Privacy Impact Assessment

for the

Assaults and Use of Force Reporting System (AUFRS)

DHS/CBP/PIA-045

August 24, 2017

Contact Point

Jaron Monholland

Law Enforcement Officer/Agent Safety and Compliance Directorate

U.S. Customs and Border Protection

(304) 724-5842

Reviewing Official

Philip S. Kaplan

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717

Abstract

The Assaults and Use of Force Reporting System (AUFRS) is a U.S. Customs and Border Protection (CBP) web-based application that allows all CBP components to record and track incidents involving assaults against CBP employees, use of force incidents, reportable firearms discharges, and vehicle pursuits by CBP law enforcement agents and officers (CBP LEO). AUFRS makes it possible for CBP leadership and the Law Enforcement Officer/Agent Safety and Compliance Directorate (LESC) to compile and analyze data related to all such incidents to better evaluate the effectiveness of policy, training on the use of force, and deployment of less-lethal devices.[1] CBP is conducting this Privacy Impact Assessment (PIA) because AUFRS collects personally identifiable information (PII) about subjects, witnesses, and CBP employees involved in these incidents.

Overview

CBP's primary mission is to safeguard America's borders, protecting the public from dangerous people and materials while facilitating legitimate travel and trade. In the course of executing this mission, incidents involving assaults against CBP employees or the use of force by CBP LEOs may occur. CBP uses AUFRS to record all such incidents, to include vehicle pursuits and reportable firearms discharges by CBP LEOs. Collection of this data may allow CBP to better evaluate the effectiveness of policy, training on the use of force, and deployment of less-lethal devices by CBP LEOs. The system also enables CBP to track and analyze use of force in response to assaults against CBP LEOs.

The CBP Commissioner mandated the creation of AUFRS in response to audits and reviews of the use of force by CBP LEOs and assaults committed against them.[2] One primary finding was that there was incomplete reporting of assaults and, as a result, insufficient documenting of how the use of force by LEOs correlated to the threat environment they faced, including how often assaults were not answered with force. Proposed actions to carry out the recommendations generated by this review included incorporating the existing CBP Use of Force Reporting System (UFRS)[3] and component assault information collection capabilities, most notably the United States Border Patrol's (USBP's) E3[4] Assaults Module, into a single agency-

[1] CBP LEOs are trained and Use of Force Center of Excellence (UFCE)-certified in the use of less-lethal devices/techniques: empty-hand strikes; Oleoresin Capsicum (OC) Spray; Collapsible Straight Batons (CSB); Electronic Control Weapons (ECW); Compressed Air Launchers; Munition Launchers; Less-Lethal Specialty Impact - Chemical Munitions (LLSI-CM); Controlled Tire Deflation Devices (CTDD); or other less-lethal devices approved by their operational component, with the concurrence of the Director of UFCE.
[2] *See* DHS Office of Inspector General, *CBP Use of Force Training and Actions to Address Use of Force Incidents*, September 2013, *available at* https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-114_Sep13.pdf.
[3] CBP plans to decommission UFRS with the deployment of AUFRS.
[4] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT and subsequent update, *available at*

wide system (AUFRS). Additionally, the consolidated system would also provide a platform to correlate information documenting assaults on CBP personnel with use of force incidents in response to those assaults. CBP established a high-level, cross-component working group to develop AUFRS. The CBP Commissioner later mandated the addition of a vehicle pursuit tracking function, which was initiated through another similar working group.

CBP's use of force policy[5] is included in the *CBP Use of Force Policy, Guidelines and Procedures Handbook*,[6] which outlines thresholds for recording use of force incidents and reportable firearms discharge incidents. While this policy is currently in revision, over time, various memos have been issued by LESC and the operational components to clarify recording and reporting requirements.[7] Under CBP policy and the rules governing AUFRS, CBP LEOs must report:

- Any use of deadly force;
- Any intentional deployment of a CBP less-lethal device or any use of a weapon, physical tactic, or technique that delivers (or is intended to deliver) a kinetic impact to a subject or results in serious physical injury or death;
- Discharges of a CBP-issued firearm including unintentional discharges and intentional discharges other than during training, practice, or qualification that do not cause injury to any person or animal or unintentional damage to private, public, or government property;
- Discharge of any firearm in violation of any law or ordinance, or that causes an investigation by any law enforcement agency, or appears to be discharged in an unsafe or reckless manner, is an act of assault against any CBP employee related to his or her CBP employment, or a discharge of a firearm by any law enforcement officer other than the authorized officer/agent when it occurs during multi-agency operations involving CBP personnel;
- All assaults on CBP government personnel associated with the execution of their duties; and
- All vehicle pursuits involving CBP personnel as driver or passenger in a pursuit vehicle.

https://www.dhs.gov/privacy.

