Privacy Impact Assessment
for the

CBP Situation Room (SITROOM)

DHS/CBP/PIA-039

February 27, 2017

Contact Point
Sergio Echazarreta
Acting Director - CBP Situation Room (SITROOM)
U.S. Customs and Border Protection
(202) 344-3926

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

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) Situation Room (SITROOM) is a 24-hour operations center staffed by CBP personnel who manage significant incident reporting and information coordination for the CBP Commissioner and senior leadership team. The SITROOM also serves as CBP's primary conduit of information to the DHS National Operations Center (NOC). The SITROOM uses the Significant Incident Reporting System (SIR) web-based application to report law enforcement, national security, or other significant incidents to senior CBP leadership. CBP is conducting this Privacy Impact Assessment (PIA) because the SITROOM uses personally identifiable information (PII) about members of the public in its significant incident reporting activities.

Overview

The CBP Situation Room (also known as the "Commissioner's Situation Room" or "SITROOM") serves as CBP's around-the-clock reporting and information coordination center. The SITROOM is staffed by CBP Officers/Agents and facilitates communication between CBP Headquarters and field operational offices by serving as a conduit for reporting law enforcement, national security, and other significant incidents. The SITROOM also serves as the primary conduit for communications between CBP and the DHS NOC and other federal agency operations centers.

The SITROOM is located in CBP Headquarters and is a 24 hours a day, 7 days a week incident notification and information coordination center. The SITROOM is the primary point of contact for significant incident reporting from all CBP operational components and offices, including ports of entry, sectors, stations, air and marine branches, international offices, and CBP Headquarters. The SITROOM collects CBP component and offices' reports to provide complete, accurate, and timely reporting to the Commissioner, Deputy Commissioner, and CBP senior management.

The SITROOM provides connectivity to the DHS NOC and other agencies on significant CBP events. The SITROOM serves as an information coordination center during times of national incidents, such as disaster management, emergency management, or international events that require CBP support. The SITROOM also acts as the primary point of contact to receive and coordinate responses to DHS NOC requests for operational information.

Reportable Incidents

While it is difficult to provide an all-inclusive list of the types of incidents, events, or issues that could be encountered and should be reported, the following types of significant incidents require a significant incident report be reported to the SITROOM (see Appendix A for a detailed description of each type of reportable incident):

1. Terrorist Related-Events
2. Weapons of Mass Destruction

3. Public Health
4. Arrests
5. Seizures
6. Incidents Involving Employees
7. Detection Events
8. Discharge of Service Issued Weapons
9. Incidents Involving Subjects Encountered by CBP
10. Agriculture Related-Events
11. Facility and Technology Disruptions
12. Any Incursion of the U.S. Border
13. Air and Marine Events

Reporting Procedures

CBP requires immediate telephonic notification to the SITROOM for all CBP events related to "reportable incidents." Initial reports should include as much concise detail as available to describe the incident that is being reported. This information should include relevant facts including: location of incident, time of incident, individuals involved, actions taken, impact on CBP operations, and the possibility of media attention.

Each reportable incident will be accompanied when possible by a GPS coordinate in latitude and longitude format of degrees/minutes/seconds indicating the exact location of the incident geographically. For example, at and between ports of entry, the GPS should reflect the actual physical location where the incident occurred (e.g., lane three on bridge two at a port of entry or lane one at a Border Patrol checkpoint), not a single GPS for an entire facility. As applicable, this reporting shall be in a format consistent with existing geo-tracking capabilities utilized by operational components.

When the SITROOM receives an initial incident report, a significant incident report is generated by a SITROOM analyst in the SIR system and sent to a manager in the field for completion. The manager in the field pulls information from his or her source systems to populate the significant incident report. The SITROOM then reviews the report from the field for accuracy by comparing the information in the report to information in source systems. The SITROOM may also search publicly available social media for situational awareness related to the specific incident.[1] The type of incident and gravity of the situation will determine the course of action of either notifying CBP leadership by immediate telephonic notification or by email.

