Privacy Impact Assessment
for the

GeoSpace

DHS/USCIS/PIA-047

July 12, 2013

<u>Contact Point</u>
Donald K. Hawkins
Privacy Officer
United States Citizenship and Immigration Services
(202) 272-8030

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

Abstract

The Department of Homeland Security (DHS) United States Citizenship and Immigration Services (USCIS) Office of Security and Integrity (OSI) developed GeoSpace to handle the tracking, receipt, and response to incidents that individuals report as Significant Incident Reports (SIR) in and around USCIS buildings and facilities. GeoSpace provides incident management for OSI in geospatial terms, which allows for the timely reporting of critical incidents, activities, and events to USCIS leadership and to the DHS National Operations Center (DHS NOC). USCIS is conducting this Privacy Impact Assessment (PIA) because GeoSpace collects, uses, and disseminates personally identifiable information (PII).

Overview

The Department of Homeland Security (DHS) United States Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States (U.S.). The Office of Security and Integrity (OSI) is an operational branch within USCIS that manages the security and emergency operations to protect employees, facilities, assets, and information and to advance the mission by ensuring effective, efficient, and continual operations. OSI has 9 core functions within the branch including: (1) administrative security; (2) command center and special security; (3) emergency management and safety; (4) field security; (5) internal review; (6) investigation; (7) personnel security; (8) physical security; and (9) integrity. As part of these functions, OSI ensures that any incident that interrupts USCIS operations is documented in a Significant Incident Report (SIR). USCIS SIRs serve two primary functions: (1) to provide situational awareness to USCIS leadership for incidents that occur in and around USCIS facilities and impact daily operations; and (2) to report incidents that fall under the DHS Directive 252-06, *Office of Operations Coordination: DHS Operational Reporting Requirements*,[1] dated February 1, 2008, to the DHS National Operations Center (DHS NOC).

Significant Incident Reports (SIR)

The SIR is the official reporting format used by USCIS to record and report significant incidents to DHS and USCIS leadership. Significant incidents are events that potentially impact USCIS facilities, operations, or personnel and generally fall into one of the following categories: (1) facilitated apprehension; (2) office closure, evacuation, or fire alarm; (3) loss of services or utilities; (4) building/physical security related incidents; (5) information loss/mishandling; (6) lost, stolen, or damaged government property; and (7) employee/contractor events.[2] A more robust list of incidents that require a SIR is included in Appendix A of this PIA.

[1] DHS Directive 252-06, dated February 1, 2008, is available at www.dhs.gov. This directive establishes the Department of Homeland Security's (DHS) operational reporting requirements for events that fall outside the scope of the National Response Plan (NRP). It is the principal document for leading, governing, integrating, and managing the situational awareness and reporting throughout DHS operational components.

[2] While GeoSpace collects information on employee misconduct, the Investigations Division Case Management System (IDCMS) is responsible for managing investigations into all allegations of employee/contractor misconduct. The forthcoming IDCMS PIA can be found at www.dhs.gov/privacy-compliance.

USCIS creates a SIR when a significant event occurs that interrupts agency operations in a domestic or international agency office. For example, if there is an injury (e.g., employee or customer) at a USCIS office, a weather-related event or natural disaster occurs that results in the closure of a USCIS office, or if government property and/or documents are or lost or stolen, a SIR must be created and reported to the OSI Command Center (C2). OSI administers C2 to ensure the integrity and continuity of secure, effective, and efficient USCIS operations by identifying, analyzing, and disseminating information for senior leaders, operational managers, and employees so that they can take appropriate action.

USCIS employees or contractors designated by leadership as their office "SIR submitter," complete the SIR Form, Form G-1399, *Significant Incident Report*, and submit it to C2 via email. SIR submitters must submit SIRs to C2 within one hour of the occurrence or discovery of the incident.

