Homeland Security

DHS 4300A

Information Technology System Security Program, Sensitive Systems

Attachment F

Incident Response

Document Change History

Version	Date	Description
1.0	April 2022	Entire document rewritten to align with current standards and directives. Incorporated Major Cybersecurity Incident Response Team and Guidance:NOSC Metrics Team Lead, My-Phung Pham

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Purpose

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

1.2 Scope & Objective

An incident is defined in the Federal Information Security Management Act of 2002 (FISMA) as "an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

Incident Response is comprised of procedures to detect, respond to, and limit consequences of malicious cyber-attacks against an organization's information systems. 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

1.3.1 Federal Laws

- Federal Information Security Management Act of 2002 (FISMA), 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
- Federal Information Security Modernization Act of 2014 (FISMA Reform), Public Law 113-283, 128 Stat 3087
- 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

1.3.2 Executive Orders and Directives

- Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003
- EO 14028, "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021

1.3.3 Office of Management and Budget (OMB) Publications

- OMB Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
- 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-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017
- OMB Memorandum M-19-02 "Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management," October 25, 2018
- OMB Memorandum M-22-05, "Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements," December 6, 2021

1.3.4 Department of Homeland Security Management Directives

- MD 140-01, "Information Technology Security Program," Revision 2, May 5, 2017
- MD 11056.1, "Sensitive Security Information (SSI)," November 3, 2006
- MD 11060.1, "Operations Security Program," September 25, 2006
- DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems, xx/xx, 2022
- HSAR Class Deviation 15-01, "Safeguarding of Sensitive Information," March 9, 2015
- DHS Instruction 047-01-006, "Privacy Incident Response and Breach Response Team," December 4, 2017
- DHS Instruction 047-01-008, "Privacy Incident Handling Guidance," December 4, 2017.
- 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 Enterprise Security Operations Center Concept of Operations (CONOPS), v1.0, July 7, 2019.
- DHS HQ Cloud Incident Management SOP, v1.0, March 5, 2021
- DHS NOSC Infrastructure Ticket Escalation, v2.0, March 22, 2021
- DHS Security Operations Communication Plan, v1.0, July 13, 2020

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

- NIST SP 800-53, Rev 5, "Security and Privacy Controls for Federal Information Systems and Organizations," December 10, 2020
- NIST SP 800-61, Rev 2, "Computer Security Incident Handling Guide," August 6, 2012
- NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response," September 1, 2006
- NIST SP 800-126, Rev 3, "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3," February 14, 2018

1.3.6 Cybersecurity & Infrastructure Security Agency Center Publications

- CISA/US-CERT "Concept of Operations for Federal Cyber Security Incident Handling," v3.2, April 2005
- Cybersecurity & Infrastructure Security Agency "(CISA) National Cyber Incident Scoring System" April 2017
- "Federal Incident Notification Guidelines" April 2017

1.3.7 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 STRUCTURE

The incident response structure provides all offices within DHS Enterprise and Component levels that will be responsible to respond to incidents within DHS based on affected assets or type of information compromise.

2.1 Roles and Responsibilities for Incident Response

2.1.1 DHS Enterprise Roles

The following offices' roles and responsibilities are written with respect to handling incident response.

2.1.1.1 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 Network Operations Security Center (NOSC)..

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

- Establish, maintain, provide oversight, and ensure compliance with the DHS incident response policy.
- Chair the Major Cybersecurity Incident Response Team (MCIRT).
- Direct DHS OCIO resources in incident response and recovery efforts.
- Coordinate with external Federal Department/Agency CIOs in a government-wide cyber incident.
- Prioritize the order of response efforts in the case of multiple systems and/or multiple Major Incidents.

2.1.1.2 DHS Chief Information Security Officer

The DHS CISO has the following responsibilities:

- Participate as a member of the MCIRT.
- Coordinate with fellow DHS CISOs in a DHS-wide cyber incident.
- Provide technical report to the Office of Legislative Affairs (OLA) for draft notifications to Congress.
- Assist Public Affairs in developing a clear and concise media report.
- Coordinate deployment of NOSC incident handling teams to Component locations.

2.1.1.3 DHS Information Technology Operations Director (ITOD)

The ITOD has the following responsibilities:

- Oversee the DHS NOSC.
- Participate as a member of the MCIRT.
- Periodically test and evaluate the effectiveness of DHS Incident Response through training exercises and testing, in coordination with Component CISOs.