[1] Further explanation of how SITROOM analysts utilize publicly available social media for situational awareness can be found in Section 2.3 of this PIA.

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?

CBP's authority to collect information on significant incidents is derived from a number of sources, including but not limited to:

- 6 U.S.C. § 202;
- 6 U.S.C. § 211;
- Homeland Security Presidential Directive (HSPD)-5 (February 28, 2003), which requires all Federal departments and agencies to adopt National Incident Management System (NIMS) information sharing standards to effectively and efficiently prepare for, respond to, and recover from domestic incidents; and
- CBP's general authority under the Immigration and Nationality Act, the Tariff Act of 1930, as amended.

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

CBP is publishing a new System of Record Notice (SORN) in the Federal Register to provide notice of the information CBP maintains as part of its SITROOM operations, named the CBP Intelligence Records System (CIRS).[2]

In addition, the DHS Office of Operations, Coordination, and Planning (OPS) is responsible for sharing information it receives from the SITROOM externally pursuant to DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records.[3]

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

Yes. SIR is a sub-system to the Enforcement Support System (ESS), which received an Authority to Operate (ATO) on April 12, 2016, and will receive a new ATO upon publication of this PIA and the forthcoming CIRS SORN.

---

[2] CIRS contains information generated, received, or collected by the CBP Office of Intelligence, or other offices within CBP that support the law enforcement intelligence mission, that is analyzed and disseminated to CBP executive management and operational units for law enforcement, intelligence, counterterrorism, and other homeland security purposes. CIRS contains data from a variety of sources within and outside of CBP to support law enforcement activities and investigations of violations of U.S. laws, administration of immigration laws, and other laws administered or enforced by CBP, and production of CBP law enforcement intelligence products.

[3] *See* DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records, 75 FR 69689 (November 15, 2010), *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-11-15/html/2010-28566.htm.

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

Yes. The SITROOM will follow the DHS records schedule for situational awareness reports:

1. Awareness Reports (Disposition Authority Number DAA-0563-20 13-0002-0001) – Records regarding information on emerging or potential significant incidents or events with possible operational consequences to offices or citizens must be retained for six (6) years. These include reports and updates which outline the real or perceived dangers to areas affected by disaster(s); or which are used to identify, detect, and assess actual and potential vulnerabilities and threats to the homeland. These records may include records pertaining to law enforcement activities. However, incidents of National Significance will be included in the Secretary's Briefing Book(s), and are retained according to N1-563-07-013 Item 2.
2. Suspicious Activity Reports (Disposition Authority Number DAA-0563-20 13-0002-0002) – Official documentation or observed behavior compiled by one or multiple sources and submitted to the Nationwide Suspicious Activity Reporting Initiative (NSI) that is reasonably indicative of pre-operational planning related to terrorism or other criminal activity related to terrorism must be retained for five (5) 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.

The information collected as part of this initiative is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

Due to the fluid nature of situational awareness reports, the SITROOM and SIR may include information about any individual about whom CBP has authority to collect information, and who is involved in a reportable incident (see Appendix A). Typical data elements collected include, but are not limited to:

- Full name;
- Date and place of birth;
- Citizenship;

- Contact information, including phone numbers and email addresses;
- Address;
- Physical description including height, weight, and eye/hair color;
- Distinguishing marks including scars, marks, and tattoos;
- Automobile registration information;
- Watchlist information;
- Medical records;
- Financial information;
- Results of intelligence analysis and reporting;
- Ongoing law enforcement investigative information;
- Historical law enforcement information;
- Information systems security analysis and reporting;
- Public source data including commercial databases, social media, newspapers, and broadcast transcripts;
- Intelligence information including links to terrorism, law enforcement and any criminal and/or incident activity, and the date information is submitted;
- Intelligence and law enforcement information obtained from federal, state, local, tribal, and territorial agencies and organizations, foreign governments and international organizations; law enforcement, domestic security and emergency management officials; and private sector entities or individuals;
- Information provided by individuals, regardless of the medium, used to submit the information;
- Information obtained from the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC), or on terrorist watch-lists, about individuals known or reasonably suspected to be engaged in conduct constituting, preparing for, aiding, or relating to terrorism;
- Data about the providers of information, including the means of transmission of the data (e.g., when it is determined that maintaining the identity of the source of investigative lead information may be necessary to provide an indicator of the reliability and validity of the data provided and to support follow-on investigative purposes relevant and necessary to a legitimate law enforcement or homeland security matter, such data may likely warrant retention. Absent such a need, no information on the provider of the information would be maintained.);
- Scope of terrorist, law enforcement, or natural threats to the homeland;

