of the DHS Inspector General, Internal Affairs, Management Investigations and Integrity Assurance, the U.S. Secret Service, Immigrations and Customs Enforcement, and other Federal, state, and local law enforcement agencies.

Components should contact law enforcement agencies directly only after obtaining guidance from the DHS ONENET SOC, except in emergencies when time is critical to saving lives or protecting property. When a Component does contacts law enforcement, the DHS ONENET SOC will be notified as soon as possible by the best means available. In the event of a significant incident (as defined in Appendix F3), Components shall defer to the DHS CSO in contacting law enforcement, except that in extreme emergency cases where time is critical to saving lives or protecting property,. In such emergencies, Components may notify law enforcement agencies in accordance with their internal procedures.

In all cases of local or external law enforcement contact, Components must notify the DHS ONENET SOC and the DHS CSO. The DHS ONENET SOC and the Component SOC will coordinate with law enforcement organizations to determine the appropriate response.

Components shall defer to the DHS Privacy Office and the Component privacy office or PPOC for law enforcement involvement in privacy incidents not related to IT.

3.8 Accessibility and Incident Reporting Timelines

This section provides guidance to DHS Components, Data Centers, and DHS Headquarters for responding to and reporting security incidents that affect DHS mission activities. DHS Contact information is provided in Appendix F-2. Incident reporting timelines are specified in Appendix F-3. The DHS ONENET SOC shall issue procedures and timelines for incident reporting throughout DHS.

3.8.1 Significant Incident Reporting

Components shall report *significant incidents*, when suspected or confirmed, to the DHS ONENET SOC at the EOC Online portal at https://Eoconline.dhs.gov or by email (DHS.SOC@dhs.gov), in accordance with the timeframe given in Table F-2. When neither EOC Online nor DHS.SOC@dhs.gov is available, reporting by telephone (1-877-347-1638) is acceptable. The Component is responsible for verifying that reports are received and acknowledged by the DHS ONENET SOC for incidents requiring immediate response.

Significant Homeland Secure Data Network (HSDN) incidents will be documented with a preliminary report that will be provided within one hour to the HSDN Government Watch Officer (GWO). Refer to *DHS 4300B National Security Systems Handbook*, Attachment H, "POA&M Process Guide," Section 3.0 for guidance. All reports regarding classified incidents that are handled on the FOUO network must exclude classified information.

3.8.2 Minor Incident Reporting

Components shall report minor incidents in accordance with the timeframe given in Table 2 unless other critical information is available that may be used for enhancing the security posture of the Department is available (e.g, IPs or domains that are not currently blocked). Incidents involving Sensitive But Unclassified (SBU) systems may be reported via the https://eoconline.dhs.gov.

The DHS HSDN SOC and the DHS ONENET SOC are separate entities that cooperate closely in response to incidents of classified information spillage and share threat intelligence.

3.8.3 Reporting to the U.S. Computer Emergency Readiness Team

US-CERT is designated as the Federal organization to which information security incidents are reported, and serves as the central repository for Federal incident data. The DHS ONENET SOC reports security incidents to US-CERT, which subsequently notifies other organizations appropriate to the situation; the organizations notified may include law enforcement agencies, the Social Security Administration, private sector POCs, and the Executive Office of the President as appropriate.

The DHS ONENET SOC will facilitate automated notification to US-CERT and designated DHS and Component management personnel within the timeframe given in Table F-2 for significant incident reports.

Suspected or confirmed privacy incidents and incidents involving PII that include information security aspects will be initially reported by the DHS ONENET SOC to US-CERT. All updates, follow-up, and closeout with US-CERT will be performed by the DHS ONENET SOC with the cooperation of appropriate privacy officials.

3.8.4 Privacy Incident Reporting

The DHS Privacy Office, in its publication "How to Safeguard Personally Identifiable Information," defines ***personally identifiable information (PII)*** as,

"Any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the employee, or contractor to the Department. S**ensitive PII** is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data is compromised."

Some categories of PII are sensitive as stand-alone data elements. Examples include: Social Security number (SSN), driver's license or state identification number, passport number, Alien Registration Number (A-Number), or financial account number. Other data elements such as a citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII."

Privacy incidents and incidents that may involve PII are subject to particularly strict reporting standards and timelines.

Any Component that discovers a suspected or confirmed incident must coordinate with its Privacy Office when evaluating and subsequently reporting the incident to the DHS ONENET SOC.

Component SOCs must report all incidents that possibly involve PII to the DHS ONENET SOC as soon as possible after discovery, in accordance with the timeframe given in Table 2.

All Component personnel (i.e., Federal employees, independent consultants, government contractors and others using, or with access to, DHS information resources) must immediately report suspected or confirmed privacy incidents or incidents involving PII to their Program Manager regardless of the manner in which the incident might have occurred or whether the PII was in electronic or physical form.

The DHS ONENET SOC treats all incidents that possibly involve PII as privacy incidents until such time as the DHS Privacy Office (DHS PO) determine otherwise. DHS personnel must refer to the Privacy Incident Handling Guidance for further instruction on handling requirements and procedures.

For additional information on the handling of incidents involving PII, refer to the *DHS Privacy Incident Handling Guidance*, v3.0, January 26, 2012.

PII disclosed through classified spillage should NOT be reported to US-CERT by the DHS ONENET SOC, but will be handled instead in accordance with Section 3.9.3 of this document.

Under no circumstances should Component SOCs report privacy incidents directly to US-CERT. Component Privacy Offices or PPOCs may submit reports or follow-up on previous reports under the guidelines established by the DHS Privacy Office.

3.9 Incident Priority Levels

When handling an incident, the DHS ONENET SOC, with assistance of the Component's SOC, determines the impact of the incident on the Component or DHS computing environment and assigns an Incident Priority Level (see Table F-2). Priority 1 is the highest level; Priority 5 the lowest. If multiple incidents occur simultaneously, each incident is addressed in accordance with its own priority level.

Priority Level	Definition
Priority 1	Protect human life and safety. Human life always has precedence over all other considerations.
Priority 2	Protect classified data as regulated by Government statutes and regulations.
Priority 3	Protect sensitive data, including proprietary, financial, law enforcement, scientific, and managerial data. This includes critical infrastructure protection assets.
Priority 4	Prevent system damage (e.g., the loss or alteration of system files, damage to hard drives).
Priority 5	Minimize disruption of computing resources.

Table 3: Incident priority levels

4.0 Computer Security Incident Reporting Requirements

This section outlines incident reporting requirements for the DHS and Component SOCs.