The SIR form can contain information about federal employees, contractors, and members of the public. The SIR submitter provides basic contact information on the SIR Form including, his or her name, work phone number, location, and e-mail address. The form also contains a free-text section for the submitter to describe the incident in detail. The SIR form specifically states that OSI encourages the SIR submitter to provide the least amount of personally identifiable information (PII) as possible. OSI does not require SIRs to include PII unless Directive 252-06 requires submission to the NOC. For example, in a facilitated apprehension, Directive 252-06 requires DHS components to submit reports to the DHS NOC with additional identifying information.

DHS Directive 252-06

All DHS components are required to comply with DHS Directive 252-06, which establishes DHS's operational reporting requirements for incidents. DHS components must report various incidents to the DHS NOC on a daily basis. The DHS NOC serves as the primary national-level hub for domestic situational awareness, a common operating picture, information fusion, information sharing, communications, and operations coordination pertaining to the prevention of terrorist attacks and domestic incident management.

DHS Directive 252-06 requires that DHS components report incidents that fall into the Directive's criterion in an Operational Summary report (OPSUM). An OPSUM includes the components' daily, scheduled, operational report covering the previous 24-hour period. It typically contains summaries of several independent incidents/events that occurred within the scope of the component's jurisdiction over the 24-hour reporting period.

The Directive requires that DHS components report on incidents including, but not limited to, arrests that occur on DHS property, when DHS encounters an individual with a warrant out for his or her arrest, lost or stolen DHS credentials, and/or any event that may cause significant media attention. Furthermore, pursuant to the Directive, DHS components must submit each incident listed in its OPSUM with a geographical reference. The geographic reference must include where the incident occurred by providing one of the following references: the address, intersection, city and state, global positioning System (GPS) coordinates, or compass driving directions in relation to a DHS facility (e.g., 3 miles Northeast of the USCIS facility Vermont Service Center). The DHS NOC uses the OPSUMs for situational awareness and to include in the DHS Headquarters leadership briefings.

Previously, OSI C2 employees handled incident mitigation and reporting through email communication and stored incident data in Microsoft Word or Excel documents on local shared drives. Since the SIR submitter varies by incident, submitters received an overwhelming amount of data calls from C2, which often results in missing and untimely information. This was a time consuming and burdensome process. To more effectively manage SIRs and to comply with Directive 252-06, OSI developed GeoSpace. GeoSpace uses Geographic Information System (GIS) software to organize and visualize the USCIS incidents in geospatial terms.[3] GIS integrates data to manage, analyze, and display the incidents with a geographic reference to understand, interpret, and visualize the incidents in ways that may reveal incident relationships, patterns, and trends. GeoSpace greatly reduces the data calls and increases timely availability of required data when necessary. It also allows OSI to collect and respond to incident reports to efficiently restore normal operations and minimize the impact of business operations.

GeoSpace allows OSI to manage the SIRs reporting process and organize and visualize incident data in geographic terms. This allows USCIS to more effectively and efficiently manage SIRs and fulfill the geographic reference reporting requirement outlined in DHS Directive 252-06.

GeoSpace

GeoSpace is a web-based incident management tool that collects and reports information related to incidents that occur within and around USCIS buildings both domestically and internationally. In order to manage, track, and receive information on incidents that occur at USCIS facilities, GeoSpace uses ArcGIS, DHS's primary GIS software, as well as a centralized data repository from the Homeland Security Infrastructure Program (HSIP).

ArcGIS provides USCIS with the ability to view, query, and create maps, view and perform spatial analysis, data analysis, and near real-time interactive data-sharing.

GeoSpace receives geospatial information from DHS OneView, a geospatial visualization application that receives its foundational dataset by the HSIP. HSIP is an infrastructure geospatial data inventory that represents the 16 critical infrastructure sectors, national hazards, and base map layers. HSIP compiles geospatial data from federal agencies, commercial vendors, state, and local partners (for common use by the Homeland Security; Homeland Defense; and Emergency Preparedness, Response, and Recovery communities). These datasets allow for nationwide infrastructure information access to assist decision makers in analyzing threats (whether natural or manmade) and modeling for emergencies and other missions. The collaboration between ArcGIS and HSIP turns incident data into actionable knowledge and allows USCIS to analyze the dynamics of an incident to make informed decisions and operational adjustments in the future, to identify and examine suspicious activity and threats, and to perform resource analysis and allocation.

