Privacy Impact Assessment
for the

# DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response

DHS/ALL/PIA-056

November 16, 2016


**Contact Point**
**Jeffrey Eisensmith**
**Chief Information Security Officer**
**Department of Homeland Security**
**(202) 233-3070**

**Reviewing Official**
**Jonathan R. Cantor**
**Acting Chief Privacy Officer**
**Department of Homeland Security**
**(202) 343-1717**

# Abstract

The Department of Homeland Security (DHS) Information Technology (IT) Enterprise and Component Network Security Operations and IT Security and Privacy Incident Response are a collection of related programs designed to protect the confidentiality, integrity, and availability of Department information and information assets. IT Enterprise and Component Network Security Operations refers to the suite of systems and processes designed to protect DHS network resources and information from external and internal threats. IT Security and Incident Response describes the set of procedures and tools designed to manage DHS IT security or privacy incidents. Because these are privacy sensitive systems that may collect, maintain, or otherwise use personally identifiable information (PII) about DHS personnel, contractors/vendors, customers, and members of the public, a Privacy Impact Assessment (PIA) is needed.

# Overview

DHS IT Systems are a vital resource that enables the Department to accomplish its mission objectives. All IT systems, however, possess inherent security vulnerabilities. As the Department's reliance on IT systems increases so does the risk that DHS operations may be significantly compromised by a disruption to its IT systems and services.[1] This Privacy Impact Assessment (PIA) will evaluate both the DHS IT Enterprise and Component Network Security Operations (hereinafter "IT Network Security Operations")[2] systems designed to secure Department IT resources, and the systems supporting DHS IT Security and Privacy Incident Response[3] (hereinafter "Incident Response") procedures.

---

[1] DHS 4300A Sensitive Systems Handbook v12.0 (November 15, 2015), 6. *Available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

[2] This PIA does not cover cybersecurity activities performed by the National Protection and Programs Directorate (NPPD) as part of the EINSTEIN, National Cybersecurity Protection System (NCPS), Enhanced Cybersecurity Services (ECS), or Automated Indicator Sharing programs. *See* DHS/NPPD/PIA-001 EINSTEIN (September 2004), *available at* https://www.dhs.gov/publication/dhsnppdpia-001the-einstein-program; DHS/NPPD/PIA-008 EINSTEIN 2 (May 19, 2008), *available at* https://www.dhs.gov/publication/dhsnppdpia-008-einstein-2; DHS/NPPD/PIA-026 National Cybersecurity Protection System (July 30, 2012), *available at* https://www.dhs.gov/publication/dhsnppdpia-026-national-cybersecurity-protection-system-ncps; DHS/NPPD/PIA-027 EINSTEIN 3 Accelerated (May 6, 2016), *available at* https://www.dhs.gov/publication/dhsnppdpia-027-einstein-3-accelerated; DHS/NPPD/PIA-028(a) Enhanced Cybersecurity Services (November 30, 2015), *available at* https://www.dhs.gov/publication/dhsnppdpia-028a-enhanced-cybersecurity-services-ecs; and DHS/NPPD/PIA-029 Automated Indicator Sharing (October 28, 2015), *available at* https://www.dhs.gov/publication/dhsnppdpia-029-automated-indicator-sharing.

[3] The term "Privacy Incident" is a DHS term of art that encompasses both suspected and confirmed incidents involving PII that raise a reasonable risk of harm. *See* Privacy Incident Handling Guidance § 1.4.12, *infra* note 8. New draft OMB guidance introduces the term "privacy breach," which is defined as, "The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) a person accesses personally identifiable information for an other than authorized purpose." DHS views the two terms as synonymous and may substitute the term "privacy breach" for "privacy incident" in future documentation once the OMB guidance is published in a final form.

This PIA covers all DHS and Component IT Network Security Operations and Incident Response systems that are in operation, or whose operational status is dependent upon this PIA, at the time of this PIA's publication. This PIA may include future IT network security systems of similar scope and purpose. DHS and Component IT Network Security Operations systems are not considered covered under this PIA until the system in question has undergone review by the DHS Privacy Office through an adjudicated Privacy Threshold Analysis (PTA) and have received express confirmation from the DHS Privacy Office that this PIA provides coverage. Separate PIAs will be required for systems, processes, or programs that raise distinct privacy risks or substantially differ in any other way from the systems described in this PIA. The DHS Privacy Office retains sole discretion to determine whether this PIA provides sufficient coverage or a separate PIA will be required for any systems in question.

This PIA will primarily focus on the systems and other forms of technical controls used by the DHS Enterprise Security Operations Center (DHS ESOC) and Component Security Operations Centers (SOC)[4] to preserve the confidentiality, integrity, or availability of Department information and information assets. These systems include tools that monitor DHS IT systems for security violations, provide automated protection from unauthorized access or misuse of IT resources, and support security requirements for applications and data. As technical controls are only effective when implemented in concert with management and operational controls, this PIA will also evaluate these other types of controls when appropriate.[5]

This PIA will also assess the programs and procedures used by DHS ESOC, Component SOCs, and DHS and Component Privacy Offices when responding to IT security or privacy incidents. IT Security Incident refers to any occurrence that "actually or potentially jeopardizes the confidentiality, integrity, or availability of a DHS IT system," or the information maintained or used by such systems.[6] IT security incident also describes any other act that violates or threatens to violate any DHS security policy, security procedure, or acceptable use policy.[7] Incidents that result in the potential or actual compromise of personally identifiable information (PII) are known as Privacy Incidents.[8] PII describes any information that directly or indirectly identifies an individual, and may include any other information that is linked or linkable to that individual.

---

[4] "Security Operations Center" is a DHS term of art used to describe the entity responsible for managing IT network security operations. Some Component SOCs may use different nomenclature (e.g., U.S. Customs and Border Protection's Computer Security Incident Response Center) but are nonetheless covered by this PIA.

[5] The DHS ESOC and Component SOC IT security activities can generally be divided into the following categories: Management Controls, Operational Controls, and Technical Controls. Management Controls describe procedural safeguards designed to assist management-level personnel in mitigating risk and establishing information system security. Operational Controls describe the organizational rules and policies that govern who is allowed access to IT systems and how those systems will be used. Technical Controls describe the tools used by the DHS ESOC and Component SOCs to secure Department IT systems and resources. *See* DHS 4300A, *supra* note 1, at 137.

[6] DHS 4300A at 197.

[7] *Id*.

[8] For more information about privacy incidents, including a formal definition, please see the DHS Privacy Incident

IT security incidents and privacy incidents may be, but are not always, synonymous with one another. For example, a violation of a DHS IT system's acceptable use policy (an IT security incident) may not compromise any PII. Similarly, PII may be compromised (a privacy incident) via low-tech methods that do not involve any IT systems. Nevertheless, it makes sense to assess both IT security and privacy incident response systems together: DHS ESOC serves as the central repository and coordination point for both types of incidents, and both incident response programs utilize the same reporting and handling systems.

## Information Technology Network Security Operations

DHS IT Network Security Operations and Incident Response systems include operationally sensitive measures to thwart adversaries. Consequently, this PIA will only describe these activities in a general manner to avoid exposing sensitive technical details about DHS operations.