4.1 DHS ONENET SOC Computer Security Incident Reporting Requirements

The DHS ONENET SOC serves as the escalated reporting function and serves as interface with external organizations.

4.1.1 Individual Incident Reports

Incidents are designated by the DHS ONENET SOC based on detection from network security monitoring activities (and possibly from SEN escalation), from media reports (as applicable to DHS), or from Component reports. Component level users should notify their Component SOC of an incident as directed within their Component security policies. A user that feels compelled to do so may contact DHS ONENET SOC directly. The Component SOC notifies the DHS ONENET SOC immediately after confirming that an event is an incident. The DHS ONENET SOC, in accordance with its SOP, notifies senior DHS leadership whenever a significant incident has been reported and confirmed. Upon incident confirmation, the Component must provide via EOC Online **(**https://eoconline.dhs.gov**)** a thorough explanation of the incident, how it took place, the impact, and actions taken in response. Communications and data storage used must be protected to a level commensurate with the security incident's classification or sensitivity. For all incidents, resolution details are documented in EOC Online.

4.1.2 Daily and Weekly Reports

The DHS ONENET SOC will compile a summary report of each day's activities and post the reports on https://Eoconline.dhs.gov, Monday through Friday. Weekend and holiday reports will be posted on the next regular Department workday. Reports to Internal and External Entities

The DHS ONENET SOC is the central POC for coordinating all incident response and reporting within DHS and between DHS Components and US-CERT. In case of classified incidents, DHS ONENET SOC may reach out to external entities to ensure cleanup efforts occur quickly. In all other cases, US-CERT should be the primary POC for coordinating incident response activities with external entities.

4.1.2.1 United States Computer Emergency Readiness Team

Suspected or confirmed privacy incidents and incidents involving PII that include information security aspects will be initially reported by the DHS ONENET SOC to US-CERT. All updates, follow-up, and closeout with US-CERT will be performed by the DHS ONENET SOC with the cooperation of appropriate privacy officials.

4.1.2.2 Law Enforcement

Under the direction of the DHS CISO, the DHS ONENET SOC coordinates law enforcement involvement for DHS computer security incidents. Enforcement organizations that may be involved include OIG, DHS Internal Affairs, USSS, ICE, as well as other Federal, state, and local agencies.

The DHS CSO, with advice from the CIO and the DHS ONENET SOC, will notify the appropriate agency of any incident that requires law enforcement involvement or designate the appropriate entity within DHS to do so. Components may contact state, local, or tribal law enforcement agencies directly, but not before obtaining guidance from the DHS ONENET SOC, except during emergencies, when time is critical to saving lives or protecting property. In these exceptional cases, the Component will notify the DHS ONENET SOC as soon as possible by the most expedient means available.

SOCs of Components that have an internal law enforcement capability may report applicable incidents to their internal law enforcement at the Component leadership's discretion. In all cases, Components must notify the DHS ONENET SOC as required in Section 3.3. Law enforcement organizations will coordinate with the DHS ONENET SOC and with the Component to determine the appropriate response.

4.1.2.3 Homeland Secure Data Network SOC

HSDN is standalone classified network, capable of rapidly exchanging data that is classified up to the Secret level. The network provides secure, real-time connectivity in a collaborative environment to collect and disseminate classified information between appropriately cleared Federal, State, and local personnel.

The HSDN SOC was established to provide security oversight to the HSDN infrastructure, to monitor and manage security devices and applications, to conduct analysis, and to respond to HSDN events and incidents.

The HSDN SOC continuously monitors all security related events on the HSDN. When an event is confirmed to be an incident, the HSDN SOC will notify the HSDN Computer Incident Response Team (CIRT), the HSDN ISSM, the HSDN Security Manager, and the DHS CISO. The DHS ONENET SOC will be notified at the discretion of the DHS CISO for incidents that may pertain to the FOUO network.

The HSDN SOC and the DHS ONENET SOC share information and collaborate when appropriate, for example in cases of classified information spillage. Incidents occurring on the HSDN are reported according to HSDN SOC guidance. DHS ONENET SOC will notify the HSDN SOC GWO and main email address of any classified spill occurring at DHS. The information provided will not contain any classified information, only relevant data pertinent to the classified spill.

HSDN CONTACT INFORMATION
Help Desk 1-877-457-4736 (1-877-HLP-HSDN)
HSDN E-mail: Unclassified hsdn.helpdesk@ngc.com hsdnsoc@ngc.com
HSDN E-mail: Classified hsdn.helpdesk@dhs.sgov.gov hsdngwo@dhs.sgov.gov hsdnsoc@dhs.sgov.gov

Table 4: HSDN contact information

More detailed information and requirements for the HSDN SOC are outlined in the Homeland Secure Data Network Security Plan, the Incident Response Plan for Homeland Secure Data Network (HSDN), and the DHS ONENET SOC SOP.

4.2 Component SOC Reporting Requirements

The Component SOCs are the primary POC for incident reporting by Component system administrators, network administrators, security officers, and component personnel. Component SOCs are responsible for reporting each incident to the DHS ONENET SOC in the timeframes given in Table 2.

4.2.1 DHS Privacy Office

Reporting privacy incidents and incidents that may involve PII are special cases subject to strict reporting standards and timelines, and are reported as standard security incidents that are "PII-related" or "suspected PII-related". Using the built-in notification mechanisms in the EOC Online portal (https://Eoconline.dhs.gov), Component SOCs and Privacy Offices/PPOCs, the DHS Privacy Office, DHS and Component senior leadership, and US-CERT are notified.

The DHS ONENET SOC treats any incident that possibly involves PII as a privacy incident until instructed otherwise by the DHS Privacy Office.

Suspected or confirmed privacy incidents and incidents involving PII that include computer security aspects will be initially reported by the DHS ONENET SOC to US-CERT. Incidents that include both privacy (whether paper or electronic) and computer aspects will be updated, followed up, and closed out by the DHS ONENET SOC, in cooperation with the appropriate privacy officials.