- Ensure that incidents are reported to CISA/US-CERT in accordance with federal regulations.
- Direct DHS NOSC and other OCISO resources in incident response and recovery efforts.
- Provide technical report to OLA for draft notifications to Congress.
- Assist Public Affairs in developing a clear and concise media report.
- Coordinate deployment of NOSC incident handling teams to Component locations.

2.1.1.4 DHS Chief Security Officer

The DHS CSO has the following responsibilities:

- Establish the DHS Insider Threat Program and Insider Threat Operations Center (ITOC).
- Support, guide, and coordinate with the DHS CISO to ensure that DHS IT systems are properly secured.
- Support, guide, and coordinate with the DHS CISO/ITOD on handling incident response involving classified spills.
- Establish partnering agreements for law enforcement support for security-related incidents.
- Coordinate and direct response to all incidents that involve malicious insider threat activity.
- Establish guidelines for reporting potential insider threat activity to the Insider Threat Program.

2.1.1.5 DHS Privacy Officer

The DHS Privacy Office has the following responsibilities:

- Serves as the senior DHS official responsible for oversight of privacy incident management.
- Consults with the MCIRT to determine whether a privacy incident constitutes a major incident.
- Activates the Breach Response Team (BRT) and begins Privacy Incident Handling Guide (PIHG) procedures for major incidents involving PII.
- Oversees the investigations through closure to complete the incident handling process when evaluating non-cybersecurity related incidents involving PII.
- Receives from Component Privacy Officers and Privacy Points of Contract (PPOCs), and from the DHS NOSC, reports on the handling of suspected or confirmed privacy incidents or incidents involving PII for further review and action.
- Coordinates with the MCIRT to provide recommendations to DHS senior officials regarding timing and content of media messaging for privacy incidents.

2.1.1.6 DHS Chief Financial Officer

For systems designated as financial systems by the DHS Chief Financial Officer (CFO), the CFO is notified of incidents and may identify specific mitigation or recovery actions. The CFO also provides a financial impact analysis to MCIRT members if financial systems or information are impacted during a Major Incident.

2.1.1.7 DHS Chief Intelligence Officer

The DHS Chief Intelligence Officer provides reach back support to intelligence community members.

With respect to incident response, the DHS Chief Intelligence Officer has the following responsibilities:

- Coordinate with MCIRT, DHS NOSC, and Component threat intelligence groups to aggregate and organize intelligence.
- Provide oversight and guidance to MCIRT on incident handling activities relating to matters of national security (e.g., classified spills) and approve incident resolution and closure.

2.1.1.8 DHS Office of Legislative Affairs

The DHS Office of Legislative Affairs has the following responsibilities:

- Compose and submit reports to Congress as required.
- Liaise between Congress and the MCIRT on reports and requests for information.

2.1.1.9 DHS Office of Public Affairs

The DHS Office of Public Affairs has the following responsibilities:

- Develop media talking points based on MCIRT reports.
- Brief public media outlets on any DHS Major Incident.
- Monitor public media outlets for news stories that deviate from facts or that compromise DHS Operational Security.

2.1.1.10 DHS Office of General Counsel

The DHS Office of General Counsel has the following responsibilities:

- Provide legal advice to MCIRT and DHS NOSC during incident investigations.
- Coordinate with other legal counsels from other federal or outside entities.

2.1.2 Component Roles

2.1.2.1 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, maintain, provide oversight, and ensure compliance with their Component's incident response policy, in alignment with the DHS incident response policy.
- Participate as a member of the MCIRT when applicable.
- Direct Component OCIO resources in incident response and recovery efforts.
- Prioritize the order of response efforts in the case of multiple systems and/or multiple Major Incidents.
- Establish a Component SOC for incident response capability.
- Ensure that incidents are reported to the DHS NOSC within reporting time requirements.

2.1.2.2 Component Chief Information Security Officer

Component CISOs have the following responsibilities:

- Oversee the Component SOC.
- Participate as a member of the MCIRT when applicable.
- Develop and maintain risk-based information security policies and procedures.
- Ensure that SOC procedures, plans and playbooks align to DHS NOSC procedures, plans, and playbooks.
- Direct Component resources in incident response and recovery efforts.
- Review final incident report for completeness and grants Component SOC to request closure an incident when all response and recovery actions have been completed.
- Request deployment of SOC incident handling teams to Component locations.