With the implementation of GeoSpace, once OSI C2 receives a SIR, they manually input the information into GeoSpace. GeoSpace has a built in SIR module with specific data fields that prompts OSI to provide an explanation of the incident that occurred. After the C2 inputs the incident, they place a geographical reference with the incident.

[3] The term geospatial means anything that has a geographic location on earth.

Once C2 enters the SIR into GeoSpace, OSI reviews it for accuracy, situational awareness, and follow-up with the SIR submitter, if necessary. OSI then refers the incident to relevant USCIS offices that may assist in resolving the incident. For example, OSI may contact the USCIS Office of Privacy if the incident is privacy-related; the Protective Intelligence Branch within OSI if an incident involves suspicious criminal or terrorist activity; or the Asset Management Branch if the incident involves lost or stolen government property. OSI ultimately closes or refers cases for follow up to local OSI personnel.

OSI consolidates information from GeoSpace into a SIR and sends them to USCIS leadership and the DHS NOC on a daily basis. As discussed above, both USCIS leadership and the DHS NOC use these reports for situational awareness. USCIS leadership primarily uses these reports for situational awareness and to gain a general understanding of what is occurring on a daily basis in USCIS facilities, both domestically and internationally. USCIS leadership may use this information to determine how to mitigate future incidents or identify patterns and trends. The DHS NOC will use the reports to provide DHS headquarters leadership with a general understanding of incidents that are occurring and impacting DHS operations.

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 legal authority for the operation of the GeoSpace system derives from the Homeland Security Act of 2002, 6 U.S.C. § 112, DHS Directive 252-06, and DHS Delegation 12000. DHS Directive 252-06 authorizes DHS components to collect incident information that must be reported to the DHS NOC. DHS Delegation 12000 grants DHS components the authority to fulfill security operations for its respective component.

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

The GeoSpace application is covered by the following SORNs:

- DHS/ALL-006 - Department of Homeland Security Accident Records, November 25, 2008, 73 FR 71661;
- DHS/ALL-010 - Department of Homeland Security Asset Management Records, October 23, 2008, 73 FR 63181;
- DHS/ALL-024 - Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, February 3, 2010, 75 FR 5609;
- DHS/ALL-025 - Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security, February 3, 2010, 75 FR 5614.

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

A system security plan is currently in development. Once complete, GeoSpace will be issued an Authority to Operate (ATO).

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

The NARA approved schedule [N1-566-11-01], permits USCIS to retain information relating to incidents in and around all USCIS buildings and facilities. This schedule was approved on September 19, 2011. Under the agreement, SIRs within GeoSpace are destroyed after five years.

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.

GeoSpace is not subject to the requirements of the PRA.

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.

GeoSpace maintains information on incidents that occur in and around USCIS facilities and buildings. The information that OSI inputs into GeoSpace derives from the SIR Form and any relevant follow up information. OSI encourages the SIR submitter to provide the least amount of PII as possible. In fact, OSI does not require the SIR submitter to provide any PII unless the incident is one of the incidents DHS components must report to the DHS NOC pursuant to Directive 252-06.

If the SIR submitter provides any PII, he or she generally only provides his or her contact information. However, there may be instances when he or she chooses to provide more information in the free-text field of the SIR Form. For example, for incidents that provoke media attention, relate to physical security, or that may involve an injury to a USCIS employee or the public (while on UCIS property), the SIR may collect contact information on employees/contractors and the public involved in the incident and a description of what occurred. OSI will collect this information for the purposes of following up with the individual involved.

GeoSpace may capture contextual information about the individual in relation to the particular incident in the free-text field, some of which may be sensitive. For example, for persons injured on an USCIS facility, the systems may record the type of injury suffered (e.g., broken leg) and the details of the event itself.