IT Network Security Operations are a complex web of interconnected systems, processes, and programs used by DHS ESOC and Component SOCs to secure DHS IT network resources. The DHS ESOC is the focal point for DHS enterprise-wide cybersecurity efforts. DHS ESOC provides the first line of active defense against cyber threats and oversees Department-wide vulnerability management and network monitoring programs.[9] Component SOCs are responsible for all IT security activities within the Component's network, which include detecting and investigating any potential security incidents.[10] In the event that a security incident does occur, Component SOCs are also responsible for reporting incidents and handling Incident Response activities.

DHS IT Network Security Operations are designed to conduct a wide variety of activities, including boundary protection, network monitoring, and vulnerability scanning.[11] Boundary protection of DHS IT network system resources is accomplished through the use of firewall systems.[12] DHS and Component SOCs are responsible for maintaining control over firewall systems and providing direction and guidance for firewall settings and rules.[13] When used in concert with other security controls, firewall systems are an effective means of securing the Department's network resources from external threats.[14]

---

Handling Guidance (Version 3.0, January 26, 2012). *Available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

[9] *Id* at 17.
[10] *Id* at 18.
[11] DHS 4300A at 146.
[12] *Id* at 152.
[13] *Id* at 154.
[14] *Id* at 152.

A firewall is a system or group of systems that enforce an access control policy between networks.[15] The actual methods by which this is accomplished may vary.[16] The most commonly-used method is to screen network data traffic for viruses, malware, and other external threats.[17] Network traffic passing through the firewall may be logged for future audit and intrusion forensic analysis.[18] DHS and DHS Components may also use firewall systems for secondary functions. Firewalls may be used to segment systems by levels of sensitivity, or to prohibit certain classified systems from connecting to the network altogether.[19] And, although not recommended as a best practice, firewalls also have the capability to implement encrypted data communications.[20]

DHS and Component SOCs are also responsible for monitoring DHS and Component network and systems for anomalies, malicious activities, and threat profiles.[21] If an anomaly is detected and its validity confirmed, the appropriate Information Systems Security Officer (ISSO) and/or the system administrator will be notified to implement corrective actions.[22] For critical events, senior management will also be notified and involved in determining the appropriate course of action.[23]

One type of network monitoring system used by DHS and Component SOCs is the Intrusion Detection System (IDS).[24] IDS tools are an integral part of a layered IT Network Security Operations strategy as firewalls are incapable of protecting a network from certain attack vectors. Firewall systems, generally designed to block external threats, can be compromised by malicious internal actors or intrusion-type attacks. By contrast, IDSs are designed to detect and alert network and system managers of inappropriate or malicious activities regardless of their point of origin.[25]

The IDS tools used by DHS and Component SOCs may vary in function. For example, some IDS tools work by halting malicious data transmissions and disconnecting communication from the originating host. A network-based IDS may work with firewalls to stop an intrusion by altering access control lists. A host-based IDS might itself function like a software firewall for the host system.[26] Some IDS tools may take the additional step of reconfiguring firewalls to permanently block attacking hosts from sending data into the network.[27]

---

[15] *Id* at 153.
[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] *Id* at 154.
[20] *Id* at 153. *See also* NIST SP 800-10, "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls," *and* NIST SP 800-41, "Guidelines on Firewalls and Firewall Policy," *available at* http://csrc.nist.gov/publications/PubsSPs.html, for guidance on firewalls and firewall functions.
[21] DHS 4300A at 149.
[22] *Id*.
[23] *Id*.
[24] *Id* at 148.
[25] *Id*.
[26] *Id*.
[27] *Id*.

Although IDS tools may function differently, most operate according to statistical anomaly and pattern matching (signature) detection principles. Statistical anomaly detection tracks system use to establish a baseline for what is "normal" activity. If the IDS detects system activity beyond what is considered statistically normal, the IDS will alert that an intrusion may have occurred.[28] Pattern matching detection compares system activity to patterns of known attacks (signatures) catalogued in the IDS database. For example, signatures for denial of service attacks, buffer overflow attacks, and backdoors are well known. If a signature is detected, the IDS will alert that an intrusion may have occurred. [29]

Because IDS tools only detect that a potential intrusion might have occurred, IDSs are paired with event correlation systems to reduce unnecessary responses to "false positive" alerts. Event correlation systems compare the information from the detected suspicious activity with information logged by various other security devices to confirm whether an intrusion has actually occurred. This filtering process optimizes DHS resources by directing IT security responses to actual threats instead of relatively harmless activities.[30]

DHS and Component SOCs may also integrate additional tools into network monitoring systems to remediate any gaps in their existing technical capabilities. For example, hostile actors may use encryption to evade detection by DHS IT Network Security Operations. To mitigate this potential gap, DHS could integrate decryption tools into its existing network traffic monitoring and control systems so that DHS may inspect encrypted network traffic.

New and innovative tools are important enhancements to DHS security capabilities. However, new tools often present novel privacy considerations. Future tools and systems, especially ones that raise new privacy issues not addressed by this PIA, must be reviewed by the DHS Privacy Office through an adjudicated PTA and receive express confirmation that the tool is covered under this PIA. New tools may require an update or, if warranted, a separate PIA.

The DHS ESOC and Component SOCs are also responsible for identifying and fixing weaknesses in DHS systems before they can be exploited by malicious actors. Vulnerability scanning is the process of identifying exploits malicious actors can use to gain unauthorized access to or otherwise compromise the system.[31] General-purpose vulnerability scanning tools work by testing target systems against known weaknesses and system design flaws. Common vulnerabilities include default passwords that have not been changed, the ability of unauthorized persons to examine or alter files within a system, authentication bypass errors, and misconfigured network equipment.[32] Some systems require further vulnerability scanning, which may include manually testing vulnerable systems and network elements or using specialized scanning tools

[28] *Id* at 149.
[29] *Id*.
[30] *Id* at 148.
[31] DHS 4300A at 162.
[32] *Id* at 163.

designed to bypass firewalls and IDS tools in order to probe internal systems.[33] DHS personnel involved with the vulnerability scanning program must possess a security clearance level commensurate with that of the system being tested.

## Incident Response

DHS IT Network Security Operations are designed to protect DHS IT resources. However, even the best security system should contain a robust Incident Response mechanism to account for the possibility of a system breach. This PIA will also assess the Incident Response programs and procedures used by DHS ESOC, Component SOCs, and the DHS and Component privacy offices to mitigate the consequences of IT security or privacy incidents.

IT Security Incident refers to any occurrence that "actually or potentially jeopardizes the confidentiality, integrity, or availability of a DHS IT system," or the information maintained or used by such systems.[34] Any other act that violates or threatens to violate any DHS security policy, security procedure, or acceptable use policy is also considered an IT security incident.[35] An incident that results in the potential or actual compromise of PII is known as a Privacy Incident.

