Privacy Impact Assessment
for

Insider Threat Reporting Mobile Platform

DHS/ALL/PIA-068

September 24, 2018

Contact Point
Sean Thrash
Insider Threat Program Manager
Office of the Chief Security Officer
(202) 447-5316a

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Insider Threat Program (ITP) was established as a department-wide effort to manage insider threat matters within DHS. In January 2017, the Secretary of Homeland Security expanded the DHS ITP beyond the protection of classified systems and information to include all threats to the Department posed by individuals who have or had authorized access to DHS facilities, information, equipment, networks, or systems. The DHS ITP is submitting this Privacy Impact Assessment (PIA) for the Department Headquarters (HQ) pilot and initial operational capability of the LiveSafe Platform. The LiveSafe Platform is a mobile application that will allow DHS mobile phone holders to use their DHS-issued mobile phone to report tips to the DHS ITP. The enterprise platform enables two-way, real-time interactions via location tagged text[1] and phone communications, as well as a scalable mass notification service. All tips go to a dashboard that is reviewed by the ITP for determination of further action. The application requires user personally identifiable information (PII) to establish an account and maintains communications that are made through the program.

Overview

The Department of Homeland Security (DHS) Insider Threat Program (ITP) was established pursuant to Executive Order No. 13587[2] and the attendant National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.[3] The ITP may maintain information from any DHS Component, office, program, record, or source, including records from information security, personnel security, and systems security for both internal and external security threats.

The ITP is a Department-wide program to identify threats to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems by collecting and analyzing data about (1) DHS personnel;[4] (2) state, local, tribal, territorial, and private sector personnel who possess security clearances granted by DHS; (3) any person who accesses DHS

[1] This is a text message that is tagged with the location from which it was sent.
[2] Exec. Order No. 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 Fed. Reg. 63811 (Oct. 7, 2011), *available at* https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.
[3] Presidential Memorandum — National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (November 21, 2012), available at https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand.
[4] Throughout the document, "personnel" has the meaning of the word "employee" as provided in section l.l(e) of Executive Order No. 12968, Access to Classified Information, August 2, 1995. Specifically, this refers to a person, other than the President and Vice President, employed by, detailed or assigned to DHS, including members of the Armed Forces; an expert or consultant to DHS; an industrial or commercial contractor, licensee, certificate holder, or grantee of DHS, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of DHS as determined by the DHS Chief Security Officer.

information technology (IT) systems or DHS information; and (4) any person with access to DHS facilities, information, equipment, networks, or systems. The ITP identifies insider threats through the collection and analysis of data.[5] Once suspected insider threats are identified, the relevant information and analysis are provided by the ITP to the appropriate Component or investigative agency for further investigation and action in accordance with the DHS Insider Threat Operations Center (ITOC) Standard Operating Procedures (SOP).

The ITP collects data from three main sources when protecting DHS facilities, information, equipment, network, and systems: (1) software that monitors users' activity on DHS computer networks; (2) information supplied by DHS personnel and prospective personnel that is provided to the Department to gain access to DHS facilities, information, equipment, networks, or systems; and (3) tips and leads received by other means, such as email or telephone. The ITP collects, uses, disseminates, and retains this data in accordance with the DHS ITP System of Records Notice (SORN).[6]

The ITP is piloting the LiveSafe Mobile Application as a mobile safety communications platform that delivers actionable, crowdsourced safety and security reporting relevant to insider threats to prevent incidents before they occur.[7] The LiveSafe application includes both the mobile application that is downloaded to a DHS provided iPhone and a dashboard available to ITOC staff. DHS Science and Technology (S&T) Directorate and the ITP have a contract with LiveSafe. Through the LiveSafe smartphone application, users communicate with the ITP who can analyze and respond via a real-time, cloud-based command dashboard that is under the operational control of the DHS Insider Threat Program.

This dashboard shows the ITP staff the user and the tip submitted and serves as an additional means for the ITP to receive tips. The tips are viewed as an initial factor and must be corroborated by additional information before they can be considered indicative of an insider threat. The process is well defined in the ITOC SOP, which explains the levels of inquiry and the thresholds to progress through the inquiry process.[8] The initial analysis performed on an incoming tip is not considered an inquiry, but rather must be further analyzed and, as necessary, augmented by additional information to ripen into a full-fledged insider threat inquiry. During this initial validation phase, ITOC analysts have a defined set of systems that can be used to assess the implications of the apparent insider threat. If the ITOC analyst is able to validate the possibility of an insider threat, the analyst then notifies the DHS Office of General Counsel, Intelligence Law Division (OGC/ILD) to obtain approval to open an ITOC inquiry. Within five days, the ITOC must

[5] *See* DHS/ALL/PIA-052(a) DHS Insider Threat Program, *available at* www.dhs.gov/privacy.
[6] DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (Feb. 26, 2016).
[7] For purposes of the DHS ITP, "insider" is defined as "any person who has or who had authorized access to sensitive or classified national security information, at any DHS facilities, equipment, networks, or systems;" it does not cover other populations that do not have access to one of those delineated departmental resources.
[8] *See* DHS/ALL/PIA-052(a) DHS Insider Threat Program, *available at* www.dhs.gov/privacy.

either mitigate the potential insider threat concern, or obtain articulable facts that warrant continuing the inquiry into whether the individual is an insider threat. If the ITOC cannot reach that threshold, the inquiry does not proceed. All ITOC requests to continue inquiries beyond the initial five days are reviewed for legal sufficiency by OGC/ILD.