While OSI does not have the authority to arrest individuals, they may assist other law enforcement agencies in facilitating arrests. When members of the public come to USCIS facilities to seek a benefit, USCIS may determine through a background check that the individual has an immigration violation or has a warrant out for his or her arrest. If this occurs, OSI contacts the DHS Immigration and Custom Enforcement (ICE), to apprehend the individual. OSI creates a SIR containing employee contact information, a description of the incident, and identifying information about the individual and apprehension to include in the report to the DHS NOC. DHS Directive 252-06 requires DHS components to collect and report this information to the DHS NOC in a daily OPSUM whenever a component apprehends an individual. USCIS does not use this information for any reason other than reporting to the DHS NOC.

The following describes the information that OSI may collect in a SIR and input into GeoSpace:

<u>From employees/contractors:</u>

- First and Last Name;
- Agency/Office;
- Telephone Number/Government Email Address; and,
- Nature of Incident (may include sensitive information depending on incident type).

<u>From the public (for typical incidents):</u>

- First and Last Name;
- Reason for being in facility;
- Escort Office;
- Government Employee involved; and,
- Telephone number, if needed for follow up.

<u>From the public (when the incident involves a facilitated apprehension):</u>

- First and last name;
- Date of Birth;
- Alien number;
- Country of citizenship;
- Country of birth;
- Reason for visit in USCIS Facility;

- Warrant type (e.g.; Federal, state or local); and,
- Reason for apprehension.

In addition to collecting PII from persons involved with the incident, OSI may collect pictures relating to the incident and retain them in the GeoSpace. Additionally, if the media reports on an incident, OSI personnel may collect media reports and retain them in GeoSpace with the SIR for documentation purposes. The media report may contain elements of PII.

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

OSI personnel draft and submit SIRs to GeoSpace. To the extent possible, OSI personnel collect information directly from the individuals involved in the incident. This includes federal employees, contractors, and members of the public (e.g., building occupants and visitors) who are victims, witnesses, or participants in an incident. Federal, state, or local police officers who also respond to or assist with the event may also provide information. C2 personnel then manually input information from the SIR into GeoSpace.

GeoSpace receives geospatial information via DHS OneView from the HSIP, an infrastructure geospatial data inventory. HSIP compiles geospatial data from federal agencies, commercial vendors, state, and local partners. These datasets allow for nationwide infrastructure information access to assist decision makers in analyzing threats and modeling for emergencies and other missions. HSIP is composed of two datasets, HSIP Gold and HSIP Freedom.

The National Geospatial-Intelligence Agency (NGA) assembles the HSIP Gold database in partnership with the Homeland Infrastructure Foundation-Level Data (HIFLD) Working Group[4] for use by Homeland Defense (HD), Homeland Security (HLS), and National Preparedness Prevention, Protection, Mitigation, Response, and Recovery communities. It is a compilation of approximately 475 geospatially-enabled baseline infrastructure data sets assembled from federal, state, local government, and private sector mission partners. HSIP Freedom, led by DHS, is a license-free subset of HSIP Gold. These datasets assist mission partners with planning, situational awareness, threat and impact analysis (natural or manmade), modeling emergencies, protection of borders, and decision making during response and recovery operations.

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

If the media reports on an incident, OSI may collect relevant news from the media and retain it in GeoSpace with the SIR for documentation purposes. GeoSpace may retain this information with the report in order to give leadership a comprehensive look at the incident that occurred.

[4] The HIFLD Working Group was established in February 2002 to address desired improvements in collection, processing, sharing, and protection of homeland infrastructure geospatial information across multiple levels of government and to develop a common foundation of homeland infrastructure data to be used for visualization and analysis on all classification domains.

Additionally, the HSIP compiles geospatial data from many sources, including commercial vendors to show a comprehensive infrastructure map.

2.4 Discuss how accuracy of the data is ensured.

OSI collects information directly from the subjects of incidents (e.g., suspects, victims, witnesses, participants, employees, and building occupants and visitors) to ensure accuracy. OSI supervisors review all submitted reports for accuracy, awareness, and follow-up, if necessary.