2.1.2.3 Component Privacy Officers 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.

Component POs and PPOCs have the following responsibilities:

- Receive, evaluate, report and mitigate instances of suspected or confirmed privacy incidents that affect their Component, through received report or through coordination with program managers, ISSM/ISSOs, or SOC.
- Coordinates with DHS Privacy Officer, Component SOC, and DHS NOSC to complete the incident handling process when evaluating non-cybersecurity related incidents, including progress and timely iterative updates.
- Collaborate with the DHS Privacy Officer, the Component CIO, and the Component CISO to prepare the release of information regarding computer security incidents involving PII or other privacy issues.
- Oversees, with the DHS Privacy Office's Director of Privacy Incidents, the activation and operational activities of the BRT, including PIHG-defined procedures, if their Component is affected by the privacy incident.

2.1.2.4 Component Office of Legislative Affairs

The Component Office of Legislative Affairs has the following responsibilities:

- Compose inputs for reports to Congress as required.
- Liaise with DHS OLA between Congress and the MCIRT on reports and requests for information as required.

2.1.2.5 Component Office of Public Affairs

The Component Office of Public Affairs has the following responsibilities:

- With DHS OPA, develop media talking points based on MCIRT reports.
- With DHS OPA, brief public media outlets on any DHS Major Incident.

- Monitor public media outlets for news stories that deviate from facts or that compromise Component Operational Security.

2.1.2.6 Component Office of General Counsel

The Component Office of General Counsel has the following responsibilities:

- Provide legal advice to the Component SOC during incident investigations.
- Coordinate with legal counsels from DHS OGC and other federal or external entities.

2.1.2.7 System Owner(s) of Affected Systems

A system owner has the following responsibilities:

- Provide all technical diagrams and documentation to incident responders to guide them in containment and eradication of the cyber threat.
- Advise the Component SOC on affected system degradation/status.

2.1.3 Users, System and Network Administrators, and Information System 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.
- Report possible insider threat activities to the Insider Threat Program SOC.

2.2 DHS Organizations Involved in Incident Response

2.2.1 Major Cybersecurity Incident Response Team

The Major Cybersecurity Incident Response Team (MCIRT), will make the determination of whether a cybersecurity incident qualifies as a Major Incident in alignment with CISA/US-CERT requirements. The MCIRT will conduct and coordinate the subsequent security investigation, while keeping both DHS senior leadership and Congress informed. The MCIRT will also be responsible for effectively responding to the incident and guiding the recovery efforts to return DHS business operations to normal operating status.

The MCIRT will be chaired by the DHS CIO and DHS CISO with the relevant Component CIO and Component CISO.

The MCIRT will have members from each of the following organizations:

- DHS HQ
- DHS Office of General Counsel
- DHS Office of Public Affairs
- DHS Office of Legislative Affairs

- DHS Information Technology Operations Director

Affected Component

- Component SOC
- System Owner(s) of Affected System(s)
- Component General Counsel
- Component Public Affairs

DHS HQ (contingent upon incident type)

- DHS Office of the Chief Security Officer (Insider Threat, Physical Security)
- DHS Office of the Chief Privacy Officer (Privacy)
- DHS Office of the Chief Financial Officer (Financial)
- DHS Office of Intelligence and Analysis (Classified Materials)

2.2.2 DHS Network Operations Security Center

The DHS NOSC is responsible for incident response for DHS Enterprise capabilities and is the central coordinating and reporting authority for all computer security incidents throughout the Department. For systems designated as financial systems by the DHS Chief Financial Officer (CFO), the DHS NOSC must report security incidents to the DHS CFO. For privacy information, the DHS NOSC must report security incidents to the DHS Privacy Officer.

Primary focus areas of the DHS NOSC include monitoring the DHS Enterprise environment for attacks, potential threats or vulnerabilities; providing DHS management with unfettered situational visibility throughout the DHS enterprise. The DHS NOSC also provides incident response status to Information Systems Security Managers (ISSM) and IT support staff during incidents, and coordinates with other internal and external resources to DHS to address and investigate incidents that require special handling.