Implementing this commercial solution will create an effective readily available infrastructure for reporting that will support and augment current approaches to insider threat reporting, making it easier to report through the DHS-issued mobile device. The tips are made through the application and appear on the dashboard at the ITP; tips are not sent or stored through email or text features on the phone. Tips from DHS personnel are collected and stored on the application dashboard for the exclusive review by the ITP; no external entities or other offices or Components of DHS will have access to the tips. After the tip is received from the application dashboard, the tip is handled just as tips received through other means are handled by the ITP, including deleting the tip from the inquiry management system if it is of no value (i.e. not insider threat tips or used for data to support ITOC), anonymizing the tip if it does not reach the threshold of an insider threat inquiry, or sending it out as a referral within 180 days.

The pilot will include up to 50,000 DHS Headquarters employees working in the National Capital Region. DHS employees, contractors, and other federal employees on detail to DHS that have a DHS-issued mobile phone are eligible for participation. Participation is voluntary. Following a successful pilot, the Department's intent is to offer the same configuration nationally to DHS headquarters elements and Components, expanding by region. The application can be configured for various tips. The initial configuration of reporting insider threat tips includes: (1) Facilities, (2) Equipment, (3) Network security issues, (4) Information, and (5) Feedback. There is an anonymous reporting option through which the information about the user is not maintained with the tip. ITP procedure, not technology, inhibits reconnecting this information for an anonymous tip.

Eligible participants will receive an invitation to participate in the LiveSafe pilot. The invitation will discuss the pilot's purpose of reporting tips to the ITP. The LiveSafe mobile app will be added to the AirWatch catalog and automatically pushed to users' mobile devices from the catalog, belonging only to the pilot population. The potential LiveSafe app-user will then register to participate (opt-in) by creating an account. In order to establish an account, the user must provide name, DHS-email, and DHS mobile phone number. With the consent of the user, the LiveSafe app interacts with the address book (during a SafeWalk) and then also uses location services for most functions. Regardless, address book information, including contacts at DHS, other Federal agencies, or outside of the Federal Government are not stored within the LiveSafe app. The LiveSafe app also has user-enabled functions including, picture, sound, and file attachment, to allow the app user to add information to support a tip.

The ITP currently allows tips by email, phone, or website. The report suspicious activity and report incident options on the home screen are reported to the ITP for processing. All other tips come as reported to the ITP for processing. The LiveSafe pilot will add an additional reporting mechanism. The application also has an emergency feature that will alert 911 based on the location of the phone making the emergency submission. The Emergency tip is connected to allow the user to talk to 911 emergency personnel or the DHS Centers (NAC, Mega, and Campus Security at St. Elizabeth's) for the area in which his or her phone is located. The emergency feature is connected to the SafeWalk safety feature. A SafeWalk is a safety feature that allows a contact within the address book of the users' mobile device to view a trip and see when the user arrives at his or her destination. SafeWalk users can invite up to three contacts to watch them walk. No information is passed to the contact unless the contact accepts the SafeWalk from the user. The contact does not have to download the LiveSafe app to watch the app user walk or drive in real-time. The contact is also provided with an estimated time of arrival (ETA) for when the user should arrive at their destination.[9] The app does not collect any information from the contact.

When a user provides a tip to the ITP, they may use free text, photos, or recorded audio files to describe the person or event of concern. To remind users to treat all PII as is required by DHS Privacy Policy,[10] privacy disclosure language is provided in the Terms of Use before downloading the LiveSafe Mobile Application or before using the Application for the first time. The text reads:

> The Department of Homeland Security (DHS) has designated the LiveSafe Mobile Application as a permissible communications method for Sensitive Personally Identifiable Information (Sensitive PII or SPII).
>
> As someone who works for or on behalf of the DHS, it is your responsibility to protect information that has been entrusted to the Department. You should exercise care when handling all PII. Sensitive PII, however, requires special handling because of the increased risk of harm to an individual if it is compromised.
>
> DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly

[9] If an app user exceeds his or her ETA, the user will have 30 seconds to call 911, based on the location of the mobile device making the emergency submission, or disable an alert by 10 minutes if he or she needs more time to get to the destination. If neither of these options are chosen, contacts are notified that the app user needs help. If there is an urgent situation while the app user is walking, he or she can press the panic button, which gives the user 10 seconds to call 911 or any of the DHS Centers. If neither option is chosen, contacts are notified that the app user needs help.

[10] *See* DHS Directives System Instruction Number 047-01-001 Privacy Policy and Compliance, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf. This Instruction applies throughout DHS regarding the collection, use, maintenance, disclosure, deletion, and destruction of Personally Identifiable Information (PII) and regarding any other activity that impacts the privacy of individuals as determined by the Chief Privacy Officer.

inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Sensitive PII is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

The LiveSafe Mobile Application has been authorized to communicate Sensitive Personally Identifiable Information (Sensitive PII) to the Insider Threat Operations Center. Authorized users of this application may send information containing Sensitive PII.

Before transmitting Sensitive PII, users acknowledge that using Sensitive PII within LiveSafe is appropriate given the purpose of the application and that the recipient(s) of the message have a need-to-know. The inclusion of Sensitive PII in a message that does not report activity potentially indicative of an insider threat may be considered a privacy incident that must be reported immediately.