If OSI assists in facilitating an apprehension, OSI inspects the individual's identification or other documents against information maintained by other law enforcement agencies in the event there is an associated investigation of another incident.

Furthermore, if OSI discovers additional information after a SIR submission, they can update the SIR with the new information. However, OSI retains all of the submitted information, regardless of whether or not OSI later deems the information is a fallacy. If new information is discovered that corrects the inaccuracies of previously submitted information, OSI will note that in the file.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk associated with the accuracy of data GeoSpace maintains. Although OSI collects information directly from the individual, it is possible for OSI personnel to enter data inaccurately. For example, "Jane Smith of USCIS" states that "John Doe" pulled the fire alarm at 2pm on Friday. However, later USCIS OSI in conjunction with state and local law enforcement identified the perpetrator as "John Smith."

Mitigation: USCIS mitigates this privacy risk by allowing OSI personnel to update SIRs in GeoSpace to correct any inaccurate, erroneous, or incomplete information. While OSI does not delete inaccurate, erroneous, or incomplete information in GeoSpace, OSI can update SIRs to note the inaccurate information and include the correct information. Additionally, OSI ensures that SIRs accurately describe the incident by having a supervisor review it to ensure the information is relevant prior to the entry of information into GeoSpace.

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.

The primary purpose of GeoSpace is to consolidate SIRs into a central location for C2 to disseminate them to USCIS and the DHS NOC in a daily OPSUM. OSI may use the information to perform necessary follow-up actions. For example, OSI may use an internal investigation to track the rate of incidents at USCIS facilities; inform other branches within OSI of security decisions; and assist in similar incidents that may occur at another facility in the future.

OSI may also disseminate SIRs to appropriate offices throughout USCIS that have a valid need-to-know. For example, an incident may occur that meets the criteria of a DHS Suspicious Activity Report (SAR).[5] A SAR is an "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." If C2 receives a SIR that meets the criteria of a SAR, OSI does not process it as a SIR. Instead, OSI contacts the Protective Intelligence Branch for handling SARs, which then assumes responsibility of the SAR. Another example is if the SIR is a privacy incident involving stolen, lost or damaged data, or PII. If this occurs, C2 contacts the USCIS Office of Privacy Incident Management Team to process the incident for follow up and mitigation. Once the Office of Privacy resolves the privacy incident, it notifies C2, which ultimately closes the case in GeoSpace. Lastly, C2 may contact USCIS Asset Management Branch if the incident involves lost, stolen, or damaged government equipment. If this occurs, the Asset Management Branch mitigates the issue and C2 closes the case.

OSI consolidates the information in GeoSpace into a report and provides it to USCIS leadership. USCIS leadership uses the reports for situational awareness and to gain a general understanding of what is occurring on a daily basis in USCIS facilities, both domestically and internationally. Additionally, the reports may assist in determining how to mitigate future incidents or identify patterns and trends

OSI also consolidates the information in GeoSpace into an OPSUM for the DHS NOC. The DHS NOC uses OPSUMs for situational awareness and to gain a general understanding of what is occurring on a daily basis within DHS components.

Furthermore, USCIS may share the information contained in GeoSpace to external agencies that have a valid need-to-know, when approved by the Chief of the DHS/Office of the Chief Security Officer (OCSO), Physical Access Security Division (PHYSD), and supervisory OSI personnel.

OSI shares incident reports with USCIS leadership, the DHS NOC and security personnel only through email or hard copy printouts. OSI transmits the information only by secure means, such as hand delivery with signature by the receiving agency employee, by facsimile, or registered mail.

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.

The predictive analytical capabilities of GeoSpace are limited to the HSIP datasets such as infrastructure, weather, jurisdictions, etc. For example, OSI uses GeoSpace to determine if there is a pattern in incidents that occur to better prepare for future incidents or to prevent incidents from reoccurring. OSI does not use GeoSpace to discover or locate a predictive pattern or anomaly regarding the PII collected for SIRs.