- National disaster threat and activity information;
- The date and time national disaster information is submitted, and the name of the contributing/submitting individual or agency;
- Limited data concerning the providers of information, including the means of transmission of the data may also be retained when necessary. Such information on other than criminal suspects or subjects is accepted and maintained only to the extent that the information provides descriptive matters relevant to a criminal subject or organization and has been deemed factually accurate and relevant to ongoing homeland security situational awareness and monitoring efforts; and
- Name of the CBP employee submitting the significant incident.

The SIR application generates a daily report by compiling significant incident reports that are reported on a 24-hour basis and the report is shared with the DHS NOC. All PII is removed from the report and the document is marked as For Official Use Only (FOUO). If the DHS NOC requires access to the underlying PII from the daily reports, it must submit a Request for Information (RFI). The RFI is reviewed by SITROOM personnel and distributed to the corresponding CBP system owner that owns the source information. The system owner will then review the RFI and determine what information can be released to the DHS NOC, and then release it as appropriate. If the system owner determines that information is not appropriate to release, he or she must provide a justification and obtain concurrence from the CBP Office of Chief Counsel.

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

The SITROOM requires that CBP employees report incidents via telephone to the SITROOM as soon as possible. Any CBP employee may report an incident to the SITROOM. Reportable incidents are based on real-time events using information already collected by CBP under border security, law enforcement, or personnel management authorities. All information maintained by SIR is compiled by CBP employees from other databases and information collections. When the SITROOM receives an initial incident report via telephone, a significant incident report is generated by a SITROOM analyst in the SIR system and sent to a manager in the field for completion. The manager in the field pulls information from his or her source systems to populate the significant incident report.

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

Yes. CBP uses publicly available data from third-party social media sources to corroborate information from other official reporting channels or to report to the appropriate responding authority. SITROOM analysts use social media sources only as a situational awareness tool to amplify information on a significant incident received through initial reporting from CBP personnel.

The information SITROOM analysts use from social media sources is provided voluntarily by social media users. It is at the user's discretion to make this information available on a third-party social media site.

Consistent with the DHS policy for the operational use of social media, DHS Management Directive 110-01 *Privacy Policy for the Operational Use of Social Media*, CBP is conducting a Social Media Operational Use Template (SMOUT) in coordination with this PIA to assess the SITROOM's social media activities.

2.4 Discuss how accuracy of the data is ensured.

CBP employees must submit reportable incidents, as described in Appendix A, to the SITROOM consistent with CBP policy. Therefore, much of the information within SIR is provided directly by CBP employees with access to law enforcement or border security databases.

However, due to the real-time nature of evolving incidents, CBP expects that initial reports may not always be accurate. SITROOM analysts may rely on information from third-party social media services submitted voluntarily by users of those sites and compare it with information from a variety of public and government sources to confirm information contained in significant incident reports. SITROOM analysts attempt to provide a more accurate picture of on-the-ground activities by bringing together and comparing many different sources of information.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information maintained in SIR, or relied upon by the SITROOM, is inaccurate.

Mitigation: This risk is partially mitigated. CBP manages this risk by leveraging publicly available data posted on social media sources and news services, as well as a variety of traditional media and government sources to corroborate the information it receives. By bringing together and comparing many different sources of information, the SITROOM is able to provide a more accurate picture of significant incidents. While CBP strives to collect the most relevant and accurate information, there is always a risk that initial reports may not always be accurate due to the real-time nature of evolving incidents.