IT security incidents and privacy incidents may be synonymous with one another. For example, the loss or theft of a Government computer containing PII would be an example of a single event that causes both an IT security incident and privacy incident. However, that may not always be the case. An IT security incident such as the violation of a DHS IT system's acceptable use policy may not compromise any PII. Similarly, PII may be compromised in a privacy incident via low-tech methods that do not involve any IT systems. Nevertheless, because DHS ESOC serves as the central repository and coordination point for both types of incidents, and because both Incident Response programs utilize the same reporting and handling systems, it will be practical to assess privacy impacts of IT security and privacy Incident Response systems together.

### IT Security Incident

IT Security Incidents begin life as security events.[36] A security event refers to any intentional or unintentional occurrence that may affect the DHS network or other IT resources.[37] When DHS IT Network Security Operations identify an event, the DHS or Component SOC (or Help Desk, in some instances) triages the event and assesses whether it requires an escalated incident handling response.[38]

---

[33] *Id*.
[34] *Id* at 197.
[35] *Id*.
[36] *Id* at 130.
[37] *Id*.
[38] *Id*. *See also* DHS 4300A Sensitive Systems Handbook Attachment F: Incident Response v11.0 (April 24, 2015), Figure 3, at 7, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.,

A typical IT security Incident Response follows six stages:

1. **Preparation** – An approach to incident handling must be developed and documented. Topics include incident handling policies, procedures, and the identification of Components involved in the response effort;
2. **Identification** – The existence of an incident is confirmed by analyzing network and system monitoring information, appropriate officials are notified, and a chain of custody for collected evidence must be established;
3. **Containment** – The impact of the incident is contained;
4. **Eradication** – The cause of the incident must be determined and removed;
5. **Recovery** – The affected system is restored to its original state;
6. **Follow-up** – Follow-up reports must be developed, lessons identified, and procedures are updated as necessary.[39]

Not every Incident Response will follow these six stages, as IT security incidents will vary in magnitude and scope, and the Department's response is tailored to the nature of the individual IT security incident. A minor IT security incident is not likely to impact the DHS mission or a critical DHS asset.[40] A minor incident may be as the result of a simple or inadvertent policy violation that can be rectified by employee training.[41] For example, an employee may violate DHS's policy for limited personal use of IT equipment by:

- Using Internet sites that result in an additional charge to the Government;
- Using Government IT resources for uses other than official governmental business that result in significant strain on Department computer systems (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games); or
- Engaging in other types of prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act.[42]

On the other end of the spectrum, significant IT security incidents constitute a meaningful threat to the DHS mission or critical DHS assets and leadership will need to be immediately notified.[43] An event may be assessed as a significant IT security incident if the event may compromise the confidentiality, integrity, or availability of critical DHS systems or sensitive data[44], or if there is a high probability that the incident will be publicly disclosed and cause

[39] DHS 4300A-F, *supra* note 40 at 28.
[40] *Id* at 3.
[41] DHS 4300A at 130.
[42] DHS 4300A-F at 3.
[43] *Id*.
[44] Examples of "sensitive data" includes information classified as PII or "For Official Use Only" (FOUO). *Id.*

embarrassment to the Department.[45] Examples of security events that may be assessed as a significant incident include:

- Introduction of malicious logic, such as malicious code or viruses, into a DHS IT system;
- Unauthorized attempts to gain access to DHS IT systems or information;
- Any compromise or unauthorized alteration of DHS information;
- The loss or theft of computer media;
- Denial of service attacks that attempt disrupt the availability of critical IT resources such as email servers, Web servers, routers, gateways, or communications infrastructure;
- Probes or reconnaissance scans of DHS networks for critical services or security weaknesses;
- Any violation of a federal law, regulation, or Department policy regarding the proper use of Government IT resources.[46]

When a security event is assessed to be an incident, an incident report must be created in the DHS Enterprise Operations Center (EOC) Incident Handling System, located within DHS ESOC's EOC Online Security Portal. Because the Component SOC, not the DHS ESOC, serves as the primary incident handling coordinator within its respective Component, the incident report provides DHS ESOC with the ability to monitor the status and assist with the handling of privacy and computer security incidents across DHS Components. The incident report contains a thorough explanation of the incident, how it took place, the impact, and the actions taken in response.[47] The incident report must be promptly updated with any new information discovered in the course of the investigation as a complete record is critical to Department Incident Response efforts.[48]

The DHS Office of the Chief Information Security Officer (OCISO) or another appropriate entity will notify and consult with United States Computer Emergency Readiness Team (US-CERT) regarding IT Security Incidents as required by 44 U.S.C. §§ 3553-54 and all related US-CERT and OMB requirements and guidance. Agencies are currently required to notify US-CERT of all computer security incidents with a confirmed impact to confidentiality, integrity, or availability within one hour of being positively identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Component SOC, or IT department.

DHS and Component offices maintain separate reporting and handling procedures, including the use of separate reporting systems, for incidents involving classified or other types of sensitive information.[49] Incidents involving classified data on a DHS system, classified data owned by DHS on a non-DHS system, or a classified data spill caused by DHS personnel are known as

[45] DHS 4300A-F at 3.
[46] DHS 4300A-F, Appendix F-3b at 48.
[47] DHS 4300A-F at 23.
[48] *Id* at 16.
[49] DHS 4300 at 131.

"technical classified spillage incidents."[50] DHS ESOC and Component SOCs are responsible for monitoring the security of DHS classified systems and handling any technical classified spillage incidents that involve IT systems.[51] All classified spillage incidents are reported and handled as significant incidents, as the protection of classified data and the handling of any incident involving classified data is of the utmost importance.[52]

**Privacy Incident**

PII incidents, also known as Privacy Incidents, are suspected or confirmed breaches of personally identifiable information in electronic or physical form. Multiple federal regulations require agencies to protect PII. PII consists of any information that allows an individual to be identified, either directly or indirectly, including any other information that is linked or linkable to that individual. PII must be protected regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, or federal employee or contractor.[53] The DHS Privacy Incident Handling Guidance (DHS PIHG) establishes a standardized set of procedures across Components that informs DHS personnel of their obligation to protect PII, establishes the responses to a privacy incident, and creates individual accountability for privacy compliance.[54]

A potential loss or compromise of PII is known as a privacy incident. The lifecycle of a typical privacy incident generally mirrors Incident Response for an IT security incident and includes the following:

1. A privacy incident is discovered and reported.
2. The Component SOC and/or Component Privacy Office begin an investigation into the privacy incident.
3. The Component SOC recommends technical mitigations. The Component Privacy Office may approve certain technical mitigations (e.g., purging an email involved in a privacy incident).
4. The Component SOC completes applicable technical mitigations (e.g., purging an email), and the Component Privacy Office completes applicable privacy mitigations (e.g., providing notification and counseling to affected individuals when appropriate).
5. Once the mitigations have been applied, the Component SOC and Component Privacy Office will request that the incident be closed.
6. DHS ESOC routes the incident closure request to the DHS Privacy Office for review.

---

[50] *Id* at 32.
[51] *Id*.
[52] DHS 4300A-F at 32.
[53] DHS PIHG at 6. *See also* DHS 4300A, at 62; OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.
[54] DHS PIHG, *supra* note 8.

7. The DHS Privacy Office will either certify that the incident has been fully remediated, and approve closure of the incident, or will request more information.
8. Once the DHS Privacy Office approves the incident closure request, the DHS ESOC closes the incident.

