Privacy Impact Assessment

for the

Team Awareness Kit (TAK)

DHS Reference No. DHS/ALL/PIA-090

July 29, 2021

Homeland
Security

Abstract

The U.S. Department of Homeland Security (DHS) is responsible for providing services and technologies to protect its workforce while increasing operational capabilities and enabling mission fulfillment. To this end, DHS has enhanced and deployed Team Awareness Kit (TAK), a government-off-the-shelf application that enables near real-time location monitoring and display with operational personnel carrying devices. TAK is a geospatial infrastructure and situational awareness application that allows for enhanced situational awareness, navigation, surrounding land formation intelligence, and data sharing. DHS is conducting this Privacy Impact Assessment (PIA) to discuss the privacy risks associated with the deployment of this type of technology.

Introduction

As a part of DHS's mission, DHS headquarters offices work to provide DHS operational Components with technology needed to effectively execute their responsibilities and statutory missions. DHS continues to leverage existing technologies to combat immediate and emerging threats, coordinate joint operations, and provide increased situational awareness across Components.[1] As such, the DHS Science & Technology Directorate (S&T) adopted the use of TAK, which provides DHS officers and agents in the field with increased tactical situational awareness. The application was developed by the Department of Defense (DoD) Air Force Research Laboratories. S&T then worked with DHS operational Components, such as the United States Secret Service (USSS), U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE), to modify TAK to meet their specific operational needs.[2]

The main purpose of TAK is to facilitate coordinated responses to mission-related events. TAK allows trusted team members to share data including location and status of friendly forces and assets (i.e., Blue Force Tracking), relevant terrain and environmental attributes, and sensor data in near real time. Depending on Component use, TAK also provides personnel with real-time mobile capabilities such as live video feeds, image sharing, navigation, and chat. Users of TAK can share this information among small teams, stations, or sectors within DHS, as well as across other state and federal agencies assigned to an incident.

TAK consists of server hardware and software (e.g., mobile application). The TAK application is installed on government-furnished mobile devices that use appropriate operating systems.[3] During joint operations, large-scale events, or natural disasters, the application may also

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CHAMPION THE DHS WORKFORCE AND STRENGTHEN THE DEPARTMENT, *available at* https://www.dhs.gov/champion-dhs-workforce-and-strengthen-department.
[2] TAK uses specific to individual Components are discussed in the appendices to this PIA.
[3] TAK was originally developed on android operating systems. However, DHS has worked to make TAK available on iOS. Windows and Internet browser versions are also available for use.

be installed on devices belonging to other federal, state, and local personnel, and those personnel may be granted access to the Component-specific TAK application(s). TAK users are organized into TAK user groups based on specific factors, such as unit and function. Users will have access only to data and information about and shared by other users within their own group. When operational circumstances dictate, or at the discretion of Sector/Station/Unit leadership, TAK Coordinators may merge TAK user groups until the need to do so has ceased.

The TAK application enables near real-time location monitoring by reporting an individual mobile user's geolocation so that others are able to monitor the location and movement of associated personnel on a shared map.[4] An individual user appears as a dot on a map associated with a "Call Sign" or location tag, which will be shared with other authorized TAK devices in the user's group so that each person is clearly identified on the map. The location tags displayed by TAK may include names, phone numbers, unique agency identifiers, and other information shared by the device user, such as Call Signs or badge numbers. During unfolding situations, TAK users are able to see who and where those elements are on a mobile screen, and even communicate with team members or assets from different components and agencies, instead of hearing intermittent radio transmissions from unknown operators at unknown locations while simultaneously engaging in an action.

TAK starts monitoring a user's location once the individual launches the application on their mobile device. Users may opt-in to use a "track history" feature on their TAK application, which will enable creation of a route of travel or path of interest for users within the same group. TAK users will also be able to share photos and videos to other users within the same group. These photos may be stored in the local TAK system as annotations to maps to provide increased situational awareness of specific terrain and area landmarks. These photos may also include images of individuals in the public area at the time of the photo. TAK also includes a chat room feature, which allows connected users to send and receive messages to communicate and coordinate activities. Information can be shared through these chats between individual users or amongst entire TAK user groups.