Privacy Risk: There is a risk that significant incident reports maintain more PII than is necessary to convey situational awareness to CBP leadership.

Mitigation: This risk is partially mitigated. Due to the fluid nature of situational awareness reports, the SITROOM and SIR may include information about any individual about whom CBP has authority to collect information, and who is involved in a reportable incident (see Appendix A). However, to mitigate the privacy risk of over-collection, the SITROOM minimizes information about all providers of information. The SITROOM only maintains information about the sources of reports if the identity of the source of investigative lead information may be necessary to provide an indicator

of the reliability and validity of the data provided. The SITROOM may also maintain such information to support follow-up investigations on law enforcement and/or homeland security matters. Information collected from publicly available sources or concerned citizens who contact the SITROOM telephonically will not include provider information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

SITROOM analysts compile information to: (a) pass to the DHS NOC for situational awareness, and (b) develop a daily briefing report of significant incidents for CBP leadership. CBP may collect the information listed in Section 2.1 to provide situational awareness that supports accurate and timely decision making. This operation is neither designed nor intended to collect PII as a regular function. Rather, the SITROOM collects information about reportable incidents, and may search publicly available sources and Internet-based platforms to understand the full scope of a situation.

CBP uses the collected information to remain advised in a timely manner of a situation that impacts border security. CBP may share critical, time-sensitive information from these efforts with federal partners as well as state, local, tribal, or territorial governments, via email, or in paper-based report form to facilitate appropriate action by an agency with authority to respond to an incident or emergency situation. Additionally, if there is an RFI, CBP may share operational information.

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.

No.

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

There is no access to SIR outside of CBP. A daily report of significant incidents is generated with all PII removed and is shared with the DHS NOC.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of inappropriate use or exploitation of PII related to CBP employees or incident subjects.

Mitigation: Users of SIR and SITROOM personnel are required to pass a background investigation before being granted access to the system, and access is restricted to the incidents they need in order to perform their duties. An audit log is used to track all system activity, including the

user, date/time of action, and what action was performed. Users are required to undergo and maintain current security and privacy training annually.

Access is strictly controlled by the SITROOM and access is given on a "need to know" basis to CBP Supervisors and Managers to generate significant incident reports. A quarterly review of access is conducted by the CBP Commissioner's Management Team.

Section 4.0 Notice

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

Reportable incidents maintained within SIR are based on information already collected by CBP under border security, law enforcement, or personnel management authorities. When appropriate, CBP provides notice to individuals at the time of collection. Notice at the time of collection is not always possible in a law enforcement or border security context.

All information maintained by SIR is compiled by CBP employees from other databases and information collections; no information is collected directly from a record subject. Therefore, CBP is providing notice in the form of this PIA and the forthcoming CIRS SORN. CBP includes information in SIR from other CBP databases pursuant to the 5 U.S.C. 552a(b)(1), "need to know" standard for intra-agency sharing. All reportable incidents are deemed "need to know" by CBP and DHS leadership.

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

Since reportable incidents may be law enforcement sensitive or indicative of a potential violation of law or policy, individuals who are subjects of significant incident reports do not have an opportunity to consent or opt-out of the collection.

In some instances, an individual has the right to decline providing PII at the time of collection, and he or she may have exercised this right. Reportable incidents are compiled from information that CBP already has in its databases, supplemented by any publicly available information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals whose data is included in SIR by CBP will not receive notice prior to the collection.

Mitigation: This risk is partially mitigated. When appropriate, CBP provides notice at the time of collection from individuals and employees. Regardless of the law enforcement or border security reasons for the information collection, CBP has published SORNs for all information types, available at https://www.dhs.gov/system-records-notices-sorns. This PIA also provides notice that

any information collected by CBP that meets the threshold of a reportable incident may be included in SIR.