The DHS NOSC provides the following functions/services:

- Perform 24x7 monitoring of shared DHS (enterprise) infrastructure, DHS HQ systems and infrastructure, and any other systems as required by DHS CISOs.
- Notify Component SOCs when enterprise monitoring and analysis activities indicate a security event requires further investigation.
- Provide incident notification and reporting to external entities such as CISA/US-CERT as well as updates in a timely manner.
- Determine incident severity below Major Incident and escalate incidents which may be major to the MCIRT.
- Develop, maintain and execute all identified requirements outlined in *Section 3.0 Incident Response Operational Requirements*

2.2.3 Component Security Operations Center

Each Component SOC is responsible for incident response within its scope assigned by the Component CISO. Component SOCs report events and incidents operationally to the DHS NOSC.

A Component SOC typically provides the following functions/services:

- Provide 24x7 incident response for the Component.
- Perform monitoring of Component systems, including networks.
- Compile and maintain a list of mission-critical systems (Mission Essential Systems and High Value Assets), financial systems, and applications.
- Provide system images, volatile memory images, and other malicious logic or intrusion related artifacts to the DHS NOSC upon request.
- Develop, maintain and execute all identified requirements outlined in *Section 3.03.0 Incident Response Operational Requirements*

2.3 Authority & Role Structure

DHS operates and maintains a federated set of SOCs responsible for incident response on unclassified networks supporting missions across Headquarters, Components, Directorates, and sub-agencies. Each Component, Directorate, and sub-agency within DHS has distinct mission support requirements that impact its SOC's roles, responsibilities, and how they perform operations.

A federated set of SOCs needs separate organizational structures for governance and for operational communications of security-relevant information. Governance and information-sharing forums with appropriate membership provide a method for collaboration across all levels of the DHS operational security program. Within the DHS federated SOC model, the DHS Chief Information Officer (CIO) establishes the DHS Enterprise SOC (DHS NOSC) and a Component CIO may establish the Component SOC and other SOCs subordinate to the Component SOC.

The incident response operational reporting structure is depicted in Figure 1.

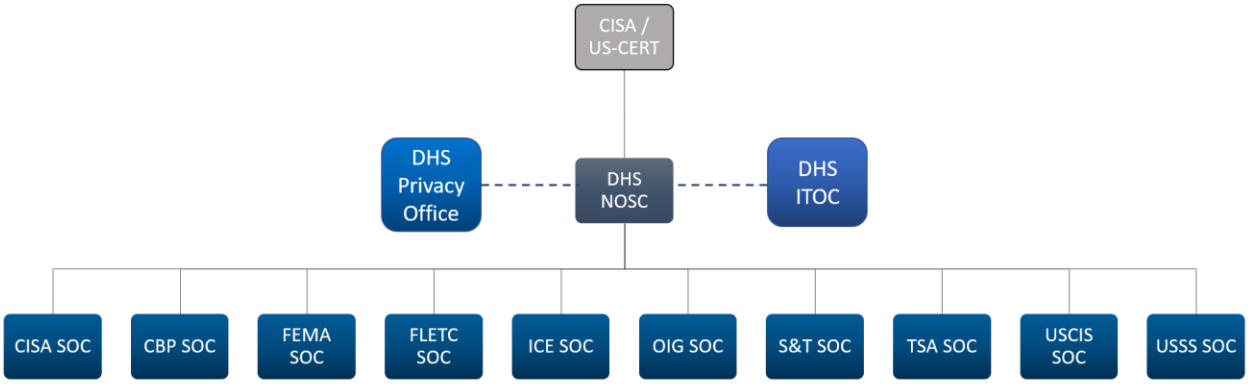

Figure 1: Incident Response Operational Reporting

As identified in *Section 2.1 Roles and Responsibilities for Incident Response* and *Section 3.0 Incident Response Operational Requirements*, the DHS Privacy Office and DHS ITOC work laterally with the DHS NOSC and are involved as cyber incidents cross into their respective mission spaces.

Additionally, as captured in *Section 2.2.2 DHS Network Operations Security Center*, DHS NOSC also provides system and network level monitoring, detection and response similar in scope to a Component SOC. In these instances, DHS NOSC will be reporting in line with Component SOC responsibilities.