The exact steps taken may vary from one incident to another, as the appropriate response is determined by the particular facts and circumstances of each incident. The particular circumstances of each incident will also determine which parties will need to be notified of the incident. For example, the US-CERT will almost always be notified as OMB Memorandum M-06-19 requires that all incidents involving PII, suspected or confirmed, be reported to US-CERT within one hour of discovery of the incident.[55] In contrast, DHS and Component Chief Financial Officers will need to be notified when a privacy incident involves Government-issued credit cards, but are otherwise not generally notified of privacy incidents.[56]

As with IT security incidents, a privacy incident report must be created in the DHS EOC Incident Handling System. The incident report contains a description of the incident, a description of the PII that was compromised, the impact, what actions were taken in response, and any documents relating to the incident or the decision to notify external parties if relevant.[57] Updates on the investigation and communications concerning the privacy incident handling process should be entered into the privacy incident report as the situation develops.[58]

The EOC Incident Handling System allows the DHS Privacy Office to review and ensure that the appropriate mitigations have been applied to all privacy incidents. The DHS Privacy Office's approval to close the incident is documented in the report log.

# Section 1.0 Authorities and Other Requirements

## 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

- The Privacy Act of 1974[59] provides privacy protections for records containing information about individuals (i.e., citizen and lawful permanent resident) that are collected and

[55] DHS 4300A at 125. *See also* OMB M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments" (July 12, 2006), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-19.pdf.
[56] DHS PIHG at 21.
[57] DHS PIHG at 52.
[58] *Id* at 25.
[59] 5 U.S.C. § 552a.

maintained by the Federal Government and are retrieved by a personal identifier. The Act requires agencies to safeguard information contained in a system of records.

- The Homeland Security Act of 2002[60], Section 222, created the position of the Chief Privacy Officer (CPO) and granted the CPO authority to create DHS privacy policy, including the DHS "mixed system" policy.[61]
- The Critical Infrastructures Protection Act of 2001[62]
- The Federal Information Security Modernization Act (FISMA), as amended[63]
- OMB Memorandum M-06-15[64] reiterates and emphasizes agency responsibilities under law and policy to appropriately safeguard sensitive PII and train employees regarding their responsibilities for protecting privacy.
- OMB Memorandum M-06-16[65] requires agencies to implement encryption protections for PII being transported and/or stored offsite.
- OMB Memorandum M-06-19[66] requires agencies to report all incidents involving PII to US-CERT within one hour of discovery of the incident.
- OMB's Memorandum Recommendations for Identity Theft Related Data Breach Notification[67] outlines recommendations to agencies from the President's Identity Theft Task Force for developing agency planning and response procedures for addressing PII incidents that could result in identify theft.
- OMB Memorandum M-07-16[68] identifies existing procedures and establishes several new actions agencies should take to safeguard PII and to respond to Privacy Incidents.

---

[60] 6 U.S.C. § 142, Public Law 107-296.
[61] "Mixed System" is the term used to describe any system of records that "collects, maintains, or disseminates information, which is in an identifiable form, and which contains information about U.S. Persons and non-U.S. Persons." *See,* U.S. Department of Homeland Security Privacy Policy Guidance Memorandum 2007-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons (January 7, 2009), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[62] 42 U.S.C. § 5195c.
[63] 44 U.S.C. § 3554.
[64] OMB Memorandum M-06-15 (M-06-15), Safeguarding Personally Identifiable Information (May 22, 2006), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-06-15.pdf.
[65] OMB Memorandum M-06-16 (M-06-16), Protection of Sensitive Agency Information (June 23, 2006), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf.
[66] OMB Memorandum M-06-19 (M-06-19), Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-06-19.pdf.
[67] OMB Memorandum: Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/task_force_theft_memo.pdf.
[68] OMB Memorandum M-07-16 (M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007), *available at*

## 1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Elements of Department incident reporting and network defense programs may also be covered by one or more of the SORNs listed below.

- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (November 25, 2008)[69]
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012)[70]

Most systems will be covered in part or in entirety by DHS/ALL-004. DHS/ALL-004 covers the collection, review, and maintenance of employee and public members' data, as well as any logs, audits, or other security data regarding the use of such information technology resources.[71]

- DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010)[72]

Some systems contain only employee PII used in a similar manner to usage by HR systems. DHS/ALL-023 covers Government employees and contractors, as well as all of the types of information collected for the purpose of "[collecting and maintaining] records of processing of personnel security-related clearance actions."[73]

- Various Source System SORNs

PII that may be compromised as part of a privacy incident remains covered by the source system SORN (i.e., the SORN that permitted the original collection). For example, if a box of Alien Files is lost in transit between DHS facilities, the compromised information and any DHS contact with the impacted individuals is covered by the Alien File, Index, and National File Tracking System of Records.[74]

---

https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

[69] DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (November 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm.

[70] DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

[71] Privacy Threshold Analysis for the Enterprise Security System (USCIS, 20160330), 8.

[72] DHS/ALL-023 - Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.

[73] OSI NSI SVR PTA at 8.

[74] DHS/USCIS/ICE/CBP-001 – Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013), *available at* https://www.gpo.gov/fdsys/pkg/FR-2013-11-21/html/2013-27895.htm.

### 1.3 Has a system security plan been completed for the information system(s) supporting the project?

As of this PIA's date of publication, all DHS IT network security and Incident Response systems covered by this PIA have been granted Authority to Operate (ATO).

### 1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Records retention schedules for Department of Homeland Security and Component programs and systems can generally be found in the National Archives Records Control Schedules (RCS) repository.[75] When DHS has not created an individualized records retention schedule for a specific program or system, DHS IT Network Security Operations and Incident Response systems may be covered by the following NARA General Records Schedules:

- 3.1: General Technology Management Records,[76]
- 3.2: Information Systems Security Records,[77]
- 4.2: Information Access and Protection Records,[78] and
- 4.3: Input Records, Output Records, and Electronic Copies.[79]

### 1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected by DHS IT Network Security Operations and Incident Response systems from Government personnel is not covered by the PRA because Government personnel are exempt from the PRA.

---

[75] U.S. National Archives and Records Administration Records Control Schedules (RCS) repository, *available at* https://www.archives.gov/records-mgmt/rcs/. *See also* Department of Homeland Security-specific records control schedules, *available at* https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-homeland-security.

[76] U.S. National Archives and Records Administration, General Records Schedule 3.1: General Technology Management Records, *available at* http://www.archives.gov/records-mgmt/grs/grs03-1.pdf.

[77] U.S. National Archives and Records Administration, General Records Schedule 3.2: Information Systems Security Records, *available at* http://www.archives.gov/records-mgmt/grs/grs03-2.pdf.

[78] U.S. National Archives and Records Administration, General Records Schedule 4.2: Information Access and Protection Records, *available at* http://www.archives.gov/records-mgmt/grs/grs04-2.pdf.

[79] U.S. National Archives and Records Administration, General Records Schedule 4.3: Input Records, Output Records, and Electronic Copies, *available at* http://www.archives.gov/records-mgmt/grs/grs04-3.pdf.