Regarding information collected from social media or publicly available sources, SITROOM analysts will only monitor social media for situational awareness purposes and will only review publicly posted information. Social media users may change their privacy settings for their individual accounts or postings at any time, consistent with that website's policy. SITROOM analysts adhere to the CBP Social Media Rules of Behavior and adhere to all third-party social media site privacy policies.

Further, because SIR is a system to which many law enforcement contexts apply, notice or the opportunity to consent to use would compromise the ability of CBP to perform its missions and could put law enforcement officers at risk. Thus, notice of collection and consent to specific uses are not available in most cases for SIR.

Section 5.0 Data Retention by the project

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

As described above, the SITROOM retains situational awareness reports for six (6) years (DAA-0563-20 13-0002-0001) and Suspicious Activity Reports for five (5) years (DAA-0563-20 13-0002-0002).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is the risk that PII may be retained in the system for a longer period than is necessary for the purpose for which the information was collected.

Mitigation: This risk is partially mitigated. During the privacy impact assessment process, the CBP Privacy Office determined that the SITROOM minimizes PII to the extent possible in reports; however, the IT system has not purged records since its inception in 2006. The Office of Information Technology (OIT) has been given six months to delete records beyond their six year retention period and develop a technical solution to meet this retention requirement going forward. The CBP Privacy Office will ensure that this requirement is completed in the allotted timeframe.

Section 6.0 Information Sharing

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.

CBP may share critical, time sensitive information from these efforts with federal partners as

well as state, local, tribal, or territorial governments, via email or in paper-based report form to facilitate appropriate action by an agency with authority to respond to an incident or emergency situation. Additionally, CBP may share information in response to an RFI. Because SIR serves as the CBP conduit to the DHS NOC, the DHS NOC may also disseminate information contained in SIR outside of the Department. In that instance, DHS OPS is responsible for sharing information externally pursuant to DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records.[4]

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

CBP may share critical, time sensitive information from these efforts with federal partners as well as state, local, tribal, or territorial governments, via email or in paper-based report form to facilitate appropriate action by an agency with authority to respond to an incident or emergency situation. Additionally, CBP may share information in response to an RFI. SIR also serves as the CBP conduit to the DHS NOC. The DHS NOC may disseminate this information outside of the Department. In that instance, DHS OPS is responsible for sharing information externally pursuant to DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records.[5]

6.3 Does the project place limitations on re-dissemination?

The DHS NOC may disseminate information contained in SIR outside of the Department and is responsible for limitations on re-dissemination pursuant to DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records.[6]

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

The SITROOM maintains an electronic copy via email of all RFIs from DHS and other law enforcement agencies. Requests for information from other law enforcement agencies are routed through traditional channels within CBP back to the source system data stewards for assistance.

The DHS NOC may disseminate information contained in SIR outside of the Department and is responsible for maintain an accounting of disclosures pursuant to DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records.[7]

---

[4] *See* DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records, 75 FR 69689 (November 15, 2010), *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-11-15/html/2010-28566.htm.
[5] *Id.*
[6] *See* DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records, 75 FR 69689 (November 15, 2010), *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-11-15/html/2010-28566.htm.
[7] *Id.*

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information shared from the SITROOM or SIR database with an external partner will be further disseminated without CBP's consent.

Mitigation: This risk is mitigated by the fact that CBP places restrictions on re-dissemination of information from the SITROOM or SIR database. At the time the information is released, CBP authorizes the requestor only to use the information for the purposes already described, and only to share the information with other parties as already specified. CBP requires the recipient to request approval for any further re-dissemination not explicitly authorized in the initial release.

Section 7.0 Redress

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

Individuals may request access to records about them in SIR by following the procedures outlined in the forthcoming CIRS SORN. All or some of the requested information may be exempt from access pursuant to the Privacy Act (5 U.S.C. § 552a) in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in SIR could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

Individuals seeking notification of and access to any record contained in SIR, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

U.S. Customs and Border Protection

FOIA Division

1300 Pennsylvania Avenue, NW, Room 3.3D

Washington, D.C. 20229

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under *Contact Information*.