4.3 Incident Reporting Guidelines for Component SOCs

Component SOCs should provide accurate and complete information at the time of reporting and continue with updates as additional information becomes available. The following must be determined for each incident:

- Incident Type
- Names of system(s) involved (spell out each acronym used at its first use)
- Number of affected hosts

- FIPS 199 categorization of system(s) involved
- Type of data involved (FOUO, PII, Law Enforcement Sensitive (LES), Sensitive Security Information (SSI), Secret, Top Secret)
- Functional use of systems involved
- Identified or suspected cause of incident
- Identified or suspected impact of incident
- Investigation, containment, and remediation steps taken
- Incident detection/identification method
- Parties involved (include descriptive titles and names if required for remediation)
- Date and timeframe of occurrence(s)
- If applicable, provide:
    - Host-based indicators, Network indicators, and Email characteristics
    - Security controls that blocked and/or detected the activity
    - Date/time the activity was blocked and/or detected
    - Host operating systems
    - Name of malicious logic
    - Actions taken by affected system
    - Network activity observed (including IPs and URLs connections made or attempted, associated ports)
    - Type of unauthorized access attempted or obtained (including capabilities associated with that type of access)
    - Method of dissemination for classified data
    - Attack vector or source of compromise
- For incidents involving privacy or PII, also include:
    - The number of individuals
    - The number of records
    - The number of data points

4.3.1 Incidents Involving Critical Information Assets

Component SOCs must take additional precautions when reporting incidents involving critical information assets. Each Component is responsible for maintaining a list of critical systems and critical information assets, which will be used when categorizing incidents. Significant incidents involving a system with a FIPS 199 categorization of ***High*** will be reported immediately to the DHS ONENET SOC and should be clearly identified as such at the time of report.

4.3.2 Incidents Involving CFO-designated Systems

Incidents involving CFO-designated systems will be reported immediately to the DHS ONENET SOC and to the DHS Chief Financial Officer (CFO). If the incidents reported involve criminal activity, the DHS ONENET SOC will pass the financial crimes information to the USSS and to US-CERT

5.0 INCIDENT HANDLING STAGES FOR COMPONENT SOCS

Typically, incident handling has the six stages described in this section. A more detailed understanding of the sequence of events will be gained from the DHS Incident Handling Checklist in Appendix F8).

The Component SOC serves as the primary incident handling capability within that Component, assisting the reporting party, the system administrator, network administrator, security officer, and users. The Component SOC reports all incidents to the DHS ONENET SOC, and can request off-site or on-site assistance in handling an incident from the DHS ONENET SOC.

For information on handling incidents involving PII, refer to *DHS Privacy Incident Handling Guidance*, v3.0, January 26, 2012. (http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf)

5.1 Definitions of the Six Incident Handling Stages

Preparation: Establish an approach to incident handling that includes development of policy and procedures, and identification of Components involved in the response effort.

Identification: Analyze detection devices (for example, intrusion detection systems (IDS), firewalls, and audit logs) to identify signs of an incident; notify appropriate officials of an incident; and begin handling the evidence to ensure a verifiable chain of custody.

Containment: Ensure that the impact of the incident does not increase.

Eradication: Determine the cause and remove it.

Recovery: Restore the system to its original state and validate the clean system.

Follow-up: Develop follow-up reports, identify lessons learned, and update procedures as necessary.

The Component SOC's role in each of the six incident handling stages is described below.

5.1.1 Preparation

The Component SOC develops and maintains a foundation to support incident response capability. Preparation activities include the following:

Developing the Component's security policy and incident response procedures.

Identifying and assigning supporting roles and responsibilities.

Establishing and implementing processes and procedures to ensure timely reporting of security incidents; development of appropriate documentation; procedures to maintain the chain of custody.

Establishing a monitoring capability with appropriate scope including all Component networked-assets.

5.1.2 Identification

In the incident identification stage, the Component SOC first coordinates with appropriate entities to identify what has occurred and the possible causes. Once it has been confirmed that a security incident has occurred, the SOC team determines what type of security incident occurred and how many systems were affected. At this point, the Component SOC must notify the DHS ONENET SOC and may request assistance in the containment, eradication, and recovery stages.

5.1.3 Containment

Once the incident has been identified, the Component SOC determines the risk of continuing to operate the affected system(s) and coordinates containment activities. Containment activities may include:

- Coordinating blocking activities with appropriate entities, if applicable
- Performing a full image backup onto unused media and safely storing it for law enforcement officials
- Making a second full image backup, if possible, for comparison purposes
- Keeping all incident handlers informed and advising the system owners of progress
- Gathering pertinent logs for review
- Changing passwords on the compromised systems and on all systems that interact with the compromised systems
- Removing a system from the network if the Component SOC or DHS ONENET SOC deems the system to be harmful to the DHS enterprise network
- Blocking or requesting blocking of a known bad IP, Uniform Resource Locator (URL), email address, etc.
- Disabling an affected user account

5.1.4 Eradication

The Component SOC must help the reporting party evaluate the symptoms and the cause of the incident. If the cause cannot be determined, a best guess should be made based on the evidence at hand and included with the initial report. The condition that was exploited that resulted in the incident must be corrected, and the most recent clean backup must be located. Action must be taken to ensure that the negative impact of the incident is no longer a threat to the DHS network. Steps associated with eradication may include:

Deleting emails as a means of containment of a disclosure or of malicious logic.

Re-imaging infected systems.

5.1.5 Recovery

Once the system is again performing normally, it must be tested and validated before it can be brought back on line in a production network. Meticulous care should be taken to ensure that restore back doors or malicious code are not restored. For example, if a root kit installation is suspected, the system should be reformatted and the operating system rebuilt, including all patches and fixes, before the system is redeployed. These changes could destroy evidence, so if the incident is being investigated by law enforcement, it is necessary that the investigator concur before changes of this nature are made. Applications and data should then be reloaded on the fresh operating system.

5.1.6 Follow-Up

The Component SOC provides a follow-up report to the DHS ONENET SOC as soon as possible to ensure a full and accurate account of all details. The Component SOC should modify policies and procedures to prevent similar incidents from occurring, if applicable.

5.1.7 Escalating the Priority of Incidents

Initial incident priority may change as more information becomes available. If an incident changes in status or character, the Component SOC incident handler in charge must update the incident report to the SOC and inform incident handling team so that the appropriate level of attention can be given to the incident.

5.2 DHS SOC Services

When a Component requests, the DHS ONENET SOC will assist the Component SOCs in the incident handling process; if the Component requests on-site support, the DHS CISO must give approval before the DHS ONENET SOC dispatches personnel to the site.

5.2.1 Gathering Information

Once it has been determined that a security incident has occurred, the DHS ONENET SOC, in collaboration with the Component SOC, gathers as much information as possible. If there is any chance that the incident may involve law enforcement, a verifiable chain of custody must be maintained. Upon request from the Component SOC or at the direction of the DHS CISO, the DHS ONENET SOC can perform log review and analysis on behalf of the Component SOC.