The LiveSafe Mobile Application also provides privacy language in the message box when a participant attempts to draft a tip after logging-in to the App. The text reads:

Before transmitting Sensitive PII, users acknowledge that using Sensitive PII within LiveSafe is appropriate given the purpose of the application and that the recipient(s) of the message have a need-to-know. The inclusion of Sensitive PII in a message that does not report activity potentially indicative of an insider threat may be considered a privacy incident that must be reported immediately.

Tips are geolocated to the last location of the individual that the mobile application has available. Locations are periodically collected by the LiveSafe mobile application when the app is open and in use, and, if a user opens the app, but does not submit a tip the mobile application overwrites the users past locations. The user can disable location sharing within the settings tab of the LiveSafe application. The user would still be able to submit tips but there would be no geotagging of the tips and the tips would be submitted with no known location. Once an individual submits a tip, the system maintains a tip history for the user that made the tip, regardless if the tip was submitted anonymously. The "tip history" is available to the user, and without personal identifiers to the dashboard analyst, and LiveSafe management personnel.

The data collected by the LiveSafe Mobile Application and Dashboard is stored on Amazon Web Services (AWS), but is controlled by DHS and managed under DHS authorities, including the DHS Insider Threat Program SORN. The only DHS personnel who will see the incoming tips are members of the ITP who have been required to take privacy training specific to ITOC staff. The members of the ITP follow standard operating protocols for evaluating and processing the tips received through the application. The only external sharing from the LiveSafe Mobile Application

is for emergencies when the user is voluntarily put in contact with 911, consistent with the safety and security purpose of the tool. The "*Emergency Options*" function connects DHS HQ app users to their local emergency services and (depending on their location) DHS's Mega Center Operations, Nebraska Avenue Complex (NAC) Command Center, and Campus Security Operations Center. LiveSafe has a location perimeter to associate the participant with the correct emergency number that is closest to them.

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?

DHS is authorized to collect this information pursuant to the following:

- Title 6 U.S.C. § 341(a)(6), Under Secretary for Management;
- Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information;[11]
- Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs;[12]
- DHS Delegation of Authority 08503, Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer (Aug. 10, 2012);
- DHS Directive 262-05, Information Sharing and Safeguarding (Sept. 4, 2014);
- DHS Instruction 262-05-01, Insider Threat Program (July 9, 2015);
- DHS Directive 121-01, Office of the Chief Security Officer (Feb. 2014);
- DHS Delegation Number: 12000, Delegation for Security Operations within DHS (June, 2012); and
- DHS Directive 11052, Internal Security Program (Oct. 2004); and
- DHS Directive 047-01, Privacy Policy and Compliance.[13]

---

[11] Exec. Order No. 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 Fed. Reg. 63811 (Oct. 7, 2011), *available at* https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.

[12] Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012), *available at* https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand.

[13] *Available at* https://www.dhs.gov/sites/default/files/publications/DHS%20Privacy%20Policy%20for%20Mobile%20Application

Authorities supporting the DHS Insider Threat Programs use of third party website data analytics include:

- OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010;[14]
- OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, *Social Media, Web-Based Interactive* Technologies, and the Paperwork Reduction Act, April 7, 2010;[15] and
- DHS Website Privacy Policy.[16]

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

The DHS/ALL-038 Insider Threat Program SORN[17] covers all records and information used by DHS ITP related to the management and operation of DHS programs to safeguard DHS resources and information assets. The SORN covers both classified and unclassified information (often marked by DHS as For Official Use Only (FOUO)).

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

System security documentation is being completed as part of the process to be granted the Authority to Operate (ATO), which is expected to be obtained following completion of this PIA.

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

Yes. Records in DHS/ALL-038 Insider Threat System of Records are subject to the National Archives & Records Administration General Records Schedule 5.6: Security Records (July 2017), which mandates that (a) records pertaining to an "insider threat inquiry"[18] are destroyed 25 years after the close of the inquiry; (b) records containing "insider threat

s.pdf

[14] OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf.

[15] OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (*April 7, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRA_Gen_ICRs_5-28-2010.pdf.

[16] *Available at* http://www.dhs.gov/xutil/gc_1157139158971.shtm.

[17] DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (Feb. 26, 2016).

[18] "Insider threat inquiry records" are defined as "records about insider threat program inquiries initiated or triggered due to derogatory information or [the] occurrence of an anomalous incident," including, but not limited to, "initiated and final reports, referrals, and associated data." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 220, 103 (July 2017).

information"[19] are destroyed when 25 years old; (c) insider threat user activity monitoring (UAM) data[20] is destroyed no sooner than 5 years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records[21] are destroyed when 7 years old. Within five days, the ITOC must either mitigate the potential insider threat concern by performing activities to ascertain whether an insider threat exists, or obtain articulable facts to warrant an inquiry into whether the individual is an insider threat. If the ITOC cannot reach that threshold, an inquiry is not initiated and the information is deleted. All ITOC requests for a full inquiry are reviewed for legal sufficiency by the Insider Threat Oversight Group (ITOG) (which includes OGC, the Office for Civil Rights and Civil Liberties (CRCL), and the DHS Privacy Office). Tips that do not become inquiries are stripped of PII except for the name of the submitter, archived in the dashboard but not deleted, and can be undeleted.

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.

LiveSafe does not collect information covered by the PRA because it only involves the collection of information from federal employees and contractors.