Requests should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request." An individual must first verify his or her identity,

meaning that he or she must provide full name, current address, and date and place of birth. The request must include a notarized signature or be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and FOIA, http://www.dhs.gov/foia or 1–866–431–0486. In addition, the following should be provided:

- An explanation of why the individual believes DHS would have information on him or her;
- Details outlining when he or she believes the records would have been created; and
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his or her agreement for access to his/her records.

Without this bulleted information, CBP may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

If individuals are uncertain what agency or system handles their information, they may seek redress through the DHS Traveler Redress Program (TRIP) (*See* 72 FR 2294, dated January 18, 2007), described below.

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

Individuals may seek redress and/or contest a record through two different means. Both will be handled in the same fashion. If the individual is aware the information is specifically handled by CBP, requests may be sent directly to CBP FOIA (via the procedures described above). If the individual is uncertain what agency is responsible for maintaining the information, redress requests may be sent to DHS TRIP at DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

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

CBP notifies individuals of the redress procedures for this initiative through this PIA and through the forthcoming CIRS SORN. In addition, DHS has provided redress procedures to the public pursuant to DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records[8] if an individual believes that his or her information was externally distributed inconsistent with the Privacy Act.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals are not aware of their ability to make record

[8] *See* DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records, 75 FR 69689 (November 15, 2010), *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-11-15/html/2010-28566.htm.

access requests for records in SIR.

Mitigation: This risk is partially mitigated. This PIA and the forthcoming CIRS SORN describe how individuals can make access requests under FOIA or the Privacy Act. Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

In addition, providing individual access and/or correction of SITROOM records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in SIR, regardless of a subject's citizenship, could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Section 8.0 Auditing and Accountability

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

The SIR application includes the following safeguards to prevent the misuse of data:

- Multiple concurrent active sessions for a user have been prevented by system security functions;
- Access privileges to SIR are deleted when the user no longer requires access to perform his or her job function;
- The system audit trail fully tracks the identity and activity of each person performing an action on the system, including the time and date of the access and logoff;
- The application software contains audit-logging routines that allow tracking activities of users that modify, bypass, or negate system security safeguards; and
- Data integrity controls (encryption, digital signatures) are used to ensure that tampering has not occurred with data transmitted and received.

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

Users of SIR and SITROOM personnel are required to take annual privacy, information security, and safeguarding national security information training prior to gaining and/or retaining access to the systems. If a user fails to complete the training by the annual deadline, then he or she loses access to the systems.

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 is requested by a Second Line Supervisor or higher depending on the level of access. Access is limited by Station, Port of Entry, U.S. Border Patrol Sector, or District Field Office, and must be granted by an approving official. National Level access is only authorized to SITROOM employees and Devolution site managers and must be approved by the Director of the CBP Commissioner's Situation Room. Access to the system is granted in one year increments and resets to no access after the access expires.

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?

All information sharing and MOUs concerning PII sharing, including those related to the SITROOM, are created by the operational owner of the system, are sent to the CBP Privacy Officer and Office of Chief Counsel for review, and to the DHS Privacy Office for final concurrence before approval and signing.

Responsible Officials

Sergio Echazarreta
Acting Director - CBP Situation Room (SITROOM)
U.S. Customs and Border Protection
(202) 344-3926

Debra L. Danisek
Privacy Officer
U.S. Customs and Border Protection
(202) 344-1610

Approval Signature

Original, signed copy on file with the DHS Privacy Office

_____

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

Appendix A: Reportable Incidents

While it is difficult to provide an all-inclusive list of the types of incidents, events, or issues that could be encountered and should be reported, the following types of significant incidents require a significant incident report be reported to the SITROOM:

1. Terrorist-Related Events

- The arrest, detention, parole, deferred inspection, or determination of inadmissibility by CBP personnel of any subject with a terrorist related record or suspected ties to terrorism. CBP operational components should file a significant incident report on encounters with known or suspected terrorists when the subject encountered is a non-resident alien AND is a positive match to a terrorist watchlist record (e.g., the Terrorist Screening Database (TSDB)), OR if routine enforcement activities disclose information potentially related to terrorism even if no watchlist record exists.
- CBP operational components are not required to file a significant incident report on encounters with known or suspected terrorists when the subject encountered:
    - is a U.S. citizen, National of the United States, or Lawful Permanent Resident, AND
    - is a positive match to a watchlist record (e.g., TSDB),