# Section 2.0 Characterization of the Information

*The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.*

## 2.1 Identify the information the project collects, uses, disseminates, or maintains.

**IT Network Security Operations**

DHS IT Network Security Operations systems may monitor, collect, and use all information transmitted over DHS network connections. This can include information contained in emails, information accessed on websites, information contained in files downloaded via the internet, and other types of information transmitted or received in various forms over DHS network connections. As such, the information collected by DHS IT Network Security Operations systems may include PII and Sensitive PII.[80] For example, IT Network Security Operations tools may inspect an email containing PII that is sent from one DHS email account to another; or, monitoring tools may monitor the PII that a DHS employee enter into a form field on a suspicious website. These information collections are necessary for the security and continued functionality of DHS IT network systems.

**Incident Response**

Information is collected, used, and maintained in the form of reports, logs, and notifications during the DHS IT security and privacy Incident Response process.

Reports and Logs

Every assessed IT security and privacy incident must be tracked by an incident report in the EOC Incident Handling System, located in the EOC Online Security Portal. Broadly speaking, incident reports contain an explanation of the incident, how the incident occurred, the impact of the incident, and logs of what mitigation actions were taken in response to the incident. Incident reports generally contain much of the following information:

- Name of the affected system;
- FIPS 199 categorization of affected system(s);[81]

[80] DHS defines Sensitive PII as "Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual." *See* DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (March 2012), *available at* https://www.dhs.gov/xlibrary/assets/privacy/dhs-privacy-safeguardingsensitivepiihandbook-march2012.pdf.

[81] National Institute of Standards and Technology, Federal Information Processing Standards Publication (FIPS) 199 "Standards for Security Categorization of Federal Information and Information Systems" (February 2004), *available*

- Functional use of systems involved;
- Component name in which the incident occurred;
- System owner POC, DHS phone number, and DHS email address;
- Type of data involved (For Official Use Only (FOUO), PII, Law Enforcement Sensitive (LES), Sensitive Security Information (SSI), Secret, Top Secret);
- 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)
- Host-based indicators, Network indicators, and email characteristics;
- Security controls that blocked and/or detected the activity;
- Host operating systems;
- Name of malicious logic;
- Actions taken by affected system;
- Network activity observed (including Internet Protocol addresses (IP addresses) and Uniform Resource Locator (URL) connections made or attempted, and 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;
- Name, phone number, and email address of the individual who discovered the incident;
- Date and time of incident, and a brief description of the circumstances surrounding the potential loss of PII, including:
    - Summary of the type of PII potentially at risk;
    - Interconnectivity of the affected system to other systems;
    - Whether the incident is suspected or confirmed;
    - How PII was disclosed (e.g., email attachment, hard copy, stolen or misplaced laptop);
    - To whom the PII was disclosed and if the individual(s) had a legitimate need to know the information;
    - Whether the information was disclosed within DHS;
    - Whether the information was disclosed to external parties;

*at* http://csrc.nist.gov/publications/PubsFIPS.html.

- If external disclosure is involved, the identity of the party that received the information (e.g., public website, personal email address, other Government entity). [82]

Attachments that include PII may also be appended to an incident report. For example, a record of email header information (e.g., to/from, date/time, subject line) for emails that have been purged as part of a privacy incident may be included. Reporting information may be created and maintained in the normal course of business on systems other than the DHS EOC Online Incident Handling System. For example, a Component Program Manager or Help Desk may be notified of a potential privacy incident via email. A record of the incident, containing some or all of the information listed above, will then also exist in DHS email accounts. Similarly, a record of the incident may reside in an individual's hard drive or shared drive.

If an IT security or privacy incident warrants an investigation, the investigation will collect all relevant evidence related to the incident and create a chain of custody log to preserve control of that evidence.[83] The chain of custody log contains PII in the form of the names and other contact information of all individuals who have touched each piece of evidence. The log may also contain other information such as the date, time, and locations of when the evidence was accessed, transferred, or stored, that could be used to indirectly identify individuals.

Other Department systems may maintain collect and maintain logs of metadata-level information.[84] For example, the DHS EOC Online Incident Handling System records and maintains logs of metadata information from DHS personnel who access the EOC system. This information can be retrieved by examining system logs. However, this type of information is generally not accessible by an individual unless authorized to do so.

Notifications

IT Security and Privacy Incidents may require notification to internal and external parties.

Internal notification generally means notifying staff and senior officials of the incident. Internal notifications may be automatically generated by the DHS EOC Online Incident Handling System or sent manually by email or voicemail. Regardless of the method, internal notifications and access to collected information are limited to those who have a legitimate need to know.

---

[82] DHS PIHG at 24. *See also* DHS 4300F at 25.
[83] DHS 4300F at 30. *See also* DHS PIHG at 43.
[84] Metadata is data that provides information about other data. For example, whereas the body of an email contains the substantive information communicated from one party to another, the metadata describes information about the communicating parties: the sender's email address, the recipient's email address, the sender's IP address, when the email was sent, what software was used to send email, which servers the email traveled through on its way to the recipient, etc. In the context of the DHS EOC Online Incident Handling System, the recorded metadata may consist of the user's identity, the user's IP address, when the user accessed the system, which records did the user access, etc.

A Privacy Incident may require notification of external parties such as the individuals affected by the Privacy Incident. The privacy incident report in the EOC Incident Handling System must be updated to reflect that decision. The Privacy Incident Report may also be updated with documents pertaining to the decision to disclose information outside of the Department.[85] Examples of documents include the External Notification Assessment, press releases regarding the Privacy Incident to the media, or the notification letter to affected individual(s).

## 2.2 What are the sources of the information and how is the information collected for the project?

The DHS IT Network Security Operations and Incident Response systems collect information directly from the use of DHS IT systems, by DHS personnel in the course of incident investigations, and from members of the public involved in incidents by virtue of their interactions with the Department or Department IT systems.

## 2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

DHS IT Network Security Operations and Incident Response systems generally use commercial data or publicly available data in only very limited circumstances. Commercial data includes "information originally collected by a private organization for non-governmental purposes, such as for marketing or credit reporting."[86] For example, IT network security systems may use commercial off the shelf tools and commercial databases such as antivirus definitions.

Publicly available data includes "information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency."[87] Some DHS IT network security systems may come into incidental contact with publicly available data. Component SOCs may review social media sites accessible to DHS personnel using Government-furnished equipment to make sure these sites do not contain issues that could compromise DHS systems. The Component SOC may encounter PII during its review of a social media site. However, it is important to note that even though this PIA covers incidental encounters with commercial and publicly available data, such as in the above example, this PIA would not cover DHS programs and systems expressly designed to access or obtain PII contained on social media sites. Any DHS IT network security operations programs or systems expressly designed to collect commercial and publicly available data must, at minimum,

[85] DHS PIHG at 52.
[86] DHS Privacy Impact Assessment Official Guidance 2010 (June 2010), at 16, *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf.
[87] *Id.*

undergo an adjudicated PTA review by the DHS Privacy Office and may be required to be covered by a separate PIA.[88]

## 2.4 Discuss how accuracy of the data is ensured.

Information is generally collected directly from the individual through his or her use of a Department IT system and is therefore considered to be accurate. Most IT network security operations systems are automated, which increases data accuracy by minimizing the opportunity for human error to be introduced within the system. In addition, DHS systems employ various internal controls and procedures to ensure the data accuracy, and the veracity of the incident is also confirmed by analyzing network and system monitoring information.