[19] "Insider threat information" is defined as "data collected and maintained by insider threat programs undertaking analytic and risk-based data collection activities to implement insider threat directives and standards," including, for example, the following categories of information: "counterintelligence and security information;" "information assurance information;" "human resources information;" "investigatory and law enforcement information;" and "public information." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 230, 104 (July 2017).

[20] "Insider threat user activity monitoring (UAM) data" is defined as "user attributable data collected to monitor user activities on a network to enable insider threat programs and activities to: identify and evaluate anomalous activity involving National Security Systems (NSS); identify and assess misuse (witting or unwitting), or exploitation of NSS by insiders; [and] support authorized inquiries and investigation." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 240, 105 (July 2017).

[21] "Insider threat administrative and operational records" are defined as "records about insider threat program activities" including, for example, "correspondence related to data gathering;" "briefing materials and presentations;" "status reports;" "procedures, operational manuals, and related development records;" "implementation guidance;" "periodic inventory of all information, files, and system owned;" "plans or directives and supporting documentation, such as independent self-assessments, corrective action plans, [and] evaluative reports." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 210, 103 (July 2017).

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.

In order to establish an account to use the LiveSafe Mobile Application, the user must provide name, DHS email, and DHS mobile phone number. When a user provides a tip, he or she may use free text, photos, or recorded audio files to submit the tip. Users will see a banner on the application highlighting that they should limit PII to information relevant to the tip, and treat all PII as is required by DHS Privacy Policy. Tips are geolocated to the last location of the individual that the system has available as described above unless location is turned off. Locations are periodically collected by the LiveSafe mobile application when the app is open, and if a user opens the app, but does not submit a tip the mobile application overwrites the user's past locations. The user can disable location sharing within the settings tab of the LiveSafe application. The user would still be able to submit tips but there would be no geotagging of the tips and the tips would be submitted with no known location. The tip is communicated to the dashboard, which is available to ITP personnel. The tips can be relevant to insider threats at (1) Facilities, (2) Equipment, (3) Network security issues, (4) Information, and (5) Feedback. The Dashboard would have user information and any PII provided in the tip.

Additionally, SafeWalk information including route, location data, and ETA are not collected or disseminated by the ITP or LiveSafe. The SafeWalk information is maintained by the contact, if he or she accepts, during the duration of the SafeWalk and then deleted unless the SafeWalk is reported as an emergency situation.

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

The LiveSafe Mobile Application Pilot collects information from participants when they register and when they are providing tips. The tips could contain PII concerning other persons. When the participant submits a tip, the application tags geolocation of the person submitting the tip from his or her mobile phone.

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

No.

2.4 Discuss how accuracy of the data is ensured.

The participants enter the data about themselves and have the ability to update the data in the application. Any information given in a tip (which may be about another person) is evaluated through a designated process to understand the veracity of the tip, to include the validity of the underlying facts of the tip. The accuracy of DHS-owned data is dependent on the original source. The individual supplying the tip can update the tip or correct the tip if he or she identifies an inaccuracy. The ITP can also request clarifying information through the application.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: More information than is necessary may be analyzed in order to determine if an actual insider threat exists.

Mitigation: When the ITOC is alerted by incoming tips to a potential insider threat, the ITOC conducts research following a standardized protocol of checks to review information that may or may not corroborate the initial insider threat concern. If the information examined by the ITOC does not corroborate the insider threat concern, it could be argued that the information viewed was unnecessary. However, the ITP can neither corroborate nor mitigate an insider threat concern provided by the LiveSafe mobile application unless it accesses the relevant information sets. The ITOC only queries additional data when necessary and appropriate to resolve an insider threat concern. Furthermore, all LiveSafe mobile activities are overseen by the DHS Chief Security Officer, the ITP Manager, the ITOG, and the ITOC Director to ensure compliance with applicable laws, regulations, and policies.

Privacy Risk: The users could provide PII or SPII that is not relevant to the provided tip.

Mitigation: This is partially mitigated through the terms of service notice and the tip notice concerning PII that warns users to only include relevant PII for the tip. If PII not directly relevant and necessary to accomplish the specified purpose of submitting the tip is included, the ITOC may report the tip as a possible privacy incident to the DHS Privacy Office for follow-up and mitigation.[22]

Privacy Risk: Tips which may be identified to the DHS ITP through LiveSafe may not be accurate or may be submitted for reasons other than an insider threat.

Mitigation: The tips are simply viewed as an initial factor and must be corroborated by multiple factors to move through the examination process. The process is well defined in the ITOC

[22] *See* the Privacy Incident Handling Guidance (PIHG) which establishes DHS policy for responding to "privacy incidents" by providing procedures to follow upon the detection or discovery of a suspected or confirmed incident involving PII, *available at* https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017.pdf.

SOP, which explains the levels of inquiry and the thresholds to progress through the inquiry process. The analysis done on the basis of a tip is not considered an inquiry. During this initial validation phase, ITOC analysts have a defined set of systems that can be accessed to assess the implications of the apparent insider threat. The ITOG must be notified before the ITOC initiates an inquiry. Within five days, the preliminary inquiry must have identified additional verified concerns or articulable facts to ITOG into whether the individual is an insider threat or be closed. If the ITOC cannot reach that threshold, an inquiry is not initiated. All ITOC requests for a full inquiry are reviewed for legal sufficiency by the ITOG.