3.0 INCIDENT RESPONSE OPERATIONAL REQUIREMENTS

3.1.1 Policies and Procedures

DHS NOSC and Component SOCs develop and maintain a document base of plans, policies, and procedures to support incident response. These include:

- Incident Response Plan
  - **DHS NOSC:** Create and maintain an Incident Response Plan (IRP) and supporting Standard Operating Procedures (SOPs) in accordance with (IAW):
    - NIST SP 800-53 Rev. 5
    - NIST SP 800-61 Rev. 2
    - CISA Federal Reporting Guidelines
    - CISA Incident Response and Vulnerability Playbook
    - OMB Memorandum M-22-05 (or subsequent memorandums)
  - **Component SOC:** Align local IRPs to the DHS NOSC IRP, furnish to DHS NOSC upon request.
- Supporting Policies and Procedures
  - **DHS NOSC**: Create and maintain policies and procedures identifying, at a minimum:
    - SOP(s) for:
      - escalation and reporting of major incidents, and those with impact on the agency’s mission.
      - notification, interaction and evidence sharing with law enforcement.
    - Contingency plans for additional resourcing and surge support, including assigned roles and responsibilities.
    - Identification/designation of a coordination lead/incident manager, when applicable.
  - **Component SOC:** Create and maintain policies and procedures identifying, at a minimum:
    - SOP(s) for:
      - escalation and reporting of major incidents to DHS NOSC, and those with impact on the agency’s mission.
      - responding to law enforcement requests as communicated through DHS NOSC.
    - Contingency plans for additional resourcing and surge support, including assigned roles and responsibilities.
    - Identification/designation of a coordination lead/incident manager to work with DHS NOSC incident manager, when applicable.

3.1.2 Instrumentation

Instrumentation refers to the collection of measurement tools deployed by DHS NOSC and Component SOCs. DHS NOSC and Component SOCs have a responsibility to:

- Develop and maintain an accurate picture of infrastructure (systems, networks, cloud platforms, and contractor-hosted networks) by:
    - widely implementing telemetry to support system and sensor-based detection and monitoring capabilities such as antivirus (AV) software;
    - Endpoint Detection and Response (EDR) solutions;
    - Data Loss Prevention (DLP) capabilities;
    - Intrusion Detection and Prevention Systems (IDPS);
    - authorization, host, application and cloud logs;
    - network flows, packet capture (PCAP);
    - and Security Information and Event Management (SIEM) systems.
- Monitor for alerts generated by CISA's EINSTEIN intrusion detection system and Continuous Diagnostics and Mitigation (CDM) program to detect changes in cyber posture.
- Implement additional requirements for logging, log retention, and log management.

3.1.3 Trained Response Personnel

DHS NOSC and Component SOCs each carry an individual responsibility in ensuring their cybersecurity analysts and personnel associated with incident response are sufficiently trained. Required components of cyber incident response training include:

- Simulated exercise events and tabletop exercises to assess incident response processes.
- Workflow exercises to assess DHS NOSC and Component SOC communication plans during an incident.
- Incorporation of a training environment in order to simulate incident response actions.
- Exercises will be conducted annually at a minimum.

3.1.4 Incident Reporting, Handling and Monitoring

DHS NOSC and Component SOCs fulfill different roles within the Incident Response cycle. DHS NOSC must report incidents, where the confidentiality, integrity, or availability of a federal information system of a civilian Executive Branch agency is potentially compromised, to CISA/US-CERT within one hour of being declared an incident by DHS NOSC. Due to this requirement,

- **DHS NOSC:**
    - Must create and maintain a centralized incident database and case management system.
    - Oversee, direct, and manage confirmed DHS cyber incidents.
    - Follow CISA Federal Reporting Guidelines and OMB Memorandums as documented, formalized processes within the DHS NOSC IRP.
    - Maintain records and track mitigation status and other pertinent information about the incident within the centralized incident database/case management system.
    - Maintain an incident handling capability for usage at the request of Component SOCs.
- **Component SOCs:**

    - Report all suspected and confirmed cyber incidents to DHS NOSC via the NOSC centralized incident database/case management system.
    - Provide timely and relevant updates to cyber incidents within the DHS NOSC centralized incident database/case management system.
    - Implement an incident handling capability and/or identify relevant Component personnel for incident handling, as captured within the Component SOC's IRP.
    - Align incident reporting requirements within the Component SOC IRP IAW DHS NOSC IRP requirements.

3.1.5 Incident Response Testing

Similar to Incident Response Training, DHS NOSC is responsible for conducting Incident Response tests among Component SOCs, DHS and Component Privacy Offices, and other stakeholders. The intent of these tests is to assess the effectiveness of the incident response capability for the DHS Enterprise and its Components. At least annually,

- **DHS NOSC:**
    - Test the incident response capability utilizing exercise events, tabletop exercises, or penetration test data both internally and with Component SOCs.
    - Coordinate with CISA/US-CERT for testing of incident reporting/response IAW the CISA/US-CERT Federal Reporting Guidelines.
    - Utilize qualitative and quantitative data from testing to:
        - Determine effectiveness
        - Identify improvement areas
        - Provide/record incident response measures and metrics
- **Component SOC:**
    - Participate in incident response tests as needed/required.
        - Include relevant Component stakeholders in testing as needed/required.