The data shown in TAK is part of mission-specific information and can be purged from the TAK server and local device, along with any associated photos, chats, and annotations, upon conclusion of the mission. Some of the data, including chat sessions and photos, is retained on the user's device until explicitly removed by that user. Depending on the Component, information may be retained in Component-specific IT systems for a longer period of time, as necessary.

This PIA is intended to document the Department's general use of the TAK application. Component-specific uses of TAK are outlined in the appendices to this PIA.

[4] This functionality is similar to Apple's "Find my Friends" or Google's "Trusted Friends" applications.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[5] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[6]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[7] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[8] and the Homeland Security Act of 2002, Section 222.[9] This PIA examines the privacy impact of TAK as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

As the purpose of TAK is to facilitate coordinated responses and communication during mission-related incidents, users understand that their location information, chats, and other actions within TAK are recorded and shared among team members or TAK user groups. In addition, the TAK application privacy policy informs all TAK users of the information collected, uses of the information, information sharing, application security, and other useful privacy-related information. After the user launches the TAK application for the first time, a splash page notifies the user of the information collected (e.g., GPS location) through the application. The user must accept before proceeding. Additionally, users are required to comply with Rules of Behavior and complete any associated training prior to being provided access to TAK. The Rules of Behavior specify that the system should only be used in the performance of official duties, sensitive information should not be disclosed to unauthorized persons or groups, users will be held

[5] 5 U.S.C. § 552a.
[6] 6 U.S.C. § 142(a)(2).
[7] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[8] 44 U.S.C. § 3501 note.
[9] 6 U.S.C. § 142.

accountable for their actions while accessing and using the system, and that failure to comply with the Rules of Behavior or any other system responsibilities could result in verbal or written warning; removal of system access, reassignment to other duties, criminal or civil prosecution, or termination.. Components may also develop Initial or Standard Operating Procedures for their specific uses of TAK.

TAK is used internally for DHS (and assisting agency) personnel to facilitate communication. During mission-related events, it may become necessary for users to take video or images, which could capture members of the public. Generally, although the video and audio recordings could clearly identify an individual's facial features and could capture any verbal communication, no additional personal information is associated with these images and recordings unless an action (e.g., apprehension) is taken, and a case file is created for tracking purposes. This process would occur outside the scope of TAK in accordance with a Component's own processes.

Privacy Risk: There is a risk that individuals may not receive adequate notice that their images and voice communications may be recorded when they are in close proximity to a DHS encounter involving TAK, regardless of whether they are directly or indirectly involved.

Mitigation: This risk is partially mitigated. DHS personnel generally attempt to provide verbal notice of their presence and purpose at the onset of any encounter when possible. Additionally, DHS personnel wear uniforms and use equipment that indicate the agency for which they work. However, given the unpredictability of DHS interactions or encounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of DHS personnel or third parties. Therefore, DHS also provides general notice to the public through this PIA.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

TAK requires consent by users upon initial launch of the application and through the general enrollment process as a user (e.g., training, Rules of Behavior). The application also uses built-in permission prompts; users are specifically asked to allow the TAK application access to the phone's GPS-derived location and camera.

DHS personnel may use TAK in a variety of environments, to include law enforcement activities. Due to TAK's multi-purpose functionality, requiring individuals to consent to DHS' potential capture of images of the public or other information in video recordings is not always practical or feasible. Requiring DHS personnel to obtain an individual's consent prior to the collection, use, dissemination, and maintenance of the TAK functionalities could potentially compromise operations and prevent DHS personnel from fulfilling their required missions. However, the main purposes of TAK are not to identify individuals, but rather use the image/video capture as a means to provide situational awareness during DHS mission-related activities.

Given that any member of the public's information captured through TAK would only be used if an action (e.g., apprehension) is taken, redress mechanisms would occur through the Component's normal process that cover the collection of that information. However, any individual seeking access to or amendment of their records may submit a request in writing to the DHS Chief Privacy and Freedom of Information Act (FOIA) Officer at the address below, or to the respective Component's FOIA officer, which can be found at https://www.dhs.gov/foia-contact-information. DHS also accepts Privacy Act and FOIA requests submitted electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form.