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 system needs to collect name, DHS email, and DHS mobile phone number to manage the participants account on the platform and to communicate with the participant. The participants see texts reminding them to limit any PII used in a tip to data relevant to the details of the tip. The tip information is simply an initial factor that requires the ITOC to examine the issue using additional data. The tip data is maintained but anonymized if it is not linked to an Insider Threat inquiry or other referral (such as referral to law enforcement)—in accordance with the DHS ITP SOP—within 180 days. The application could access the participants' address book, contacts, photos, and other location information on the users' phone with the participant's consent following the setting up of an account. However, DHS maintains complete autonomy and ownership of all LiveSafe-related DHS data. The application would only use this information to augment an activity (e.g., adding a picture from the participant's phone to the tip). Photos and address book information, including contacts at DHS, other Federal agencies, or outside of the Federal Government are not stored within the LiveSafe app.

The SafeWalk feature allows the user to identify an individual from the address book of he or she's mobile device so the contact can observe the route of the SafeWalk and receive an ETA.

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. However, the system could be capable of identifying the location of individuals who submit multiple tips, and those tip types. DHS does not plan to use the potential capability.

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

Yes. The ITP has specific protocols for sharing outside of the Program, which include referrals to other DHS elements (i.e., the DHS Privacy Office, CRCL, or OGC) and law enforcement. This would only be done after significant examination and legal review. While the raw tips would not be shared outside of the ITP, information obtained from developing the tip would be shared through referral with appropriate parties permitted to conduct follow-up actions. In general, there would be no reason to share PII collected by the LiveSafe application unless it is inextricably embedded in the tip.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: When a tip is offered to the Insider Threat Program through LiveSafe, there is a risk that the information will reveal other information that could result in an adverse action being taken against an individual outside the scope of the Insider Threat Program. For example, an analysis of information could result in identifying that an individual has committed a criminal act or misconduct, even if the same evidence to support that decision does not indicate an insider threat concern.

Mitigation: Although the ITP monitoring focuses specifically on insider threat, derogatory information relevant for other purposes may be reported through LiveSafe. This privacy risk is mitigated by due process procedures in place when adverse action is taken against a DHS employee by appropriate elements of the Department or the United States Government (i.e., elements beyond the Insider Threat Program, which does not take any adverse employment actions against anyone), both within and outside of DHS. Examples of these processes include filing an appeal with the DHS Security Appeals Board for security clearance matters; the DHS grievance process for human resource actions; and filing a complaint with the OIG, Office of Special Counsel, or the Merit Systems Protection Board for whistleblower matters.

Privacy Risk: There is a risk that information unrelated to DHS might be reported that contains PII (e.g., someone reporting a simple encounter of two people in Washington, D.C.).

Mitigation: The pilot instructions inform individuals to limit themselves to DHS-relevant reports. The emergency link could be used in reporting to 911. The privacy notices will highlight that the use of PII should only be for relevant PII to a given DHS tip. DHS phone use is also limited to official business.

Information identified and accessed through the LiveSafe for the purpose of identifying insider threats must bear a rational relationship to the scope of the analysis contained in the tip. The clearance process for issuing an insider threat report involves supervisory and legal review to ensure that the analysis and conclusions of the report are germane to the purpose for which the

report was intended. If the information is irrelevant to ITP then it would not move onto the Inquiry. PII maintained in the tip would be removed except for the name of the submitter.

Privacy Risk: There is a risk that members of the ITP will review data that is not relevant to analysis of insider threats.

Mitigation: The ITOC SOP guides the analysts' review of data needed to resolve instances that are reasonably indicative of an insider threat. The periodic review of immutable audit logs by the ITOG to ensure that the ITOC analysts are complying with the ITOC SOP also helps mitigate this risk.

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.

Any user of the system will do so voluntarily, and will directly provide the information collected. It is possible that a user may provide a tip that has tip relevant PII concerning another individual. This third-party would not have notice that his or her PII was being shared with the Insider Threat Program. Although the individual would not have notice, the Insider Threat Program has procedures to ensure no action is taken towards an individual without thorough analysis.

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

All users will be doing so voluntarily and will be able to decline to provide information or opt-out of the program altogether. A person listed in a tip would not have that option. This is similar to any tip provided by email, phone, or in person to the Insider Threat Program. Users can enable or disable location services and choose not to use all features of the app if they create an account. The user can disable location sharing within the settings tab of the LiveSafe application. The user would still be able to submit tips but there would be no geotagging of the tips and the tips would be submitted with no known location.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: A tip concerning another individual can be provided to the ITOC by a LiveSafe user; thus, the individual about whom the tip was made may not have notice that his or her information was provided to the ITP.

Mitigation: This risk is partially mitigated. LiveSafe is one form of reporting tips and tips received by the ITOC through LiveSafe are subject to the same rigorous process as tips received

by other means. Notifying an individual that he or she is the subject of a tip could frustrate the inquiry process and purpose of the ITP program. Moreover, notification of receipt of a tip by the ITOC prior to its validation or a consequential inquiry could also escalate the threat or advance the timetable for carrying-out the threat. Notification to individual employees of tips received that may relate to them is therefore neither practical nor efficacious. Notice is provided through annual required insider threat awareness training for all DHS personnel, not just those who use LiveSafe, and the training also provides notice to individuals that tips can be reported by anyone and through a variety of means. LiveSafe is covered by the Insider Threat Program System of Records[23] and is publishing this PIA to inform individuals what information may be provided to the ITOC and how it is used.