[5] CBP policy on the use of force by Authorized Officers/Agents is derived from constitutional law, as interpreted by federal courts in cases such as Graham v. Connor, 490 U.S. 386 (1989) and Tennessee v. Garner, 471 U.S. 1 (1985), Federal statutes, and applicable DHS and CBP policies.

[6] *See* CBP *Use of Force Policy, Guidelines and Procedures Handbook* (May 2014), *available at* https://www.cbp.gov/document/guidance/final-use-force-policy-handbook.

[7] For example: Austin L. Skero, II, Exec. Director, LESC. (January 31, 2017). *Clarifying Reportable Assaults and Uses of Force*.

AUFRS reporting occurs concurrent with any reporting required by CBP, its operational components, or local chains of command. AUFRS is the only system that records this information agency-wide, across all CBP components, and in a consistent manner. Policy for vehicle pursuit reporting is still in draft form,[8] but all data collection and reporting elements established by the vehicle pursuit working group have been incorporated into the system. Because all CBP employees are potentially subject to assault while performing their duties, AUFRS must be accessible to any CBP employee at all times for inputting reports of such incidents.

AUFRS replaced and greatly expanded the recording and reporting functions of UFRS, which was designed around the hardcopy CBP Form 318.[9] CBP developed Form 318, *Reportable Use of Force Incident Data*, to capture incidents in which officer/agent force was used, what kind of force was used/how it was applied, and any gaps in training or issues with equipment that might have caused the incident to be less than successful. CBP has replaced this form with the AUFRS Incident Report, which reflects the data recorded into each AUFRS incident record. For USBP incidents involving assaults, AUFRS also produces an automated version of U.S. Border Patrol Form G725, *Report of Assault on Service Employee*.

AUFRS leverages a web service provided by the E3[10] system team to pull both CBP employee and subject data into AUFRS for the end user. Most of the incident data in AUFRS is entered manually by CBP employees in accordance with business rules built into the system that assist the user and help ensure the accurate and complete recording of required and complete incident information. CBP policy requires that reports be finalized in the system within 72 hours of an incident, after being subject to review and approval by designated CBP supervisors.

In order to properly identify CBP LEOs involved in each incident, the CBP employee Hash ID[11] is used as the primary identifier when adding involved employees to an incident report. It is displayed in one table within the system. Involved employees' first, last, and middle names are also recorded, along with gender, age, height, weight, duty location, entry on duty (EOD) dates, and previous training data.

First, last, and middle names may be used to identify involved subjects, witnesses, and injured bystanders. Additionally, gender, date of birth, height, weight, immigration status, and country of citizenship may also be collected about involved subjects to further identify them. The system uses standardized terminology, Unknown-1, -2, etc., to document unidentified subjects.

---

[8] Operations Support Office. (March 2017, draft). *Emergency Driving Including Vehicular Pursuits by U.S. Customs and Border Protection Personnel*.
[9] *Use of Force Policy Handbook* (October 2010), *available at* https://www.dhs.gov/sites/default/files/publications/cbp-use-of-force-policy.pdf.
[10] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT and subsequent update, *available at* www.dhs.gov/privacy.
[11] Hash ID is unique CBP employee identifier derived from the Social Security number.

Injured bystanders may also be recorded as Unknown. CBP may also record witness addresses, for contact and follow-up purposes, although this is not required information.

Section 1.0 Authorities and Other Requirements

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

CBP is authorized to collect information within AUFRS through CBP's mandate to gain operational control of the U.S. border as codified by 8 U.S.C. § 1357 and 8 U.S.C. § 1103(a)(5).

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

AUFRS relies on information from underlying enforcement systems to populate and update the system for accurate reporting. CBP maintains records related to its efforts to secure the U.S. border between official Ports of Entry (POE) in accordance with the Border Patrol Enforcement Records (BPER) SORN.[12] In particular, the BPER SORN governs records relating to encounters of individuals between official POE, which may include information about Border Patrol Agents and assaults made against them, as well as the use of force that may be exercised during such an encounter. Records of assaults against CBP Officers at a POE are covered by the TECS (not an acronym) SORN,[13] which covers information regarding individuals, firms, and organizations to whom DHS/CBP has issued detentions and warnings.