Chief Privacy Officer and Chief Freedom of Information Act Officer
Privacy Office, Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

Privacy Risk: There is a risk that members of the public may not be able to access or modify their records given the nature of the activities potentially captured in the audio and visual recordings.

Mitigation: This risk is partially mitigated. DHS considers all individual requests to determine whether or not information may be released. Individuals can contact the DHS Chief Privacy and Chief FOIA Officer at the address/website listed above. If an individual's image is recorded inadvertently, there may be no way to associate that individual with any record because there is no other PII about that individual collected. Further, there remains some risk to access, given DHS may be authorized to withhold records when the release of those records may compromise investigations or proceedings.

Privacy Risk: There is a privacy risk to individuals who are in the range of a device using TAK but are not direct participants in interactions with DHS, as their images or voices may be captured without consent or opportunity to opt-out of the collection.

Mitigation: This risk is partially mitigated. DHS personnel attempt to provide verbal notice of their presence, purpose, and use of TAK during the onset of any encounter when possible. In addition, the purpose of TAK is not to capture images or video of individuals, but rather provide situational awareness to other TAK users by capturing images of relevant area landmarks/geography. Further, TAK training and Rules of Behavior provide all users with their roles and responsibilities of using this technology. However, due to the unpredictability of DHS interactions or encounters, there may be times when receiving consent is impractical, impossible, or jeopardizes the safety of DHS personnel or third parties.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Any data collected through TAK is done so as part of DHS's, and the respective Component's, authorized mission. TAK is used as a tool to enhance situational awareness, which generally precludes the need to collect PII. However, there may be some cases where PII may be necessary to share or is inadvertently collected. In those cases, it would be done so in accordance with the respective Component's system of records notice, and the legal authorities therein.

Privacy Risk: There is a risk that information collected through TAK may be used for unauthorized purposes.

Mitigation: This risk is mitigated. All DHS personnel are required to undergo annual privacy and security awareness training. Additionally, specific TAK training is provided before users are granted access and all users must sign and adhere to Rules of Behavior. TAK servers also have appropriate safeguards and audit trails in place to restrict access and viewing of recorded data to those with an official need to know.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

TAK captures users' information to provide access and use of the application. This data is covered by the following system of records notices, DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[10] and DHS/ALL-014 Department of Homeland Security Personnel Contact Information,[11] and includes:

- Name;
- Agency Identifier;
- Badge Number or Call Sign;
- Phone Number;
- Mobile Device ID; and

[10] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[11] *See* DHS/ALL-014 Department of Homeland Security Personnel Contact Information, 83 Fed. Reg. 11780 (March 16, 2018,), *available at* https://www.dhs.gov/system-records-notices-sorns.

- Location (i.e., GPS).

During the use of TAK, users may also capture photographs and video,[12] contribute to chat messages, and share files.

Once a user opens the TAK application and accepts the prompts on the splash screen, location data is sent to the TAK server and continues to be collected until and unless the TAK user closes the application. This data is retained to allow users, for example, to retrace past routes for mission-related activities. Other TAK functionalities are stored directly on the TAK mobile device, until the user deletes the data. Photographs and chats taken from the mobile device may also be stored in the TAK system and mobile device as annotations to maps. Information that is part of a mission-specific event can be removed/purged, along with all photos or annotations, at the conclusion of a mission (for example, the end of a National Security Special Event).

Data sent to the TAK server is stored for auditing and after-action analysis. Specific TAK retention requirements are determined by each Component and outlined further in the Appendices below, as necessary.

Privacy Risk: There is a risk that photos may unnecessarily capture PII, including images of members of the public.

Mitigation: This risk is partially mitigated. Users take training and are instructed to not collect unnecessary PII to mitigate this risk. However, due to the nature of the Component use of TAK, there may be an operational need to capture images and PII associated with individuals. If PII is captured inadvertently in an image, it would not be tied to an individual's records as no other PII would be captured. Further, information retained on the TAK server may be purged upon conclusion of the specific mission, so any relevant information will not be retained.

Privacy Risk: There is a risk that chat sessions and the information contained within a user's session will be retained for longer than necessary on the user's device.