5.2.2 On-site DHS ONENET SOC Support of Incident Handling

When a Component SOC asks for on-site assistance, the DHS ONENET SOC will evaluate the request and provide assistance if deemed necessary and will coordinate on-site assistance visits and forwarding visitor requests to the Components. The DHS ONENET SOC shall assist Component SOCs with incident handling. On-site support responsibilities for the DHS SOC incident handler may include the following:

- Documenting the incident
- Acting as liaison between the Component SOC and the DHS ONENET SOC
- Ensuring Department incident handling guidelines and "best practices" are followed
- Containing damage
- Creating, if possible, backups of the affected systems
- Helping the Component resume business

To prevent duplication of effort, the on-site DHS ONENET SOC incident handler must ensure that only one individual is in charge and that each team member reports to that person. Typically, the Component SOC is in charge of incident handling within the Component, with the SOC's on-site team assisting. The SOC incident handling team is responsible for providing reports to the SOC as each phase is completed, once a day; as each phase is completed; or when there is a significant change in the incident status. The DHS ONENET SOC also provides updates to the DHS CISO.

5.2.3 Forensic Services - Digital Media Analysis

Using purpose-designed software, the DHS ONENET SOC provides forensic services Digital Media Analysis (DMA) as part of its charter to all DHS Components and program areas. These services assist in performing detailed incident analysis. Costs for local image capture shall be the sole responsibility of the Component.

DMA provided by the DHS ONENET SOC is not intended for law enforcement or to be court-admissible. The DHS ONENET SOC can coordinate such services with appropriate agencies. In the event that law enforcement services are required, the DHS ONENET SOC makes initial contact with the DHS Office of the Chief Security Officer, and with OIG, ICE, USSS, and other DHS enforcement organizations to establish evidentiary chain of custody. DMA shall have adequate resources to accomplish its primary mission, including:

Dedicated evidence storage and analysis facilities with physical access limited to authorized forensics team personnel.

Mobile evidence gathering tools required to establish chain of custody; to collect and label evidence at incident sites; and to securely package and transport the collected evidence.

The DMA Team shall:

Develop, maintain, and follow SOP for computer forensics collection and analysis.

Support and coordinate with appropriate DHS organizations, including but not limited to: the DHS ONENET SOC, CIO, CISO, OIG, and Component SOCs.

As directed by the DHS ONENET SOC, coordinate with law enforcement as appropriate.

Report the results of computer forensics activities to the DHS ONENET SOC and other appropriate parties.

Follow DHS disclosure and privacy guidance.

Maintain a chain of custody of evidence.

5.2.4 Deployment Considerations

When advanced incident analysis capabilities are required, or when criminal activity involving the DHS IT infrastructure is suspected, the DHS ONENET SOC will coordinate with the DHS CISO, CIO, CSO, HSDN, and the Office of Inspector General, and Component SOCs to:

Access the digital media associated with the incident;

Isolate, secure, and preserve the state of any equipment suspected of being involved in a crime;

Coordinate with appropriate law enforcement organizations; and

If necessary, package and ship equipment to a designated computer forensic processing facility.

If it is determined that the source of the suspected criminal activity is external to DHS, the appropriate law enforcement organization will notified immediately by the DHS ONENET SOC, or if necessary, by other organizations who will inform the DHS ONENET SOC at the earliest time possible.

6.0 TECHNICAL CLASSIFIED DATA SPILLAGE INCIDENTS

Detailed procedures can be found in the Classified Data Spillage Incident Handling Playbook maintained by DHS ONENET SOC with input and approval by DHS CSO.

6.1 Overview

The procedures described in this overview are not intended to supplant any current procedures for handling and protecting either classified data or spillages of classified data, especially procedures that may be more stringent than those described here. This document does not address any potential legal issues relating to incident response. Authoritative guidance on such legal issues should be sought by the CISO. All spillage incidents are handled, and reported as significant incidents, the highest incident level. Spillage incidents are never considered minor incidents.

Only Technical Classified Spillage incidents that meet one or more of the following criteria can be processed by DHS ONENET SOC:

- The incident involves classified data on a DHS system
- The incident involves classified data on an non-DHS system where the data owner is within DHS
- The spillage was caused by DHS personnel

The DHS ONENET SOC will process all classified spillage incidents where the spillage occurred within the FOUO environment. Incident reports will not include any classified data, rather, it will only include the information necessary for management and IT personnel to understand where the spill occurred and the actions taken or to be taken for remediation.

The DHS ONENET SOC no longer handles non-technical classified incidents, which are classified incidents not involving IT systems; all such incidents should be sent to SSPDsupport@dhs.gov.

6.2 DHS Component Handling of Spillage Incidents

The following are handling stages and general guidelines. For more detailed guidance see the *Classified Data Spillage Incident Handling Playbook*; a copy should be maintained in every Component SOC.

Assess:

- Confirm that a spillage has occurred.
- Determine the classification level of the data.
- Determine the clearance level of the system or person that received the data.
- Determine the owner or source of the data.
- Ascertain the number and identity of any users, systems, or applications involved.
- Obtain contact information for the person or authority that determined the classification level, for the persons and organizations responsible for handling the spillage, including organization affiliation of each all involved user and system.

Report:

- Immediately use the approved incident reporting procedures to notify the necessary persons and organizations, including, if required, Internal Affairs and law enforcement.
- Ensure that reports have appropriate security markings and are handled properly.
- Track the necessary information and incident handling progress until closure.
- Contain:
- Identify all affected systems and applications.
- Execute approved procedures to prevent further spread of spilled data.
- If approved procedures do not exist, coordinate with DHS ONENET SOC who will obtain guidance from the DHS Office of Security.

Eradicate:

- Execute approved sanitization procedures using approved utilities to remove spilled data from contaminated systems, applications, and media.

Recover:

- Recover and restore affected systems and applications to a secure and functional configuration.
- Submit a final report to the necessary persons and organizations, using appropriate data markings and handling, to certify closure of the incident.
- Incident Monitoring Capability

The DHS ONENET SOC shall provide 24x7 continuous monitoring, analysis and reporting of security information. Technical security staff monitor the DHS TICs, PEPs, and the DHS EMSG, and analyze incoming data flows searching for indications of events that fit into one of the Security Incident Categories shown in Table F-5. Analysts also use security tools to discover security events of interest , prioritize them by asset criticality and exposure, and triage them for viability as a true-positive alert that will yield an incident upon further investigation. The DHS ONENET SOC shall perform 24x7 security monitoring and analysis of event data from all infrastructure as determined by the DHS CISO.