3.1.6 Incident Response Assistance

Incident Response Assistance refers to support resources in the form of advice, labor assistance, and incident handling assistance provided either by DHS NOSC or as request by DHS NOSC from CISA.

- **DHS NOSC:**
    - Make available and facilitate access to Incident Response and Handling resources IAW incident handling capabilities defined in *Section 3.1.4 Incident Reporting, Handling and Monitoring.*
    - Coordinate/facilitate CISA-provided assistance via the DHS Federal Network Authorization (FNA) on file with CISA to enable incident response and hunt assistance.
    - As needed/required, coordinate third-party IR service providers for assistance through the NSA National Security Cyber Assistance Program (NSCAP).
- **Component SOC:**
    - Request incident response assistance from DHS NOSC IAW the formal process outlined in the DHS NOSC IRP.

3.1.7 Information Spillage Response

Information spillage refers to instances where information is placed on systems that are not authorized to process such information or information exposed to users without a need to know. Classified information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level.

Per OMB Memorandum M-17-12 or subsequent memo, a breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for other than authorized purpose. DHS will treate breachs as Privacy spills.

In preparation for and in the event of an information spillage event,

- **DHS and Component Privacy Offices:**
  - Creates and maintains a Privacy Incident Handling Guide (PIHG).
  - Executes PIHG procedures in the event of breach/privacy spillage.
- **DHS and Component Security Offices:**
  - Create and maintain the Continuity Communications Capabilities (D-16-1) Security Classification Guide (DHS SCG D-16-1).
  - Determines spillage has occurred and classification level of spilled data.
- **DHS NOSC:**
  - Facilitates delivery of PII Breach incidents to CISA/US-CERT IAW CISA Incident Handling requirements in alignment with the DHS NOSC IRP.
  - Notifies and works with FSO for incident handling of classified spills.
- **Component SOCs:**
  - Facilitates incident handling in alignment with the DHS NOSC IRP through its associated Component IRP.

Appendix F1. ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations are used in this document:

Acronym	Meaning
AV	Anti-virus
BRT	Breach Response Team
CBP	Custom Boarder Protection
CDM	Continuous Diagnostic and Mitigation
CFMA	Cyber Security Forensics & Malwre Analysis
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Office
CISA	Cybersecurity and Infrastructure Security Agency
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CONOPS	Concept of Operations
CSO	Chief Security Officer
CTI	Cyber Threat Intel
DC1	Data Center 1
DC2	Data Center 2
DHS	Department of Homeland Security
DHS HQ	DHS Headquarters
DLP	Data Loss Prevention
EDR	Endpoint Detection and Response
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Centers
FNA	Federal Network Authorization
FOUO	For Official Use Only
GWO	Government Watch Officer

Acronym	Meaning
HSDN	Homeland Secure Data Network
I&A	(Office of) Intelligence and Analysis
IAW	In accordance with
ICE	Immigration and Customs Enforcement
IDC	Intrusion Defence Chain
IDCM	Intrusion Defence Chain Methodology
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
INC	Incident
INV	Investigation
IRA	Incident Response and Analysis
IRP	Incident Response Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITOC	Insider Threat Operations Center
ITOD	Information Technology Operations Director
LES	Law Enforcement Sensitive
M&A	Monitoring and Analysis
NIST	National Institute of Standards and Technology
NCCIC	National Cybersecurity and Communications Integration Center
NOSC	Network Operations Security Center
NSA	National Security Agency
NSCAP	National Security Cyber Assistance Program
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OLA	Office of Legislative Affairs
OMB	Office of Management and Budget

Acronym	Meaning
PCAP	Packet Capture
PIHG	Privacy Incident Handling Guide
PII	Personally Identifiable Information
PO	Privacy Office
PPOC	Privacy Point of Contact
S&T	Science and Technology
SCAP	Security Content Automation Protocol
SEN	Security Event Notification
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration
VAT	Vulnerability Assessment Team
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Services
VAT	Vulnerability Assessment Team