Privacy Risk: Persons not required to receive DHS Insider Threat training who may nonetheless obtain temporary access to DHS networks, facilities, or resources may be unaware that their information and actions may be reported through LiveSafe.

Mitigation: This risk is partially mitigated by the ITP SORN and this PIA, which provide general notice to non-DHS users that their information may be included in the ITP. In addition, persons who receive approval to access or use DHS networks, facilities, or resources are vetted by DHS and are informed through online banners, physical signage, and/or briefings that they are subject to search and activity monitoring. Further, individuals who conduct any form of business with DHS officials should be aware that the content of any discussions, emails, documents, or forms shared with DHS are subject to departmental procedures.

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.

The retention period for the information collected by the ITOC varies depending on the type of data. DHS-owned data is retained in accordance with the SORN for the underlying system from which the data is obtained, as well as the written terms and conditions required by the ITOC's Bulk Data Transfer Procedures. Once an underlying source system deletes or changes the data, the ITOC deletes or changes its data during its next refresh from that system.

Records in Department of Homeland Security/ALL-038 Insider Threat System of Records are subject to the National Archives & Records Administration General Records Schedule 5.6: Security Records (July 2017), which mandates that (a) records pertaining to an "insider threat inquiry"[24] are destroyed 25 years after the close of the inquiry; (b) records containing "insider

[23] DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (Feb. 26, 2016).
[24] "Insider threat inquiry records" are defined as "records about insider threat program inquiries initiated or triggered

threat information"[25] are destroyed when 25 years old; (c) insider threat user activity monitoring (UAM) data[26] is destroyed no sooner than 5 years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records[27] are destroyed when 7 years old. Within five days, the ITOC must either mitigate the potential insider threat concern by performing activities to ascertain whether an insider threat exists, or obtain articulable facts to warrant an inquiry into whether the individual is an insider threat. If the ITOC cannot reach that threshold, an inquiry is not initiated and the information is deleted.

SafeWalk data is not retained by ITP or LiveSafe. Previous, SafeWalk information is maintained by the contact, if he or she accepts, during the duration of the SafeWalk and then deleted unless the SafeWalk is reported as an emergency situation.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: The ITOC may retain more information from a LiveSafe tip than is necessary when the data fails to indicate a potential insider threat.

Mitigation: The risk is mitigated because pursuant to the ITOC SOP, when insider threat concerns are reported to the ITOC that do not reach the threshold of an insider threat inquiry, the information is permanently anonymized or deleted within 180 days if the information has not been associated with an identified cleared individual and has not been sent out as a referral. This will be done manually by the ITP in the application to save the tip info for metrics but remove personal information.

Privacy Risk: Many insider threat referrals are based on or contain time-sensitive

due to derogatory information or [the] occurrence of an anomalous incident," including, but not limited to, "initiated and final reports, referrals, and associated data." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 220, 103 (July 2017).

[25] "Insider threat information" is defined as "data collected and maintained by insider threat programs undertaking analytic and risk-based data collection activities to implement insider threat directives and standards," including, for example, the following categories of information: "counterintelligence and security information;" "information assurance information;" "human resources information;" "investigatory and law enforcement information;" and "public information." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 230, 104 (July 2017).

[26] "Insider threat user activity monitoring (UAM) data" is defined as "user attributable data collected to monitor user activities on a network to enable insider threat programs and activities to: identify and evaluate anomalous activity involving National Security Systems (NSS); identify and assess misuse (witting or unwitting), or exploitation of NSS by insiders; [and] support authorized inquiries and investigation." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 240, 105 (July 2017).

[27] "Insider threat administrative and operational records" are defined as "records about insider threat program activities" including, for example, "correspondence related to data gathering;" "briefing materials and presentations;" "status reports;" "procedures, operational manuals, and related development records;" "implementation guidance;" "periodic inventory of all information, files, and system owned;" "plans or directives and supporting documentation, such as independent self-assessments, corrective action plans, [and] evaluative reports." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 210, 103 (July 2017).

information. The referrals lose accuracy or relevance after a finite period, and there is a risk that resulting agency actions involving the potential to affect encountered persons will be handled inappropriately because the information is no longer accurate or relevant.

Mitigation: This risk is mitigated. This process is part of the assessment process to which tips are subject and why additional information is needed to recommend any issue to the level of an inquiry. The tip is simply one piece of data and must be corroborated.

Privacy Risk: LiveSafe may retain information regarding persons who are suspected of insider threat activity without resolving whether the referral was upheld or vacated by the investigative Component or agency.

Mitigation: This risk is partially mitigated through the ITOC process to maintain contact on referrals and to record the disposition. Although it is possible that follow-up could fail or be difficult due to the sensitive nature of the follow-up, the ITOC maintains relationships with partners to improve this reporting.

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.

Yes. The information in LiveSafe is shared internally to the Insider Threat Program[28] or to Emergency Services if an emergency is identified by the user. Once the information is shared to the Insider Threat Program, there are robust protocols to evaluate the tip, assess its validity, and refer the matter to the correct office, as appropriate. If a crime was identified, it would be shared to the appropriate law enforcement agency through the Insider Threat Program's referral procedures.