The DHS ONENET SOC categorizes events by groups as shown in Table F-5.

Event Group	SEN Categorization	Examples
Malicious Logic	Critical or Moderate	ZeusBot, FakeAV, SpyEye, Poison Ivy (malware not detected by AV, APT malware or a network worm)
Probes or Scans	Low or Moderate	Internal Transmission Control Protocol (TCP) Sweep,External Brute Force Attempt
Unauthorized Access	Critical or Moderate	Suspicious login, successful external intrusion

Event Group	SEN Categorization	Examples
Misuse	Critical, Moderate, Low	Inappropriate web sites
Classified Spillage	Critical	Disclosed Classified information to external or internal entity
Alteration/Compromise of Information	Critical or Moderate	Disclosed FOUO to external entity, Disclosed PII to internal/external entity
Denial of Service (DoS)	Critical or Moderate	Syn Flood, Internet Control Message Protocol (ICMP) flood

Table F-4: DHS ONENET SOC Security Event Classifications

- Security Event Notifications and Pursuant Investigations

Security Event Notifications (SEN) are tickets generated in EOC Online indicating that a monitored event has been identified and analyzed by a SOC analyst to be associated with activity that may be considered a security incident and as such the event requires a thorough investigation. SENs are generally the product of the DHS ONENET SOC monitoring and analysis service, but may be generated based on information from other sources such as US-CERT, intelligence reports, law enforcement agencies, etc.

The DHS ONENET SOC must monitor shared infrastructure and open/closed source information analysis, create a SEN as soon as this activity is detected and triaged to have a high probability of being a true-positive. DHS ONENET SOC will identify events of interest that require further investigation, and will create SENs that outline pertinent event information. SENs are the primary method the DHS ONENET SOC uses to coordinate with Component SOCs in performing analysis of Component security events.

A SEN will be sent to the Component SOC when the DHS ONENET SOC becomes aware of an event involving one or more of that Component’s systems, when the event may pose a security risk. Once received, it is the Component's responsibility to acknowledge the SEN and to begin an active investigation to identify the event as false positive or a confirmed incident. Among others, activities during an investigation may include reviewing application and firewall logs, checking host-based and network intrusion detection systems, and forensic analysis on the host. It is the Component's responsibility to gather as much information as possible about the event. If the event is confirmed as an incident, the SEN must be escalated by the Component using EOC Online. When it deems necessary, the DHS ONENET SOC may also escalate a SEN.

DHS Components must track all network security investigational activity within EOC Online by creating a SEN for any event that has been triaged to have a high probability of being a true-positive. All SENS drafted by the DHS ONENET SOC or the Components must be published or closed within 24 hours of creation.

To facilitate a more in-depth Component investigation, SENs will contain all available security event background information applicable. If the Component requires additional information not contained in the SEN, such information may be requested at any time.

When a Component has completed investigation pursuant to receipt of a SEN, the SEN must be replied to via EOC Online. The reply must include the Component’s detailed analysis indicating that the event was false-positive or a confirmed incident. If the event was confirmed as an incident, the SEN must be escalated using the EOC Online escalation mechanism. Escalation must not occur until the activity within the SEN has been confirmed. Premature escalations will be routed back to the SEN stage by DHS ONENET SOC. For some incidents, the DHS ONENET SOC may request additional findings, system logs, system images, malware samples, or other information to facilitate systematic reporting to DHS leadership and US-CERT, and to assess overall impact to DHS and assist in the determination of intrusion scope.

The DHS ONENET SOC conducts security monitoring for DHS Components as set forth by its charter. In order to provide the best possible service to Components, the Program Manager, Information System Security Manager (ISSM), and the DHS ONENET SOC shall agree upon various focus areas and prioritize monitoring goals prior to commencement of monitoring operations. Categorization levels determine the escalation path as well as the reporting levels to which alerts are disseminated. It is important to note that Intrusion Detection System (IDS) vendors' classification levels are not always an accurate gauge as to the severity of the alert. Additionally, correlation of alert data may lower or raise the IDS signature categorization. DHS ONENET SOC analyst's determinations are the standard to which all alerts are reported.

DHS ONENET SOC may create informational SENs as a means of notifying Components of events that have a low probability of applicability yielding an incident or to increase situational awareness of Components in regards to cyber security issues. Components are not required to take action on situational awareness if the notification is not applicable to their environment.

APPENDIX F1 ACRONYMS AND ABBREVIATIONS

Acronym	Meaning
CBP	United States Customs and Border Protection
CCE	Common Configuration Enumeration
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
CONOPS	Concept of Operations
CPE	Common Platform Enumeration
CSO	Chief Security Officer
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DMA	Digital Media Analysis [forensics]
EAIR	Enterprise Architecture Information Repository
FEMA	Federal Emergency Management Administration
FLETC	Federal Law Enforcement Training Center
FOUO	For Official Use Only
GWO	Government Watch Officer
HSDN	Homeland Secure Data Network
I&A	(Office of) Intelligence and Analysis
ICE	U.S. Immigration and Customs Enforcement
IDS	Intrusion Detection System
IIMG	Interagency Incident Management Group
IP	Internet Protocol
ISSM	Information Systems Security Manager
ISVM	Information Security Vulnerability Management
IT	Information Technology
LES	Law Enforcement Sensitive
NCRCG	National Cyber Response Coordination Group
NIST	National Institute of Standards and Technology
NLECC	National Law Enforcement Communication Center
NOC	Network Operations Center

Acronym	Meaning
NSA	National Security Agency
NSIRC	National Security Incident Response Center
OCISO	Office of the Chief Information Security Officer
OIG	(DHS) Office of the Inspector General
OMB	Office of Management and Budget
PEP	Policy Enforcement Points
PII	Personally Identifiable Information
PO	Privacy Office
PPOC	Privacy Point of Contact
SCAP	Security Content Automation Protocol
SEN	Security Event Notification
SOC	Security Operations Center
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TIC	Trusted Internet Connection
TRM	Technical Reference Manual
TSA	Transportation Security Administration
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
USSS	United States Secret Service