      UNLESS—
    - adverse action (e.g., arrest) and/or parole or deferred inspection of the individual is taken and/or the secondary examination of that individual did reveal additional potentially related terrorism information.
- Any bomb threat or other terrorist-related threat.
- Any discovery or seizure of currency, negotiable instruments, documents, passports, birth certificates, recorded media, printed matter, journals, writings, or any other items suspected of being possibly associated with a terrorist, terrorist-related activity, or organizations.
- Any seizure or arrest resulting from a coordinated CBP anti-terrorism enforcement action initiated from terrorist related intelligence or targeting effort.
- Any significant suspicious encounter or activity at or near any CBP operational component and/or office that involves law enforcement intervention or has potential international media interest.
- Absconders, stowaways, or arrests of Aliens from Special Interest Countries as identified by each office.
- Any other incident or activity not specifically addressed that, in the judgment of the

reporting supervisor, has the potential to contribute to the interagency effort to combat terrorism.

2. Weapons of Mass Destruction

   - Any CBP seizure, situation, incident, or other enforcement action associated with a potential Weapon of Mass Destruction (WMD). WMDs would include a chemical, biological, radiological, nuclear or explosive device, or a precursor or component of such a device.
   - Any detection incident when the CBP Office of Information Technology (OIT), Laboratories and Scientific Services Division (LSS) has determined that a radiation alarm warrants a request for response from the DHS Secondary Reachback program or the Department of Energy, consistent with CBP policy. In this instance, the operational component would file the significant incident report while LSS will be responsible for notifying the SITROOM of the DHS Secondary Reachback request.
   - Any intelligence information discovered or received indicating that a suspected terrorist, WMD or precursor component, or explosive device will enter or depart the United States by any means at a specific time or place--or that any dangerous device has been or will be placed at or near a CBP facility.

3. Public Health

   - Any admission or denial of admission of any person that is an exact match to a Centers for Disease Control and Prevention (CDC) public health-related lookout, or who in the judgment of CBP personnel is showing symptoms of a highly contagious and serious disease that requires public health notification.
   - Any refused entry or quarantine of any animal for showing signs or symptoms of a highly contagious disease requiring veterinary health notification.

4. Arrests

   - Arrest of a subject for a high profile crime that is the subject of media interest.
   - Any arrest involving a rescue. For the purposes of this directive, a rescue would be defined as when lack of intervention by a CBP officer or agent could result in imminent death or serious bodily injury.
   - Any arrest or detention of a high profile individual, dignitary, government representative, or official regardless of the charges.
   - Arrest of aliens with significant felony history of murder, forcible rape, arson, manslaughter, or other felonies related to sexual crimes.
   - Any arrests related to child pornography.

- Any arrest or detention of a member of a high profile gang or drug trafficking organization as listed in the Department of Justice's "Consolidated Priority Organization Target List."[9]

5. Seizures

- Seizure or extended detention of a foreign or domestic commercial passenger or cargo conveyance.
- Seizure or detention of any foreign government vehicle, aircraft, or vessel.
- Seizure of $100,000 or more in currency or negotiable instruments.
- Property seizures with a domestic value of $500,000 or more and issuance of penalties of $1,000,000 or more.
- Inbound or outbound stolen vehicles, vessels, or aircraft with an estimated total value of $100,000 or more.
- Discovery and/or seizure of weapons and/or ammunition.
- Discovery and/or seizure of illegal drugs if the seizure of illegal drugs meets and/or exceeds certain thresholds.
- Each seizure will be annotated as to the method of apprehension (e.g., cold hit, K-9 detection, TECS match, Vehicle and Cargo Inspection System) and how it was concealed. Seizures below the established thresholds should be reported when there is an unusual circumstance or other significance associated with the seizure, and/or the possibility of national and/or international media attention.