[5] For more information on SARs, please review the DHS/ALL/PIA-032 DHS Information Sharing Environment Suspicious Activity Reporting Initiative at www.dhs.gov

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

No other DHS components have a role or responsibilities within GeoSpace. However, USCIS may share GeoSpace information with other USCIS program offices and directorates and DHS HQ for reporting, investigatory, evidentiary, prosecutorial, or for civil proceedings purposes.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of misuse or unauthorized access to the information.

Mitigation: To mitigate this risk, all actions within GeoSpace are subject to an audit. The system tracks what is done, when it was done, and by whom. The system creates an audit trail that tracks users who access a record, the time of access, and any changes made to the record. This would enable a system administrator to reconstruct the actions of a user.

Privacy Risk: There is a privacy risk that USCIS uses GeoSpace for purposes outside the scope of this PIA.

Mitigation: OSI only uses GeoSpace to track and manage significant incidents that occur in and around USCIS domestic and international facilities. USCIS OSI reports incidents as a SIR in GeoSpace and then creates reports for both USCIS leadership and the DHS NOC. Per DHS Directive 252-06, DHS components are required to report incidents with a geographic reference. OSI only uses the geographic feature of GeoSpace to track and report incidents to USCIS and DHS NOC. If USCIS were to use GeoSpace for any purpose outside the scope of this document, USCIS will update this PIA.

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.

The publication of this PIA and the System of Records Notices (SORN) for the DHS/ALL-006, DHS/ALL-010, DHS/ALL-024, and DHS/ALL-025 provide general public notice of the collection of this information. When OSI obtains information through victims, witnesses, participants, employees, and building occupants and visitors, they are given notice that any information they provide in the interview is retained for reporting purposes. OSI works with the individuals to get a description of the incident and completes a SIR on behalf of the individuals. Formal written notice is not provided to individuals (involved in an offense/arrest) at the point of collection of this information because of the law enforcement context in which it is collected. However, in some instances, providing notice to individuals interferes with ability to carry out an OSI mission by potentially frustrating the confidential nature of its investigations, methods, or sources.

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

Individuals generally provide information to OSI on a voluntary basis. However, the following describes the consent by individual:

Employees/Contractors: SIR submitters submit a SIR when an incident occurs. The SIR submitter provides notice to the employees and contractor that the information they provide is included in a SIR for reporting purposes. Additionally, if OSI interviews employees/contractors and asked the employees/contractors to provide a statement to OSI about an incident, they may opt-out of providing information.

The public: The public can opt-in or opt-out of providing PII or a description of the incident. However, if they opt-in to providing the report, OSI verbally notifies them that their statement and any PII they share may be included for reporting purposes.

The public (when facilitating an apprehension): OSI requests individuals suspected of committing an offense to provide information pertaining to their identity. Because these individuals may decline to provide further information, their PII may not be included in a SIR or GeoSpace. However, OSI creates a SIR discussing the incident and that the apprehension is now the responsibility of the appropriate law enforcement agency.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a possibility that an individual is not aware that USCIS is collecting his or her information.

Mitigation: The notice USCIS provides to individuals varies depending on from whom OSI is collecting information.

Employees/Contractors: OSI provides employees/contractors notice that the information they provide is being included in a SIR for reporting purposes.

The public: If OSI requests a statement about an incident from the public, OSI verbally tells them that their information is included in a SIR for reporting purposes.

The public (when facilitating an apprehension): Individuals who DHS apprehends at a USCIS facility may not be notified that their information is being collected. Providing notice to individuals may interfere with ability to carry out OSI mission by potentially frustrating the confidential nature of its investigations, methods, or sources.

Additionally, this PIA, the DHS/ALL-006, DHS/ALL-010, DHS/ALL-024, and DHS/ALL-025 SORNs provide notice of the collection of information from all individuals.

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.

NARA approved a records retention schedule for GeoSpace on September 19, 2011. The retention schedule [N1-566-11-01] states that SIRs are destroyed after five years. This five-year retention schedule is based on the operational needs of the Department.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a possibility that USCIS will retain information for longer than necessary.