When a system requires human input, such as during the Privacy Incident response process, accuracy of data is ensured through procedural safeguards and the source records system. Communication and mutual decision-making between multiple DHS and Component offices and personnel are required throughout Incident Response activities, and all open incidents must be reviewed by the DHS Privacy Office before they may be closed.

## 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk**: There is a risk that information may be attributed to the wrong individual. For example, one individual may allow another to use his or her account, which can cause inaccurate information to be attributed to the wrong individual.

**Mitigation:** This risk is first partially mitigated on the front end by DHS IT Security Awareness and Privacy Awareness training (*see* Section 8.2, below). DHS personnel are trained and advised to refrain from engaging in behavior such as sharing credentials. Other technical safeguards built into DHS systems, such as automated system log-outs after periods of inactivity and requirements to re-authenticate credentials when accessing different areas of a system environment, also partially mitigate the risk of inaccurate attribution of information to individuals. In these addition to these preventative measures, human analysts and investigators ultimately determine whether or not the information presented by monitoring systems are accurate.

[88] *See* discussion *supra* at note 2.

**Privacy Risk**: There is a risk of the over-collection of information, including PII.

**Mitigation:** This risk is partially mitigated for DHS IT Network Security Operations systems. Network security operations systems are designed to monitor, collect, and use all information transmitted over DHS IT systems and networks. Some projects contain "whitelists" that omit certain types of known websites, such as banking or health insurance websites, from the scope of the information collection. The risk of over-collection is also partially mitigated by the limited use of the information, a controlled user base with access to information collected, and a limited retention schedule for any information collected. However, on the whole, the Department concludes that security risks of under-collection outweigh the privacy risks of over-collection.

The risk is mitigated for DHS Incident Response programs. The scope of information collection increases only in response to a demonstrable need for more information. When a potential incident is reported, subsequent written reports will contain only what information is necessary to verify that the incident has actually occurred, assess harm, and to apply appropriate mitigations.

Privacy Incidents also possess an additional organizational safeguard as incident handling efforts will be supervised by the DHS Privacy Office. The DHS Privacy Office reviews all DHS Privacy Incidents to ensure that harms or impacts have been fully remediated by selected mitigation actions. As no privacy incident can be closed unless the DHS Privacy Office has certified that the incident has been fully remediated, this policy ensures the DHS Privacy Office oversight into the scope of information collection into all Incident Responses.

# Section 3.0 Uses of the Information

*The following questions require a clear description of the project's use of information.*

## 3.1 Describe how and why the project uses the information.

Although DHS IT Network Security Operations and Incident Reporting programs work closely together to identify and mitigate threats to DHS information systems, the different program-level mission objectives and system requirements mean different systems may use information in very different ways. Typical uses are described in general terms below.

**IT Network Security Operations**

DHS IT Network Security Operations systems use information to secure other Department systems from threats both external and internal. Uses of information can generally be categorized into three broad categories across various Department programs: monitoring and evaluation, incident response and mitigation, and post-threat review.

DHS IT Network Security Operations projects utilize a number of tools and systems with which to monitor and evaluate network traffic. Threat evaluation often occurs in real-time with monitoring. For example, automated tools search outgoing traffic for keywords (e.g., TOP SECRET) that would signal a loss of data. DHS analysts generally rely on automated tools to inspect the contents of the web traffic for intrusion detection or data loss.[89]

When a potential security incident is identified, information about the event is analyzed to assist DHS personnel in identifying the appropriate response. Information may be necessary in technical incidents to analyze and reverse-engineer malicious software, or in non-technical incidents to determine which policy and procedures were violated that resulted in the incident. Relevant information may also be shared within appropriate DHS Component or HQ offices for mitigation and response purposes.

Once the incident is resolved, it may be used for reporting and other post-incident evaluation purposes. Projects will often compile information to report statistics to leadership, or to provide real-world examples for incident trainings. Some projects may use a database of past incidents to identify trends that would inform practices to better prevent or mitigate future incidents.

**Incident Response**

The collection of information by DHS personnel is a necessary and vital part of incident management in order to quickly and effectively respond to IT security and privacy incidents. In the initial phases of reporting, information is collected to determine whether a potential security event may be assessed as an incident.[90]

That information will assist incident responders to determine the appropriate response to mitigate any harms arising from the incident. Information is necessary to identify the source of the incident and identify what information may have been compromised by the incident. For example, DHS or Component privacy offices may need to identify the data elements that have been compromised during a privacy incident as part of their effort to assess the harm to the individuals impacted by the incident. Information about affected systems and processes is also needed for incident responders to contextualize the value of the lost or compromised information.

When an unauthorized disclosure affects individuals or entities outside of DHS, information collected about the incident is used to assist DHS personnel in identifying the

[89] It is important to note this PIA does not cover any systems or processes operated or maintained by the DHS Insider Threat Program. The Insider Threat Program is covered by DHS-ALL-PIA-052 "DHS Insider Threat Program" (July 2015), *available at* https://www.dhs.gov/publication/dhs-all-pia-052-dhs-insider-threat-program.
[90] DHS 4300A-F at 34. *See also* DHS PIHG § 4.5, et seq.

appropriate officials or parties affected by the incident, and help DHS personnel when or whether those parties should be notified of the incident.[91]

Information is used post-incident to evaluate the Department's response to the incident. This evaluation improves the effectiveness of DHS Incident Response programs for future events.

## 3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

DHS ESOC and Component SOC IT Network Security Operations and Incident Response systems do not perform "data mining" as defined by the Federal Agency Data Mining Reporting Act of 2007.[92]

DHS IT Network Security Operations systems use pattern analysis and other such data analysis tools and systems to accomplish their mission objectives. See Overview, Section 2.1, and Section 3.1 for a description of how these technologies are being used.

DHS Incident Response systems generally do not use technology to analyze patterns or anomalies in databases.

## 3.3 Are there other Components with assigned roles and responsibilities within the system?

DHS and Component IT Network Security Operations systems are highly interconnected with other IT network security systems throughout the Department. For example, if a network monitoring system detects network traffic that violates Department policy, information may be shared with DHS Components and HQ offices to investigate and remediate the policy violation. If criminal activity is detected, relevant information would be shared with the appropriate DHS Component or HQ offices (e.g., Component Internal Affairs or Office of Professional Responsibility, the Office of the Inspector General, or the Office of the Chief Security Officer) as well as law enforcement. Finally, information may be shared with US-CERT or other DHS Components or offices responsible for IT security (e.g., DHS National Cybersecurity and Communications Integration Center (NCCIC), Component Security Operations Centers).