Mitigation: This risk is mitigated. Users are provided training and sign Rules of Behavior that outline how users should maintain TAK data on their mobile devices. All data transmitted or received by TAK will be treated as per DHS Management Directive 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information.[13] All TAK users are further required to follow all policies related to the use and storage of government-issued mobile device on- and off-duty.

[12] Video is not currently used by all Components.

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS MANAGEMENT DIRECTIVE 11042.1, SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION, *available at* https://www.dhs.gov/sites/default/files/publications/mgmt/security/mgmt-dir_md-11042-1-safeguarding-sensitive-unclassified-official-info.pdf.

<u>Privacy Risk</u>: There is a risk that a user may forget to close the application after leaving the operational situation, resulting in collection of unnecessary location data.

<u>Mitigation</u>: This risk is mitigated. Users are provided training and sign Rules of Behavior that outline how users should use the TAK application and how to safeguard the data contained therein. Depending on the requirements of each Component, some personnel may be required to leave their equipment at DHS facilities, rather than retain them while off-duty, further mitigating this risk. Moreover, TAK users are well aware of the tracking functionality—as this is one of the main purposes of TAK's use—and are provided sufficient training and notice that the application continues to track location data until it is closed on the mobile device.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

TAK is used as a situational awareness enhancement tool and is only used during authorized DHS mission-related activities. Any data collected through TAK is related to DHS's, and the respective Component's, authorized mission. DHS may disclose TAK data outside of DHS consistent with the applicable disclosure provisions of the Privacy Act. There may be cases when personnel from other government agencies are permitted to join TAK user groups to facilitate more efficient communication and collaboration during a DHS mission-related event. In cases in which DHS would disclose TAK data to third-party agencies outside of DHS, those activities would be covered by the source system system of records notice, and the legal authorities therein, applicable to the data and sharing.

Further, TAK users are trained how to use the different functionalities and must adhere to Rules of Behavior. All DHS Components work with their respective Privacy Offices to ensure TAK is used and deployed in a manner to limit use and sharing of unnecessary PII and follows the guidance laid out in this PIA.

<u>Privacy Risk</u>: There is a risk location tracking may allow for tracking of users outside the scope of their authorized responsibilities.

<u>Mitigation</u>: This risk is mitigated. Users are provided training and sign Rules of Behavior that outline how they should use the TAK application and how to safeguard the data contained therein. Depending on Component requirements, some personnel may be required to leave their equipment at DHS facilities, rather than retain them while off-duty. TAK users are well aware of the tracking functionality, as this is one of the main purposes for using TAK. Users are provided sufficient training and notice that the application continues to track location data until it is closed on the mobile device.

Privacy Risk: There is a risk that TAK data may be shared inappropriately outside the Department.

Mitigation: This risk is mitigated. TAK users are organized into TAK user groups based on specific factors, such as unit and function. Users will have access only to data and information shared by or about other users within their own group. During joint operations, large-scale events, or natural disasters, personnel from other federal, state, and local entities may be invited into TAK user groups to contribute to the mission. For example, a United Nations General Assembly session may require USSS and New York City Police Department personnel to share information. TAK user groups can also be merged, when operational circumstances dictate—at the discretion of Sector/Station/Unit leadership or TAK Coordinators. TAK users are able to see who and which elements are in a group, to better effectuate communication during multi-agency events.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

DHS captures TAK data in real-time to maintain an accurate accounting of personnel locations, communications, and other mission-related requirements. DHS also uses photos and video to document other mission-related needs or encounters, such as landmarks and other perishable intelligence needed to assist in operations or as navigational aids. Although the collection of TAK photos and video does not routinely involve the collection of PII, all TAK data is encrypted both at rest and in transit. In addition, any image and video recordings of a DHS encounter would not be the sole source by which DHS takes any action. This data would supplement existing processes or authorized enforcement or other action.

Privacy Risk: There is a risk that DHS will identify and take action based solely on inaccurate information captured by TAK.