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

The DHS/ALL-038 Insider Threat Program SORN[29] covers all records and information used by DHS ITP related to the management and operation of DHS programs to safeguard DHS resources and information assets. Information is shared for law enforcement, intelligence, or national security purposes and with contractors working for the Federal Government to accomplish

[28] *See* DHS/ALL/PIA-052(a) DHS Insider Threat Program, *available at* www.dhs.gov/privacy.
[29] DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (Feb. 26, 2016).

agency functions related to the system of records, *i.e.*, to counter potential and actual insider threats. No information will be shared outside the Department from LiveSafe directly unless it is an emergency call placed by the user through the application.

6.3 Does the project place limitations on re-dissemination?

Recipients of information from the ITP are provided the information consistent with their authorities to investigate or take action on the referral. These recipients maintain the information consistent with their authorities and report the resolution back to DHS ITP. DHS has negotiated Memoranda of Agreement (MOA) with all external organizations to which the ITP would refer, which requires those organizations to acquire consent from the ITOC prior to re-dissemination. As a condition of accessing ITOC data, Components are required to get consent from the ITOC for re-dissemination. Only individuals with a need-to-know are able to gain access to ITOC data or ITOC referrals.

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

The information would not be shared directly from LiveSafe. The ITP uses the existing processes and procedures within DHS for recording disclosures of information as appropriate to the situation causing the disclosure, and it does not establish or maintain an additional record of the disclosures within the ITOC's systems. Policies and procedures in use include: DHS Directive 047-01 Privacy Policy and Compliance, DHS Instruction 047-01-001 Privacy Policy and Compliance, DHS Form 191 Accounting for Disclosure, DHS Form 11000-8 Disclosure Record, DHS Form 11000-10 Document Record of Transmittal, and DHS Form 11000-10 Record of Security Violation.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: ITOC referrals containing incorrect information may be disseminated.

Mitigation: This risk is mitigated through policies describing the correction and re-dissemination process. All referrals that leave the ITOC are marked with their classification and are subject to re-dissemination restrictions.

Privacy Risk: There is a privacy risk that more information than necessary will be shared externally.

Mitigation: This risk is mitigated because, prior to any external disclosure of information, the ITOC Director and DHS OGC/ILD review all referrals in order to minimize the amount of information shared to the least amount necessary in order for the recipient to perform his or her official responsibilities. The ITOG monitors compliance with this requirement through quarterly audits, as required by the ITOC SOP.

Privacy Risk: Authorized users are exposed to PII as a routine part of their official duties. These users may make inappropriate disclosure of this information, either intentionally or unintentionally.

Mitigation: All ITOC analysts are required to complete annual specialized privacy training, including the appropriate and inappropriate uses and disclosures of the information they receive as part of their official duties. The analysts' use of the system and access to data is monitored and audited by the ITOG. Should a user inappropriately disclose this information, he or she are subject to loss of access and disciplinary action up to and including termination. Additionally, all ITOC analysts are required to sign DHS Form 11058, which contains specific provisions regarding the non-disclosure of ITOC information without the appropriate permissions and approvals.

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?

Users have control over the information they provide and can correct any information in their application. No information will be acted upon within the LiveSafe system. Once the information is removed from the LiveSafe system and enters the ITP systems it falls under the redress procedures discussed in the ITP PIA.[30]

Because the ITP systems contain sensitive information related to intelligence, counterterrorism, and homeland security, as well as law enforcement programs, activities, and investigations, DHS has exempted the ITP system and the records therein from the access and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. §§ 552a(j)(2), (k)(1), (k)(2), and (k)(5).

Notwithstanding the applicable exemptions, DHS reviews all such requests for information on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of DHS, and in accordance with procedures and points of contact published in the applicable SORN. Individuals seeking notification of and access to any record contained in this system of records, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

[30] *See* DHS/ALL/PIA-052(a) DHS Insider Threat Program, *available at* www.dhs.gov/privacy.

Chief Privacy Officer/Chief Freedom of Information Act Officer
Department of Homeland Security
245 Murray Drive, S.W. STOP-0655
Washington, D.C. 20528

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 contacts.

Although DHS has exempted this system from the access and amendment provisions of the Privacy Act, individuals may make a request to view their records. When seeking records about oneself from this system of records (or any other DHS system of records), the request must conform to the Privacy Act regulations set forth in 6 CFR Part 5. 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. Although no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition, the following should be provided:

- An explanation of why the individual believes the Department 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/her agreement for access to his/her records.

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

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

Although the information within LiveSafe is exempted, any action based on this information would be subject to ITOC rules and procedures.

ITOC analysts are responsible for the integrity and confidentially of the data they provide. Should erroneous information be entered, the analyst is required to correct his or her entry immediately upon determining it is incorrect. This requirement applies to any data to which an analyst has access, not just data provided by the analyst.

At times, erroneous information may be published in an ITOC referral product. When incorrect information is discovered, a revised referral is provided to correct the information or note the questionable fact or content. The incorrect referral is then removed from the ITOC's system. For any referrals that were externally disseminated, and therefore require recall or correction, recall messages or revised referrals are disseminated to the recipients of the original referral(s), with appropriate instructions.

As noted in 7.1 above, requests from the public for information from the ITP are reviewed on a case-by-case basis.

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

Individuals are notified of the procedures for correcting their information through the ITP SORN and this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Given the sensitive nature of the ITP, a robust program to permit access, review, and correction of raw information and referrals cannot be provided. This lack of direct access and a formal redress mechanism poses a risk to individual privacy; however, it is pragmatic given the heightened sensitivity of and potential harm to Government activities supported by the ITP. Although individuals do not have a formal mechanism for access or redress, DHS has internal mechanisms to correct inaccuracies and protect against abuse through the information system security protections and controls established within the ITP system. All dashboard administrators will be assigned and monitored by the ITP.