Mitigation: Although there is always risk inherent in retaining PII for any length of time, the data retention period for the GeoSpace System is based on case type identified in the NARA retention schedule and is consistent with the concept of retaining PII only for as long as necessary to support the agency's mission. GeoSpace retains information for five years to allow OSI to perform necessary follow-up actions such as an internal investigation, track the rate of incidents at USCIS facilities, and inform OSI personnel of security decisions made to assist in similar incidents that may occur in the future.

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.

OSI disseminates SIRs outside of DHS strictly on a need-to-know basis. In the event that USCIS facilitates an apprehension, OSI may share information with law enforcement. USCIS may share information with DHS law enforcement agencies or external law enforcement organizations for reporting, investigatory, evidentiary or prosecutorial purposes, or for civil proceedings. Recipient agencies may include INTERPOL, the U.S. Department of Justice, and state and local law enforcement agencies.

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

External sharing is consistent with the original collection of information, specifically the reporting of incidents so that they may be further investigated. The SORNs that permit the collection and disclosure of this information are the SORNs DHS/ALL-006, Department of Homeland Security Accident

Records, DHS/ALL-010 - Department of Homeland Security Asset Management Records, DHS/ALL-024 - Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, and DHS/ALL-025, Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security. Each SORN has routine uses allowing USCIS to share the information for law enforcement, criminal, and civil litigation purposes. Routine Use A states that information can be shared externally to the Department of Justice (including U.S. Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body when it is necessary to the litigation under certain situations. Routine Use G states that this information can be shared with an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

6.3 Does the project place limitations on re-dissemination?

Recipient agencies cannot re-disseminate information outside of its agency unless authorized by USCIS. If the information is shared, external organizations secure SIRs in accordance to the terms of information sharing agreements, which include provisions for appropriate and adequate safeguarding of sensitive information and restrictions on re-dissemination.

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

External organizations secure SIRs in accordance to the terms of information sharing agreements, which include provisions for appropriate and adequate safeguarding of sensitive information and restrictions on re-dissemination.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a potential risk of receiving agencies leaking, misusing, or losing SIRs.

Mitigation: OSI narrowly tailors the distribution list of external entities that receive SIRs to include only agencies that have a need-to-know. No external organizations have individual user accounts, and therefore do not have direct access to the GeoSpace. Any external sharing is consistent with the routine uses listed in the DHS/ALL-006, DHS/ALL-010, DHS/ALL-024, and DHS/ALL–025 SORNs.

Privacy Risk: There is a potential risk that receiving agencies further disseminating SIRs.

Mitigation: When OSI distributes a SIR it clearly labels this information as sensitive information. Receiving agency personnel have been trained on proper use of sensitive information and understand that they may only provide the information to those who have a need to know.

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 seeking access to any record containing information that is part of a USCIS system of records, or seeking to contest the accuracy of its content, may submit a Freedom of Information Act (FOIA) or Privacy Act (PA) request to DHS. Given the nature of some of the information in the GeoSpace System (relating to an incident and offenses/arrests), USCIS may not always permit the individual to gain access to or request amendment of his or her record. However, requests processed under the PA are also processed under FOIA; requesters always receive the benefit of the statute with the more liberal release requirements. The FOIA does not grant an absolute right to examine government documents; the FOIA establishes the right to request records and to receive a response to the request with non-exempt records. Instructions for filing a FOIA or PA request are available at uscis.foia@dhs.gov.

The FOIA/PA request must contain the following information: Full Name, current address, date and place of birth, telephone number, and email address (optional). Privacy Act requesters must either provide a notarized and signed request or sign the request pursuant to penalty of perjury, 28 U.S.C. § 1746. Please refer to the USCIS FOIA website for more information.

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

If an individual believes that he or she has suffered an adverse consequence that is related to GeoSpace, the individual is able to provide any information that he or she deems relevant with a request that it be included within any record maintained in the GeoSpace System regarding a particular incident, activity, transaction, or occurrence. OSI C2 handles all correspondence and researches GeoSpace to ascertain whether any record correlates to the information provided. If there is correlative information, the OSI personnel enters the information provided into that record and marks it as first-party amplifying[6] information.