Mitigation: This risk is mitigated. The purpose of TAK is to provide enhanced situational awareness and communication for DHS personnel during a mission-related event. TAK users undergo required training on the proper uses of TAK and must adhere to Rules of Behavior that outline requirements and stipulations on using the technology. If, during the course of a mission-related event, TAK users encounter a situation that requires them to take enforcement or other action under their respective authorities against an individual, that action would be taken in accordance with the other legal, policy, and program responsibilities of that individual TAK user. DHS personnel are trained in accordance with their respective Component’s authorities to take in the totality of information to fully understand a situation before engaging in any such actions.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The technology infrastructure used to implement TAK meets all DHS security requirements stipulated in DHS Sensitive Systems Policy Directive 4300A.[14] TAK servers maintained by DHS meet the level of security defined for the data and its availability; any data transferred to the cloud environment will be transferred using FedRAMP-approved infrastructure.[15]

DHS policy also requires that various security measures be put in place before using applications on mobile phones, to include Mobile Device Management solutions that help to secure and manage the overall configuration of mobile devices. Before accessing the TAK application, government-furnished equipment requires two-factor authentication, including biometric or Personal Identity Verification (PIV). Access to the data on the TAK servers requires user verification, consisting of two levels of security at each stage: Local Area Network (LAN)/Operating System (OS) level security (i.e., DHS Network access) and TAK-application level security (e.g., username/password).

TAK data is also encrypted both at rest and when transiting between the mobile device and the appropriate TAK server.

Privacy Risk: There is a risk of unauthorized access, use, disclosure, or removal of TAK data.

Mitigation: This risk is mitigated. TAK adheres to the security requirements outlined in DHS 4300A. Data on TAK servers can only be accessed by those individuals who have been granted access to the DHS Network, have been provided a TAK user account, and log in with the correct credentials. Data is securely encrypted both in transit and at rest. TAK servers also have appropriate safeguards in place to restrict access and viewing of recorded data to those with an official need to know. Such safeguards include automatically logging employee access to TAK and retaining that data necessary to audit TAK's use. Lastly, prior to issuing TAK credentials, potential users must complete appropriate TAK training and sign the Rules of Behavior.

Every DHS employee also has a duty to report any matters that could reflect substantive misconduct or serious mismanagement. Any unauthorized access, use, release, or removal of recorded data or other violations of confidentiality laws and Department policies may result in disciplinary action and/or criminal or civil sanctions.

[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS SENSITIVE SYSTEMS POLICY DIRECTIVE 4300A (2017), *available at* https://www.dhs.gov/privacy-policy-guidance.

[15] *See* U.S. GENERAL SERVICES ADMINISTRATION, FEDRAMP, *available at* https://www.gsa.gov/technology/government-it-initiatives/fedramp.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

TAK training for using the application's basic functions consists of a series of short instructional videos that were developed by S&T to quickly conduct remote training for disparate personnel. Additionally, S&T developed an Interactive Training Guide to support CBP U.S. Border Patrol's (USBP) deployment of TAK to its agents. The training has been made available to appropriate CBP Office of Field Operations (OFO) and Air and Marine (AMO) personnel and may be used by other Components as appropriate. The training covers the use of TAK in local operations, such as how to provide updates (e.g., symbols to use and naming conventions), how to respond to those updates (e.g., all in the TAK user group go to the updated locations or only the user closest to the updated location responds), and other standard operating procedure considerations so everyone within an organization uses TAK in the same way. All users are required to complete basic training before accessing TAK. Additionally, Components may develop their own specific training to better fit their operational needs.

TAK servers, whether in physical data centers or in the cloud, allow for data auditing. These servers and the government-furnished equipment TAK adhere to DHS 4300A.

Conclusion

DHS uses TAK as a geospatial infrastructure and situational awareness application that allows for enhanced situational awareness, navigation, surrounding land formation intelligence, and data sharing. More specifically, it supports the complex communication and coordination needs of Components and the multi-jurisdictional response activities they engage in as part of their authorized missions. As part of TAK deployment, DHS Components work with their respective Privacy Offices to ensure the technology is used in a manner to protect PII and follows the measures laid out in this PIA.

Approval Signature

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

____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A: U.S. Customs and Border Protection

The CBP Team Awareness Kit (TAK) technology enables users to see the location of friendly forces and assets, visualize the operating environment, and ingest and display threat data from existing surveillance capabilities. In addition, CBP may use data derived from the TAK application to measure agent response times to sensor alarms and rescues and better coordinate ground personnel with CBP assets operating in the Air and Marine domains.