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?

The ITP system implements extensive auditing through the various applications that compose the system. Although the specifics of the system and applications are classified, the system logs every action by ITOC analysts. The ITOC's audit logs are immutable and they are subject to quarterly and unannounced reviews by the ITOG. ITOC analysts are not able to access the audit logs. Audit logs are maintained for 25 years. On a retroactive basis, should an incident occur, logs can be reviewed post-incident. The ITOG, along with management, can determine who accessed what information to a certain level of granularity.

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

All DHS employees are required to complete insider threat training that discusses what information to report. All ITOC analysts are required to complete specialized annual training in privacy awareness provided by the ITOG. The specialized training is provided by the ITOG on supplemental policies and procedures prior to access to data, and once per year thereafter. In addition, ITOC personnel consult with the ITOG prior to developing or implementing any automated information system to be maintained by the ITP that is reasonably likely to contain significant amounts of PII concerning U.S. Persons. This training is completed in addition to the annual privacy training that all DHS personnel receive and the open source training, which is completed by all ITOC analysts. ITOC analysts who do not complete the required specialized annual training lose access to all computer systems in the ITOC, which are integral to their duties.

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

The LiveSafe DHS Community of Interest is limited to DHS users and the ITP. Only authorized ITOC personnel and analysts who require access to the functionality and data of LiveSafe in the ITP as a part of the performance of their official duties and who have appropriate clearances or permissions have access to LiveSafe data. The number of ITOC personnel and analysts is limited in order to prevent widespread access to the sensitive information available to the ITOC. All ITOC personnel and analysts are required to hold and maintain TOP SECRET//SENSITIVE COMPARTMENTED INFORMATION access. Everyone in the ITOC is required to sign a Non-Disclosure Agreement (NDA) (DHS Form 11058), specific to the ITOC prior to accessing any ITP data. Any personnel not employed by the DHS Office of the Chief Security Officer are required to be detailed (as opposed to assigned) to the Office of the Chief Security Officer prior to assignment within the ITOC. ITOC operations are conducted in a restricted access Sensitive Compartmented Information Facility in order to maximize the security of the location and effectively monitor the activities of ITOC personnel. If issues are raised concerning ITOC compliance with approved policies and procedures, the issues are immediately reviewed by the ITOG. The ITOG may conduct system audits or policy/procedure reviews and recommend remedial actions to the Senior Insider Threat Official.

DHS maintains ITP access records showing which ITOC analysts have accessed the system, which functions they have used, and which data they have accessed. ITP management revokes a user's access when no longer needed or permitted. No personnel outside of the ITOC are given access to the data until such time a formal referral is provided in accordance with the SOP.

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?

Information sharing agreements, MOUs, new uses of the information, and new access to ITP data by organizations both within DHS and external are reviewed and approved by the ITOG, as required by the DHS ITP Instruction and the ITOC SOP.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: LiveSafe could become a target for unauthorized users (e.g., hackers).

Mitigation: LiveSafe is built upon the secure and scalable Amazon Web Services platform and all data is stored within AWS. There is no software, hardware, or data resident behind the DHS firewall. All data is encrypted in transit and at rest. Additionally, LiveSafe stores user PII data encrypted at the row level in the database using industry standard AES-256 encryption. Encryption keys are all stored in Amazon KMS (Key Management Service) and are stored separately from the encrypted application data. All access to the keys are logged using CloudWatch). LiveSafe hosts the data in AWS, but DHS retains ownership of the data.

DHS will determine who in the ITP will have access to the Live Safe dashboard. Dashboard Administrators (authorized by DHS) can access the Command Dashboard via a web browser with user name/password or Single-Sign-On (SSO) authentication. ITP analysts interact with the data via access to the LiveSafe dashboard. Analysts will be set up as dashboard administrators, with dashboard privileges set by DHS per individual. Analysts will be able to remove tips from the dashboard (the data will remain in the system per DHS retention policy). Specific protocols will be developed for each tip type within the Standard Operating procedures of the ITP.

Privacy Risk: The data maintained by AWS for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. The Office of the Chief Security Officer (OCSO) is responsible for all PII associated with the LiveSafe system, whether on OCSO infrastructure or on a vendor's infrastructure, and it therefore imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.[31] OCSO cloud service providers must be FedRAMP-certified. By using FedRAMP-certified providers, OCSO leverages cloud services assessed and granted provisional security authorization through the FedRAMP process to increase efficiency while ensuring security compliance. All contracted cloud service providers must follow DHS privacy and security policy

[31] See https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

requirements. Before using AWS, OCSO verified through a risk assessment that AWS met all DHS privacy and security policy requirements. Further, all cloud-based systems and service providers are added to the DHS Federal Information Security Modernization Act (FISMA) inventory and are required to undergo a complete security authorization review to ensure security and privacy compliance.

As part of this process, the DHS Senior Agency Official for Privacy reviews all FedRAMP cloud service providers for privacy compliance and privacy controls assessments as part of the privacy compliance review process.

Responsible Officials

Richard D. McComb
Senior Insider Threat Official
Chief Security Officer
Department of Homeland Security

David J. Glawe
Under Secretary for Intelligence and Analysis
Department of Homeland Security
Undersecretary for Management

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security