DHS Components play an integral role within the DHS Incident Response program. If an incident originates in a Component, Component offices and personnel will be involved in all phases of incident handling, including reporting the incident, escalating the incident, investigating

[91] DHS PIHG at 28.
[92] 42 U.S.C. 2000ee–3(b).

the incident, notifying affected parties, participating in incident mitigation, and closing the incident. Furthermore, any incident involving PII must be reported to US-CERT.[93]

The DHS ESOC, Component SOCs, DHS Privacy Office, or Component privacy offices may consult with other parts of DHS entities (e.g., Office of the General Counsel, Office of the Chief Human Capital Officer, Component program personnel) as part of Incident Response activities.

## 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk:** There is a risk of unauthorized use of the information maintained in DHS IT Network Security Operations and Incident Response systems.

**Mitigation:** This risk is mitigated generally through role-based access controls so that only authorized DHS personnel have access to the system. DHS personnel are granted access only to information necessary to perform their official duties as determined by their position. Additionally, DHS personnel receive training regarding the proper use systems and rules of behavior prior to being granted access to the system. For example, access to the EOC Portal is limited to individuals involved in IT Network Security Operations or Incident Response and is based on least privilege (e.g., a Component can only see its own incidents or incidents that involve the Component).

All DHS personnel are required to complete annual mandatory privacy and security training stressing the importance of appropriate and authorized use of personal data in Government systems before they are granted access to Department systems. Contractors are not exempt from privacy and security training; all contracts involving the use of sensitive systems contain clauses that ensure contractors are aware of Department requirements to protect data collected and report any incidents relating to their access of the information or any other special requirements. Furthermore, all employees and contractors must pass a fully Qualified Background Field Investigation (FFBI) at or above the level based on position sensitivity designation prior to gaining access to Department systems.

Furthermore, risk is generally mitigated with respect to DHS IT Network Security Operations projects as many of these projects are comprised of automated systems that require little to no input from users.

[93] DHS PIHG at 7. *See also* OMB Memorandum M-06-19 (OMB M-06-19), *supra* note 69, and OMB Memorandum M-07-16 (OMB M-07-16), *supra* note 71.

# Section 4.0 Notice

*The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.*

## 4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Most information is collected from individuals through their use of Department systems. DHS personnel using Department systems consent to terms of use allowing for collection of information before they can receive access. Notice of DHS and Component IT usage policies is present on the log-in screen of all DHS computer stations and in the Rules of Behavior DHS personnel sign before receiving access to DHS IT equipment. Notice is also provided by this PIA as well as the publication of the SORNs identified in Question 1.2.

## 4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Since the information collected from individuals by DHS IT Network Security Operations and Incident Response systems is received from their use of DHS information systems, individuals do not have the option to withdraw consent to particular uses of their information after collection. Once collected, their information is used for the purposes described in this PIA and the SORNs identified in Question 1.2.

## 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** There is a risk that individuals will not be aware that DHS IT Network Security Operations and Incident Response systems collect and use their information.

**Mitigation:** This PIA provides notice that the DHS IT Network Security Operations and Incident Response systems use data resulting from his or her use of DHS systems. Additional notice is also provided by the publication of the SORNs identified in Question 1.2 as well as by Privacy Act statements at the time of initial collection.

When PII has been collected as part of the response to a privacy incident, DHS may provide a separate notice to the individual that their information has been impacted by a privacy incident. However, sometimes notification is not appropriate. For example, notification may not be the most appropriate method to mitigate a Privacy Incident. When there is little or no risk of harm, notification might create unnecessary concern and confusion, and desensitize affected individuals from responding to notifications in another incident when the risk of harm is greater. Notification

must also be consistent with the needs of law enforcement and national security, as well as any measures necessary for DHS to determine the scope of the incident and, if applicable, restore the reasonable integrity of the data system. Under circumstances when notification could increase a risk of harm, the best course of action may be to delay or forgo notification entirely.[94]

# Section 5.0 Data Retention by the project

*The following questions are intended to outline how long the project retains the information after the initial collection.*

## 5.1 Explain how long and for what reason the information is retained.

DHS IT Network Security Operations and Incident Response systems retain all information described in Section 2.1. Information is generally maintained until it is no longer relevant, per the system's individualized records retention schedule. The length of retention may also depend in part on technological limitations, such as how much storage space the security tool possesses.

Other reasons for retaining information include requirements to compile and report statistics for leadership.[95] Some programs use information to identify trends in order to establish or improve best practices, or to provide examples of real-world incidents for future trainings. DHS IT Network Security Operations and Incident Response programs may also uncover personnel actions that can result in corrective and disciplinary actions, including criminal prosecution, for which information must be maintained.[96] Information is then appropriately disposed of when no longer needed.

When DHS has not elected to create an individualized records retention schedule, retention is determined by General Records Schedules (see Section 1.4).

## 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** There is a privacy risk that information will be retained on individual DHS employee computer terminals longer than necessary to accomplish the purpose for which the information was originally collected, inconsistent with the requisite records retention schedules.

**Mitigation:** This risk is mitigated through operational training. DHS reminds DHS IT Network Security Operations and Incident Response System users through policy and training, including required records management training, that they must follow the applicable information retention schedules, regardless of where it is stored.

[94] DHS PIHG at 47.
[95] DHS PIHG at 52.
[96] *Id.*

**Privacy Risk:** There may be a privacy risk in retaining information after an incident has been resolved.

**Mitigation:** NARA General Records Schedules advise that records be kept until follow-up actions have been completed, with exceptions when required for business use. Although the immediate incident may be resolved, information may be required for disciplinary or corrective purposes, and for program reporting and evaluation purposes. Given the safeguards of DHS systems, as well as the fact that for most programs retained records will contain only a minimum amount of PII, the risk of retention beyond incident resolution is acceptable.

## Section 6.0 Information Sharing

*The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.*

### 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information may be shared outside of DHS for a number of purposes as a normal part of the agency operations. DHS may share information to fulfill law enforcement or national security information sharing requirements, as part of incident mitigation activities, or as required by OMB guidance (e.g. sharing certain information with Congress).

DHS IT Network Security Operations systems are generally not designed to share information with external parties. Any sharing of information would likely be to possible law enforcement or intelligence gathering agencies in response to events or incidents that are malicious in nature or done with malicious intent.

Within the context of DHS Incident Response procedures, information sharing with outside parties is most likely to occur as a result of mitigation procedures. For example, if an incident is reported to US-CERT, US-CERT may interact with other entities and officials regarding the incident and coordinate appropriate incident response activities. These appropriate officials may be located outside of DHS. For example, DHS also requires notification to any affected bank(s), if a Privacy Incident involves government-issued credit cards, or individuals' bank account numbers used for direct deposit of credit card reimbursements, Government salaries, travel vouchers, or any benefit payment.