6. Incidents Involving Employees

- Death or serious injury of any CBP employee, any other individual, canine, or horse working directly with CBP either on- or off-duty. Serious injury for the purposes of this directive would be any injury that would require hospitalization.
- Assault of a CBP employee or any individual directly working with CBP during the performance of his or her duties or as the result of his or her position.
- Arrest, detention, incarceration, or indictment of a CBP employee or any individual directly working with CBP while on- or off-duty.
- Threats or allegations against or by a CBP employee, or any individual directly working with CBP, or their family as a result of their position.
- Any incident that involves the discharge of a firearm/weapon as an act of assault against any CBP officer, agent, or employee, and the assault is, or reasonably appears

[9] *See* https://www.justice.gov/criminal/organized-crime-drug-enforcement-task-forces.

to be, related to his or her CBP employment.

- Accident in a government conveyance that results in extensive property damage and/or results in serious injury to those involved.
- Accidental or intentional death or serious injury of an individual caused by any off-duty CBP employee.
- Lost or stolen government issued badge, credentials, or any government-controlled equipment that is considered sensitive in nature to the degree that CBP operations may potentially be impeded or compromised if lost or stolen (e.g., weapons, body armor, vehicles, radios, scopes).

7. Detection Events

- Detection of any cross-border tunnel.
- Detection of a significant concealed human smuggling attempt in a conveyance, including the trailer portion of a tractor trailer, rail car, aircraft, vessel, or air/sea cargo container.

8. Discharge of Service Issued Weapons

All firearms/weapons discharges, whether intentional or unintentional, must be reported as follows:

- While on-duty (except for intentional discharges which occur during firearms training, practice, or qualification, and do not cause any injury to a person or animal, or damage to private, public, or government property).
- While off-duty, and causes any injury to any person, or any damage to either private, public, or government property in violation of any law or ordinance, or results in an investigation by any law enforcement agency.
- Any incident that involves the discharge of a CBP-issued firearm/weapon, including by any person other than a CBP employee, and causes any injury to any person, or any damage to either private, public, or government property in violation of any law or ordinance, or causes an investigation by any law enforcement agency.

9. Incidents Involving Subjects Encountered by CBP

- The death, injury, or attempted suicide of an individual occurring while in CBP custody or during an encounter with CBP officers/agents or any individual directly working with CBP.
- Escape of a subject in CBP custody; this requirement does not extend to incidents involving subjects who abscond during field encounters prior to the establishment of a full custody arrest.

10. Agriculture-Related Events

- Any suspected agro terrorism or bioterrorism-related event.
- Cargo arriving from a country with any foreign animal disease status of concern (such as Foot & Mouth Disease or Highly Pathogenic Avian Influenza) that is erroneously or illegally allowed to enter into U.S. commerce.
- Any discovery or positive identification of a plant pest, noxious weed, mollusk, or animal/plant disease encountered in the cargo environment that may have very severe agricultural and economic consequences in the United States and for which immediate action and response is critical.

11. Facility and Technology Disruptions

- Any unscheduled major disruption of a CBP facility as a result of weather, fire, hazmat, power disruption, unscheduled computer communication systems outages (e.g., Automated Targeting Systems [ATS-AT/L/N/P], TECS, Intelligence & Operations Framework System [IOFS]), bomb threat, or other causes.
- Incidents at facilities used by CBP resulting in a major law enforcement response.
- CBP ports of entry experiencing processing wait times that meet certain thresholds.
- Major communication system outages of two hours or more.

12. Any Incursion of the U.S. Border

Any border incursion by a foreign government, military, or law enforcement official must be reported, whether armed or unarmed, regardless of length of time or distance.

13. Air and Marine Events

Any Air and Marine event that results in the arrest and/or seizure of contraband, vesse1(s), aircraft, or conveyance that falls within the parameters otherwise outlined in this list.