APPENDIX F2 DHS SOC CONTACT INFORMATION

DHS ONENET SOC Phone Number (Direct)	202-372-8600
DHS ONENET SOC Mailing Address	Department of Homeland Security Security Operations Center (SOC) Mail Stop 0700 245 Murray Lane, SW Washington, DC 20528-0700
DHS ONENET SOC 24/7 Contact Number (OneNET NOC/SOC)	1-877-DHS1NET or 1-877-347-1638
DHS ONENET SOC Fax number (unsecured)	202-372-8950
DHS ONENET SOC E-MAIL	DHS.SOC@dhs.gov
DHS ONENET SOC SECURE E-MAIL	DHS.SOC@dhs.sgov.gov
DHS ONENET SOC Web portal	https://Eoconline.dhs.gov

APPENDIX F3 RESPONSE GUIDELINES

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Exercise/network defense or incident handling testing • US-CERT Category CAT 0	• SEN Category: Informational • Incident Criticality: Non Incident • This category is used during national, state, local, SOC, and Component incident handling tests, including certification and accreditation (C&A) and audit compliance.	• National Level Exercise cyber event testing.	• Document testing activity within Informational SENs. • Review Informational SENs to identify applicability and feasibility of taking action if recommended.	• None Required.
• Unauthorized Access (Intrusion) • US-CERT Category CAT 1	• SEN Category: Critical • Incident Category: Significant • Unauthorized access with system-level or user-level privileges to critical or line-of-business systems/applications. This includes externally-facing system intrusion and major alteration of web content.	• Remote management of internal device by external, unauthorized entity. • Indication of lateral movement from one internal device to another • Exfiltration of data from a host to an external unknown entity. • Unauthorized entity embeds a malicious iframe.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 48 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, email, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC.	• Report incident to US-CERT within 1 hour of confirmation.

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Unauthorized Access (Intrusion) • US-CERT Category CAT 1	• SEN Category: Moderate • Incident Category: Minor • Limited unauthorized access that relates to a noncritical system or does not impact the mission capability of a critical system. This includes externally-facing system intrusion and minor alteration of web content.	• Remote management of internal device by internal entity, appears to be authorized. • Report of password sharing amongst individuals to a non-critical application. • Unauthorized entity removes legitimate content and replaces with unauthorized content.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 120 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC.	• Report incident to US-CERT within 48 hours of confirmation.
• Denial of service • US-CERT Category CAT 2	• SEN Category: Critical • Incident Category: Significant • Critical system or network resources are unavailable or degraded to the point of being unusable by the authorized user community due to attack activity	• Publicly available mission-critical website becomes unavailable after major spike in network traffic. • Users indicate E-mail usage unavailable on a large scale.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 48 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC.	• Report incident to DHS/ Component management through EOC Online within 2 hours of confirmation. • Report incident to US-CERT within 2 hours of confirmation.

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Denial of service • US-CERT Category CAT 2	• SEN Category: Moderate • Incident Category: Minor • Small scale (19 or fewer users) system or network resources for general line-of-business applications/services are unavailable for use by the authorized user community due to attack activity (malicious or inadvertent), and attack source is known and no likelihood of further attack exists (internal incident).	• Non-critical, internally accessible application is unavailable due to user error or misconfiguration. • Small, non-critical site with less than 20 users is intentionally taken off-line by a disgruntled employee.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 120 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC.	• Report incident to US-CERT within 48 hours of confirmation.
• Malicious code or logic (virus, Trojan, worm, etc.) • US-CERT Category CAT 3	• SEN Category: Critical • Incident Category: Significant • A DHS systems is infected by malicious logic where antivirus was bypassed allowing successful infection and post-infection activity by the malware including Command and Control or Exfiltration. • The malicious logic is widespread (10 or more) infections by the same malicious logic.	• A Trojan successfully installs, the machine successfully beacons out to external IP without being blocked. • The same piece of malicious logic propagated to more than 10 workstations within multiple Components in less than 24 hours with different delivery vectors.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 48 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC. Components are to provide specific information as to the network, host-based, or e-mail header indicators identified or send the malicious logic to DHS ONENET SOC for forensic analysis.	• Report incident to DHS/ Component management through EOC Online within 1 hour of confirmation. • Report incident to US-CERT within 1 hour of confirmation.

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Malicious code or logic (virus, Trojan, worm, etc.) • US-CERT Category CAT 3	• SEN Category: Moderate • Incident Category: Minor • Any malicious logic successfully installed but Department or Component protective measures blocked activity prior to the malware successfully performing any post-infection activity. • Any malicious logic infection not listed as significant. • Malicious Logic code transmitted to a DHS host that did not result in a successful infection but was not detected by the host-based antivirus.	• A Trojan successfully installs but beaconing activity is blocked at the proxy. • Malware attempts to install but is blocked by a Component HIPS. • Adware infection not through a toolbar.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 120 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC. • Components are to provide specific information as to the network, host-based, or e-mail header indicators identified or send the malicious logic to DHS ONENET SOC for forensic analysis.	• Report incident to US-CERT within 48 hours of confirmation.

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Misuse • US-CERT Category CAT 4	• SEN Category: Critical • Incident Category: Significant • An authorized user violates Federal law regarding proper use of computer resources.	• Network traffic indicates criminal activity.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 48 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC. Components are to provide specific information as to the network, host-based, or e-mail header indicators identified or send the malicious logic to DHS ONENET SOC for forensic analysis. • Component may report to Internal Affairs or similar, however, the Component must work with DHS ONENET SOC to notify external Law Enforcement if required for incident.	• Report incident to DHS/ Component management through EOC Online within 48 hours of confirmation. • Report incident to US-CERT within 48 hours of confirmation.

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Misuse • US-CERT Category CAT 4	• SEN Category: Moderate or Low • Incident Category: Minor • An authorized user commits a policy violation of Departmental or Component computer security policies. This may include use of unauthorized password/account sharing, personal use of government resources or information, software such as (i.e. chat programs, peer-to-peer services, browser toolbars), or insecure configurations enabled on a DHS system.	• User installs unauthorized software on a DHS asset • User views pornographic material using a DHS asset.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 120 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC. • Component may report to Internal Affairs or similar, however, the Component must work with DHS ONENET SOC to notify external Law Enforcement if required for incident. • Note: SEN with a category of “Low” are not subject to a close/escalation requirement.	• Report incident to US-CERT within 48 hours of confirmation.