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

Mechanisms for correcting information are set forth above, as well as the DHS/ALL-006, DHS/ALL-010, DHS/ALL-024, and DHS/ALL-025 SORNs.

[6] First-party amplifying information means any material that is provided by a subject involved in the incident that adds value to the incident report.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that USCIS may not afford an individual adequate opportunity to correct information that USCIS maintains.

Mitigation: To mitigate this risk, USCIS affords individuals the opportunity to request access or amendment to their records by either submitting a FOIA or a PA request as outlined above.

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?

Privacy protections include strict access controls, including passwords and real-time auditing that tracks access to GeoSpace. Authentication and role-based user access requirements ensure that users only can access or change information that is appropriate for their official duties. USCIS conducts background checks on users to ensure they are suitable for authorized access to USCIS systems. The effectiveness of authentication and security protections are verified through audits of system operation and usage. USCIS employees may be subject to discipline and administrative action for unauthorized access and disclosure of this information.

Additionally, all actions within GeoSpace are subject to an audit. The system tracks what is done, when it was done, and by whom. In addition, GeoSpace maintains a record of changes that enables a system administrator to reconstruct the actions of a user.

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

All GeoSpace users complete annual privacy training to ensure they properly handle PII. After an initial training, all USCIS personnel must complete an annual refresher training, specific to their security and privacy responsibilities.

USCIS maintains training records, including name and position, type of training received, and costs of training. USCIS requires IT security and privacy awareness training before authorizing IT accounts.

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

Access to GeoSpace is granted to USCIS employees who are the business owner of a specific SIR dataset, such as a specific Field Office. For example, the New York District Director is the business owner for his or her region. As the business owner, he or she determines who has access to GeoSpace, such as their SIR submitter. Business owners only grant access to those who have a need-to-know.

Privacy protections include strict access controls, including passwords and real-time auditing that tracks access to electronic information. Authentication and role-based user access requirements ensure that users only can access or change information that is appropriate for their official duties. Background checks are conducted on users to ensure they are suitable for authorized access to the SIRs. The effectiveness of authentication and security protections are verified through audits of system operation and usage.

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?

Because OSI does not routinely share SIR information outside of DHS, no MOUs are in place. However, the USCIS program manager, Office of Privacy, counsel, and the DHS Privacy Office reviews any external routine information sharing agreements prior to disseminating any information.

Responsible Officials

Donald K. Hawkins
Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

____

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

Appendix A: Types of Significant Incidents

The following types of incidents must be reported to C2 as a SIR, as required by local, USCIS, and DHS management directives. This list includes only mandatory reportable items and is not all inclusive. SIRs that are submitted outside of the mandatory reporting requirements are reviewed but may not be entered into GeoSpace.

- Any incident that interrupts USCIS Operations;
- Arrest/Detention of Person within USCIS Space (warrant, detention, removal, etc.);
- Building/USCIS Office Evacuation (for any reason);
- Civil Disorder (riot, demonstration, or general civil disorder affecting USCIS operations);
- Continuity of Operations activation;
- Death or serious injury of employee/visitor in USCIS space;
- Emergency Medical Service response;
- Explosion of any type affecting USCIS operations;
- Fires/fire alarm within USCIS Space;
- Mishandling, improper destruction, and/or data loss;
- Loss of Service (power, water, information technology);
- Loss/Theft of Government Property;
- Loss/Theft of IT Equipment;
- Loss/Theft of Sensitive Property;
- Loss/Theft of Badges and Credentials;
- Mail Room incident;
- Missing/Kidnapped employee (Domestic & International Operations);
- Office closing (include expected time of reopening);
- Other issue related to building damage;
- Shelter-in-Place situation;
- Suspicious activity potentially affecting USCIS;
- Suspicious package (other than Mail Room);
- Threat (bomb or other, whether verbal, written, telephone, email) to any U.S. Government Operation, Facility, or Person (including contractor); and,
- Weather-Related emergency affecting office operations (severe winter storm, hurricane, tornado, flooding, etc.).