DHS may elect to notify public and private sector agencies who may not receive mandated notification from US-CERT. For example, a Privacy Incident involving medical information may

warrant notification of the incident to health care providers and insurers. Any notifications or disclosure of information to these parties will be made on a need to know basis.[97]

Affected individuals may also receive information as notification of the incident. Depending upon the severity of the incident, DHS and/or its components may enter into a contract with an external ID Theft and Credit Protection Company to offer the services necessary based upon the incident's remediation. As such, the contracted company may assist in carrying out remediation efforts such as mailing incident notification letters to the affected individuals. In these instances, DHS and/or its components will share limited contact information so that mitigation efforts can be fulfilled. The notification will likely include the following elements:[98]

- A brief description of the Privacy Incident, including the date(s) of the Privacy Incident and of discovery
- A description, but not the PII itself, of the types of personal information involved in the Privacy Incident (e.g., full name, Social Security Number, date of birth, home address, account number, alien registration number/file)
- The steps the affected individuals can take to protect themselves from potential harm
- What the Component is doing to investigate the Privacy Incident, mitigate losses, and protect against a likely recurrence
- Who affected individuals should contact at the Component for more information, including a telephone number, email address, and postal address.

## 6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing described above is compatible with the original purpose for which the information was collected. For example, the GITAARS SORN notes that DHS collects PII about individuals using IT resources for the purposes of "track[ing] use of DHS IT resources" and collecting, reviewing, and maintaining "security data regarding the use of such [IT] resources."[99] In other instances, DHS shares information with external parties (e.g., with law enforcement or intelligence partners) to support the Department's efforts to secure DHS IT resources, to facilitate the Department's investigation of the perpetrators who accessed the data, or for other critical objectives. Similarly, if DHS shares information with law enforcement about an employee's criminal misconduct, this sharing supports "personnel security management responsibilities at DHS," including determining "eligibility for access to classified information or assignment to a

[97] DHS PIHG at 51.
[98] For an example of a template notification letter, *see* DHS PIHG, Appendix G: Sample Notification Letter.
[99] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

sensitive position" or conducting "adverse personnel actions."[100] All external sharing falls within the scope of published routine uses defined in the SORNs identified in Question 1.2.

## 6.3 Does the project place limitations on re-dissemination?

The limitations on re-dissemination may vary, depending upon the individual program or system. Any further sharing of data received from DHS IT Network Security Operations and Incident Response programs is permitted as authorized by the recipient agency's SORN(s) or information sharing policies.

## 6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Generally speaking, disclosures of PII outside of the Department are only made in very limited circumstances. Notifications by the DHS ESOC or Component SOCs to law enforcement that include PII (e.g., information about an individual engaging in criminal activity) should be recorded in the logs for the applicable IT security incident.

Disclosures to third parties for privacy incidents would be recorded in the Privacy Incident Report.

## 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There is a privacy risk that information from DHS IT Network Security Operations and Incident Response systems may be improperly disclosed outside of DHS.

**Mitigation:** These risks are mitigated by the fact that information maintained in DHS IT Network Security Operations and Incident Response systems is shared in a manner consistent with the routine uses prescribed in the SORNs identified in Question 1.2 or as required by law. Moreover, any external or Extranet connection with DHS or any DHS Component requires a Memorandum of Understanding (MOU) and an Interconnection Security Agreement (ISA) reviewed and signed by the Component, DHS Chief Information Security Officer, and, if applicable, the Component Privacy Office.

The Incident Response program also builds in additional safeguards that reflect the increased likelihood that information will be shared by this program. DHS personnel may not disclose or cause to be disclosed information about a Privacy Incident to any person without an authorized need to know the information.[101] This restriction applies to all internal and external

[100] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.
[101] DHS PIHG at 46.

communications, including congressional notifications, press releases, and notifications to individuals potentially affected by the Privacy Incident.[102]

# Section 7.0 Redress

*The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.*

## 7.1 What are the procedures that allow individuals to access their information?

Individuals may request access to records about them in DHS IT Network Security Operations and Incident Response systems by following the procedures outlined in the SORNs identified in Question 1.2. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interest.

## 7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If individuals obtain access to the information in DHS IT Network Security Operations and Incident Response systems pursuant to the procedures outlined in the SORNs identified in Question 1.2, they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the SORNs identified in Question 1.2.

## 7.3 How does the project notify individuals about the procedures for correcting their information?

The procedures for submitting a request to correct information are outlined in the SORNs identified in Question 1.2 and in this PIA in Questions 7.1 and 7.2.

## 7.4 Privacy Impact Analysis: Related to Redress

[102] *Id* at 47.

**Privacy Risk:** There is a risk that individuals may not have access to information maintained about them in DHS IT Network Security Operations and Incident Response systems or that individuals may not be able to correct inaccurate information because they do not know which systems maintain information about them.

**Mitigation:** Individuals can request access to information by submitting a Freedom of Information Act (FOIA) request.[103] Individuals may also file a Privacy Act request to request access to information the Department may have about themselves, request amendment or correction of those records, and request an accounting of disclosures of their records by the Department.[104]

## Section 8.0 Auditing and Accountability

*The following questions are intended to describe technical and policy based safeguards and security measures.*

### 8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

DHS safeguards information collected by the DHS IT Network Security Operations and Incident Response programs in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information being stored, including implementing strong practices of data minimization, providing access to information on a least privilege basis, sharing information securely (e.g., via encrypted system connections or within the DHS firewall), and further password protecting sensitive information within secure systems. The logs within the EOC Portal note which users have performed activity as part of Incident Response.

### 8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

DHS has an organizational commitment to accountability for external legal and privacy policy requirements as well as internal DHS policies and procedures. This commitment includes transparency and, when appropriate, the means for remediation and external enforcement.

All DHS personnel must undergo and complete annual Privacy Awareness Training and Education. The annual privacy training teaches DHS personnel how to identify and report incidents

[103] Additional information about DHS FOIA requests can be found at https://www.dhs.gov/foia.
[104] Additional information about DHS Privacy Act requests can be found at https://www.dhs.gov/file-privacy-act-request.

before they are permitted access to agency information and information systems.[105] This annual training also informs DHS personnel of their responsibilities to safeguard PII, and the consequences for violating these responsibilities.[106] All DHS personnel must also undergo and complete annual general and role-based (when applicable) IT Security Awareness training.[107]

## 8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Specific user access control policies and procedures may differ across the Department. But generally, each user account is assigned a specific role with a defined set of privileges to ensure overall system integrity. Access is limited to personnel who have a need to access the system based on their operational roles, which are predetermined depending on the user's function. For example, Components can only see their incidents or incidents involving their Component within the EOC Portal, and privacy staff cannot create or modify security events.

Procedural restrictions may also limit user access to information, such as with the Privacy Incident response process. Information is compartmentalized within Components or groups working on a particular incident.

## 8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Incident response and network defense programs follow several different information sharing frameworks.

Some programs do not share data with external parties. Some programs do not have formal information sharing agreements in place. For these programs, information sharing is carried out if and when it is found to be the appropriate course of action.[108] Several factors may influence the decision to share information: the incident review process may determine notification and information sharing is the appropriate course of action,[109] or the program may detect a security event or security incident where sharing information with an external agency, such as law enforcement, is the appropriate course of action. Information sharing, especially with law enforcement, is likely when detected incidents or events possess an element of malicious intent or criminal activity.

---

[105] DHS PIHG at 11.
[106] *Id* at 56.
[107] DHS 4300A at 80.
[108] DHS PIHG at 47.
[109] *Id*.

## Responsible Officials

Jeffrey Eisensmith
Chief Information Security Officer
Department of Homeland Security

## Approval Signature

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security