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Probes and reconnaissance scans • US-CERT Category CAT 5	• SEN Category: Moderate • Incident Category: Minor • Unauthorized system probing and/or data gathering that appears to be widespread and/or unusually threatening. • Unauthorized system probing that penetrates network perimeter defenses with the capability of gathering information from internal resources	• Scanning activity occurs from a workstation that is confirmed not to be malicious logic or an authorized scanner.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 120 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC. • *1 hour for any Classified system	• Report incident to US-CERT within 336 hours of confirmation (or 1 hour for any Classified system).
• Probes and reconnaissance scans • US-CERT Category CAT 5	• SEN Category: Low • Incident Category: Minor • Unauthorized system probing and/or data gathering directed towards a specific system. This does not include generic probes and reconnaissance scans taking place on Internet-facing connections.	• Scanning activity occurs from a device that appears to be an authorized scanner but cannot be confirmed.	• For SEN (created by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 336 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC.	• Report incident to US-CERT within 336 hours of confirmation.

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Classified Spillage incident • US-CERT Category CAT 4	• SEN Category: Critical • Incident Category: Significant • Classified information is introduced to a computer system/device that does not have the appropriate classification level or is transmitted without appropriate protection. • Any security incident that involves a system used to process national security information.	• Document with classified markings attached and sent via e-mail to an external webmail account.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 48 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC.	• Report incident to DHS/ Component management through EOC Online within 2 hours of confirmation. • Report incident to US-CERT within 96 hours of confirmation.
• Alteration/ compromise of information • US-CERT Category CAT 1	• SEN Category: Critical • Incident Category: Significant • Any incident that involves the unauthorized altering of critical information, or any incident that involves the disclosure of critical information. This includes PII as documented in M-06-19 • The DHS Privacy Office can subjectively determine the criticality of any privacy incident and are the final authority in these matters.	• Document with FOUO markings attached and sent via e-mail to an external webmail account • An email containing the sensitive PII information of several thousand DHS Component employees was found on a file share without any access restrictions.	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 48 hours of creation. • Notification to DHS ONENET SOC via EOC Online, immediately after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC.	• Report incident to DHS/ Component management through EOC Online within 1 hour of confirmation. • Report incident to US-CERT within 1 hour of confirmation.

Incident Type or Category	Criticality and Description	Example Incident or event	Component Action	DHS ONENET SOC Action
• Alteration/ compromise of information • US-CERT Category CAT 1	• SEN Category: Moderate • Incident Category: Minor • Any incident that involves the unauthorized altering of sensitive information, or any incident that involves the disclosure of sensitive information that does not seriously jeopardize DHS/Component mission. This includes non-sensitive PII as documented in M-06-19.	• A hacktivist posts a large number of DHS email addresses on a publicly available website • A lost package containing one PII record (e.g. Alien Number).	• For SEN (published by DHS ONENET SOC): Investigate, verify and close/escalate to DHS ONENET SOC within 120 hours of creation. • For reported incident: Notification to DHS ONENET SOC via EOC Online, within 24 hours after the Component SOC is made aware of actual or suspected incident if reported directly to Component SOC.	• Report incident to DHS/ Component management through EOC Online within 1 hour of confirmation. • Report incident to US-CERT within 1 hour of confirmation.
• US-CERT Category CAT 6 • Until the highest or most serious category is determined. Then for US-CERT purposes, it is changed to that category.	• N A /	• Unconfirmed report of externally facing website being defaced.	• For reported incident: Notification to DHS ONENET SOC via EOC Online, within 24 hours after the Component SOC is made aware of suspected incident if reported directly to Component SOC.	• N/A

APPENDIX F-3B….SEN ESCALATION GUIDELINES

This table is intended to be a list of guidelines for use by Components when requesting SEN escalation. The items listed are not all-inclusive, and other activity may be used if it indicates confirmation of an incident. DHS ONENET SOC has oversight to disallow SEN escalation if adequate supporting evidence is not provided

Event	Activities to Report
Malicious Logic	• confirmation that the internal host falls within the Component's purview (e.g. internal IP address is within the Component address space if detected through network traffic) as specified in the SEN • the total number of internal hosts involved • external IP(s)/URL(s) where the connections are directed and traffic is either malicious or suspicious (e.g. non-federal, unlikely to be associated with component mission function) • network traffic from an internal host to an external host that is indicative of malicious logic (post- infection) such as • connections to known bad IPs/URLs* • known command and control or data exfiltration sites • encrypted or obfuscated outbound traffic to a known bad or suspicious IP/URL • beaconing activity • patterned intervals with multiple failed or successful attempts • traffic with user agent strings known to be associated with malicious logic infection* • data exfiltration activity • host-based forensic analysis confirms malicious artifacts associated with an infection are identified on an internal host such as • files or registry settings associated with malicious logic • suspicious settings associated with malware persistence • network traffic from an internal host to an external hosts that is indicative of malicious logic (pre-infection) such as • traffic to known bad IPs/URLs* • sites known to host exploit code • suspicious patterns within the URL • network traffic that is determined to be the result of data exfiltration or any activity associated with "goal attainment" phase • source of Detection** • infection vector (either confirmed or likely)

Event	Activities to Report
Unauthorized Access (Intrusion)	• Internal host falls within the Component's purview (e.g. internal IP address is within the Component address space if detected through network traffic) as specified in the SEN • Device type of the internal host(s) (e.g. workstation, server) • host-based logs support activity that indicates successful access that is unauthorized such as • suspicious time of event(s) • user associated with account is remote and without access • host-based forensic analysis confirms unauthorized access led to the mishandling, exfiltration or other unauthorized use of sensitive information • trusted third party such as US-CERT confirms compromise • logs indicate that a successful unauthorized access was granted (example: web server web access logs) • source of Detection**
Denial of Service	• externally-facing system becomes unavailable or nearly unusable due to high utilization and web logs indicate DoS activity through excessive connection attempts or specific network traffic which causes a DoS condition (e.g. malformed packets) • confirmation that the host being impacted is associated with the component specified within the SEN • date and timeframe the activity took place • details on source of attack such as country/entity that hosted attack IP • not a regular network outage but one stemming from an external or otherwise unauthorized entity • source of Detection**
Probes and Reconnaissance Scans	• confirmation that the internal host falls within the Component's purview (e.g. internal IP address is within the Component address space if detected through network traffic) as specified in the SEN • type of device(s) [i.e. workstation, server, router] or application(s) was/were scanned • details on source of scan such as country/entity that hosted scanning IP • confirmation that the external scanning entity is from an outside source that is not authorized to perform scans • source of Detection**
Classified Spillage Incident	• component SOC is confident that the classification of the document is Confidential, Secret, or Top Secret (reporting source should be knowledgeable in these matters). • there is verifiable proof that the data has been spilled onto a network that is not authorized to process the classification level (e.g. e-mail, verified review of fileshare, notification from Component or DHS Office of Security). • classification of the unauthorized system(s) now hosting classified data (e.g. FOUO system owned by DHS HQ) • source/cause of the spillage