When the CBP officer or agent launches the TAK application, other TAK users, CBP assets, and (based on mission need) Tactical Operating Centers will be able to see real-time CBP officer and agent locations (as well as non-CBP TAK users in the same TAK user group), tactical infrastructure, shared images and chats, and CBP assets deployed in the area, while also receiving sensor alarms from those assets. Users can also filter the data based on certain characteristics. Location data is immediately sent to the TAK server and continues to be collected until and unless the TAK user closes the app, thus turning off all functions, including location services.

CBP does not maintain PII on subjects in TAK but may share photos that indicate recent travel by foot, landmarks, or other perishable intelligence, which may later be associated with an individual in another enforcement system.

CBP has developed TAK Initial Operating Procedures, which delineate Rules of Behavior and expectations. In addition to the initial operating capability, CBP provides TAK training to all users, including TAK Administrator (Power User) and standard end user training. All current TAK users, including non-CBP users have been trained and have signed a participation form which explains what data is being collected by TAK. TAK data will be retained for two years. Retention of data will assist CBP in doing data analysis and to help identify capability gaps with regard to response times.

Applicable SORN(s)

- DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 Fed. Reg. 72601 (October 20, 2016)

Appendix B: U.S. Immigration and Customs Enforcement

ICE Homeland Security Investigations (HSI) uses the Team Awareness Kit (TAK) mobile application to promote situational awareness, agent safety, and accountability. TAK also facilitates coordinated operations involving multiple Law Enforcement (LE) elements (or levels of LE participation). HSI personnel will have the TAK application loaded onto their government-issued mobile device (smart phone or tablet) and will be able to share tracking and location information as well as potential threats or points of interest in a real-time manner. When authorized HSI users launch the mobile application, other HSI agents in the same TAK user group will be able to see each user's location in near real-time. During an operation, the agent's location data is viewable until such time that the agent closes the mobile application. TAK users may share and retain specific data types on the device until the end user deletes the data. Examples include internal Short Message Service (SMS) (like "chat" messages between TAK users), map markers, and photographs/videos.

All information necessitating or related to criminal investigation is stored in the Investigative Case Management (ICM) system. TAK information will be retained in accordance with General Records Schedule 5.2 Item 020, Intermediary Records. Information that becomes part of an HSI case file is retained in accordance with N1-36-86-1-161.3.

HSI will provide end user training for all users before granting access to the TAK system. In addition, all HSI TAK users must agree to the Rules of Behavior.

Applicable SORN(s):

DHS/ICE-009 External Investigations, 85 Fed. Reg. 74362 (November 20, 2020)

Appendix C: U.S. Secret Service

The United States Secret Service (USSS) Office of Protective Operations uses the Team Awareness Kit Services system (TAKS) to enable near real-time location monitoring and display of USSS personnel carrying devices enabled for Team Awareness Kits (TAK). The main purpose is to facilitate coordinated responses to security incidents which may impact a Secret Service Protection Detail and/or which may also be needed to facilitate a subsequent criminal investigation. Special Security Events may also involve collaboration with non-Secret Service personnel, connecting the Secret Service TAK server with TAK servers of other agencies or law enforcement organizations, sharing location data and other situational awareness and mission-specific information. This information shared is "event" specific information, such as traffic shutdowns, security perimeters for public safety, and tactical communications details.

Management of the personnel working within proximity of an incident will be coordinated from a central hub (which may be at the USSS Headquarters Data Center or local Operations Center during Special Events). TAKS reports individual mobile users' geolocation (while their device application is open and monitors the location and movement of associated personnel nearby using their mobile devices with the appropriate TAK application. When the application is closed, a "disconnect" message is sent to the server removing the device from the display.

TAKS include a Chat Room feature which allows connected users to send and receive unrestricted text messages which may include other event-specific information. These chat sessions are retained on the user's device until explicitly removed by the user. Photographs taken from the mobile device may also be stored in TAKS as annotations to maps – such photographs will often include images of persons in the public area at the time of the photo. These maps are part of mission-specific information, and are removed/purged, along with all photos or annotations, at the end of a mission or event.

Applicable SORN(s):

DHS/USSS-004 Protection Information System, 85 Fed. Reg. 64519 (October 13, 2020)