Event	Activities to Report
Misuse	• confirmation that the user associated with the policy violation is associated with the Component specified within the SEN • details of the infraction that took place (actions taken by the user that resulted in policy violation) • specific files are found and logs are provided that indicate misuse had occurred including logs that indicate which user was logged in at that time • source of Detection**
Alteration Compromise of Information	• confirmation of the associated data type (e.g. FOUO and/or PII) • some quantification of the data compromised (for PII specify number or records and if possible, number of individuals) • confirmation of the spillage location (internal or external) • method of dissemination • confirmation that involved parties did not have a need to know

Table 5: SEN escalating guidelines

*as identified by direct analysis or trusted open or closed source intelligence

** e.g., IDS/SIEM rule, user incident reporting or trusted intelligence source

Appendix F4 US-CERT Federal Agency Incident Categories

The DHS ONENET SOC will use the following guidelines and taxonomy when reporting to US-CERT:

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

Table 6: Guidelines and taxonomy for reports by ONENET SOC to US-CERT

APPENDIX F5 DHS SECURITY INCIDENT REPORT FORM

This form is to be used by Components that do not have access to the DHS ONENET SOC online portal for incident reporting. Component incident responders may adapt and use this document for internal Component security incident reporting as appropriate.

DHS Security Incident Report Template

This form is used for reporting incidents to the DHS ONENET SOC. DHS personnel who need to report significant incidents may use this form, but they should first call the DHS ONENET SOC via phone and report the incident in a timely manner. They may use this form to provide additional information. HSDN incidents should be reported to the HSDN SOC at this time. In the future the DHS ONENET SOC will have the capability to accept HSDN incident reporting. Components may also adapt and use this form for internal security incident reporting.

Sample Incident Response Form		
Incident Report		
Component Service Desk Ticket Number: _____	**Highest data classification level** FOUO □ CONFIDENTIAL □ SECRET □ TS □ SCI □	
Is this a Critical Information Asset? Yes □ No □	**Is this a DHS Financial System?** Yes □ No □	
Does this incident possibly involve PII? Yes □ No □	**Is this a high FIPS categorized system?** Yes □ No □	
Incident Site:		
Organizational Unit:	Acronym:	Location:
Date and Time of Incident:	Priority: (1-5)	
Incident POC:		
Name:	E-mail:	Phone:
Incident Type and Summary: (Please be as specific as possible. Include how the incident was		
Type of Incident: (Select all applicable for multiple component) Detection of Incident: Description of the Incident:		

System Information: (Please be specific, e.g., Critical Information Asset, Version and Patch

Description of Affected Resources:

Mission of System Attacked: (Administration, Command and Control, Message Handling, etc.)

Damage:

Estimated Operational Impact of Attack (High, Medium, Low): _____

Impact to Data	Impact to Systems	Impact to Service
Loss or Compromise of Data: _____	Damage to Systems: _____	Loss of Service (Yes/No): _____
Identification of Information Compromised: _____	Number of Systems Affected: _____	System Downtime (Hours): _____
Monetary Value to Repair:	Number of Employees Affected: _____	Loss of service to the public (Yes/No):

Contact Information for the Incident Reporter

Name:	E-mail:	Phone:

Notification Tracking	Notified	
Date & Time – NOC / SOC	□	
Date & Time - ISSM	□	
Date & Time - ISSO	□	
Date & Time - Other Organizations	□	

Incident Status:

Site Under Attack: □ Past Incident: □ Repeated Incidents: □ Unresolved: □

Sample Incident Response Form

APPENDIX F6 GLOSSARY

Chain of custody: A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. To ensure a verifiable chain of custody, the evidence must be accounted for at all times.

Classified Incident: Any event that involves a system used to process national security information, or a CIP asset; any discovery of classified information on any system not certified for that level of classified information (for example, discovery of SECRET information on a system not certified to process classified information, or discovery of TOP SECRET information on a system certified only for processing SECRET information).

Compromise of Information: A type of incident where information is disclosed to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred

Denial of Service (DoS): The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Digital Forensics: The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Event: Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

Incident: An assessed event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident handling: Actions taken to protect, document, and restore to normal operating condition computers and the information stored in them when an incident occurs; incident handling involves contingency planning and contingency response.

Incident response: Same as incident handling.

Incident response plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT systems(s).

Internal Incident: An incident that has no impact on any other Component or outside entity and does not require law enforcement investigation.

Intrusion: [see Unauthorized Access]

Malicious Logic: Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

Minor Incident: A security-related incident that does not represent a significant threat to the DHS mission and does not require immediate leadership notification.

Misuse: Misuse occurs when a user violates Federal laws or regulations or Department policies regarding proper use of computer resources.

Multiple Component Incident: Any incident involving or affecting more than one Component.

Probe: A technique that attempts to access a system to learn something about the system.

Procedure: The implementation of a policy in the form of workflows, orders, or mechanisms.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent attack.

Significant Incident: A computer-security-related incident that represents a threat to the DHS mission and requires immediate leadership notification.

Spillage: Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level.

Triage: The process of collecting, sorting, recording, tracking, and prioritizing information to facilitate its appropriate handling.

Unauthorized Access: An unauthorized act of bypassing the security mechanisms of a system.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Appendix F7 DHS Incident Handling Checklist

Incident Handling Checklist: Major steps to be performed in handling a computer security incident.

Identification	
	Determine whether an incident has occurred
	Analyze the precursors and indications (network forensics)
	Acquire, preserve, secure, and document evidence (host-based forensics)
	Look for correlating information
	Perform additional research
	As soon as the handler believes that an incident has occurred, begin documenting the investigation and gathering evidence.
	Categorize the incident (e.g. denial of service, malicious code, unauthorized access, inappropriate usage, multi-category)
	Prioritize incident handling based on the business impact
	Identify what resources have been affected and forecast what resources will be affected
	Estimate the current and potential technical effect of the incident
	Report the incident to the appropriate Component and DHS personnel
	Identify and mitigate vulnerabilities that were exploited
Containment/Eradication	
	Initiate blocks of known bad URLs, IPs or other e-mail/host-based indicators
	Remove the affected the host from the network
	Re-image host if necessary
	Confirm that the affected systems are functioning normally
Recovery/Post Incident Activity	
	Return affected system(s) to an operationally ready state
	Conduct all reporting to external organizations
	Implement additional monitoring to look for future related activity