The information created by CBP LEOs within the AUFRS system is covered by the forthcoming CBP Intelligence Records System SORN,[14] which covers information created using underlying law enforcement and intelligence information. Records maintained in the CIRS SORN support CBP's collection, analysis, reporting, and distribution of law enforcement, immigration administration, terrorism, intelligence, and homeland security information in support of CBP's law enforcement, customs and immigration, counterterrorism, national security, and other homeland security missions. The CIRS SORN is expected to be published in the Federal Register in September of 2017.

[12] *See* DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).
[13] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[14] Forthcoming September 2017.

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

Yes. AUFRS has undergone the Security Authorization process in accordance with DHS and CBP policy, which complies with federal statutes, policies, and guidelines. The system is expected to receive a renewed Authority to Operate pending the publication of this PIA.

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

CBP is working to develop a records retention schedule for NARA approval. Consistent with the BPER SORN, CBP intends to retain records in AUFRS relating to arrests, detentions, and removals for 75 years. Investigative information not resulting in arrest, retention, or removal should be retained for 20 years after the investigation is closed, consistent with N1-563-08-4-2. CBP maintains user account management records for ten years following an individual's separation from federal service; statistical records for ten years; audit files for fifteen years; and backup files for one month.

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.

Due to the law enforcement nature of this information collection, all information maintained within AUFRS is not covered by the Paperwork Reduction Act.

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.

AUFRS collects and uses PII about CBP employees, subjects, witnesses, and injured bystanders. A detailed description of PII collected is presented below.

CBP Employees:

- Name (first, middle, last);
- Hash ID (unique employee identifier derived from the Social Security number);

- Gender;
- Age;
- Height;
- Weight;
- Service Entry on Duty (EOD); and
- Duty location.

Other information collected regarding employees relates to their involvement in the incident and is not PII, specifically:

- Duty status (*e.g.*, on or off duty);
- Years of armed law enforcement experience and CBP training received other than basic;
- Apparel, including body armor;
- Whether the employee was assaulted;
- Whether the employee used reportable force, and if so the specifics of each use of force;
- If applicable, whether the employee took part in a vehicle pursuit, and if so the employee's role and other vehicle information;
- If applicable, whether the employee discharged a firearm in a reportable, non-use of force manner, and if so, the particulars of that discharge; and
- Whether the employee was injured, and if so, treatment received.

Subjects:

- Name (first, middle, last);
- Gender;
- Date of birth;
- Height;
- Weight;
- Immigration status (not required); and
- Country of citizenship (not required).

When a subject is unidentified (for example, one who absconds during the incident), the fields listed above may be designated "unknown" or may be estimated within a range. Other information collected regarding subjects related to their involvement includes:

- The subject's activity during the incident;
- Any assault committed by the subject, including weapon information and whether or not the subject was within the U.S. border;
- Whether force was used against the subject;
- If applicable, the subject's involvement in a vehicle pursuit, including role and vehicle information;
- The subject's current location, if known; and
- If the subject was injured (or claimed to be injured), injury and treatment information.

Witnesses:

- Name (first, middle, last - only last name is required); and
- Address and phone - not required.

Witness statements are also collected and may include additional PII.

Injured Bystanders:

- Name (first, middle, last); and
- Gender.

Injured bystanders may be unidentified, so the fields listed above may be entered as unknown. Other information collected regarding injured bystanders relates to their injuries and treatment and does not generally include PII.

The remaining information collected in AUFRS related to the incident includes the following:

- Incident type(s) - assault, use of force, vehicle pursuit, reportable firearms discharges (non-use of force or unintentional);
- Involved organizations, internal to CBP and external;
- Incident location and environment;
- Qualitative narrative and descriptive information;

- Other individuals and agencies notified at the time of the incident (not part of an AUFRS report);
- Interrelationship of specific assaults, injuries, and uses of force;
- Vehicle pursuit information, such as who initiated or terminated the pursuit, involved vehicles, route, duration, speed, and contraband seized;
- Collateral damage information (for property damage whether it was private or government property, a description of the damage, and an estimated value; for personal injury, the name and gender of the injured party - only last name is required, both name and gender may be recorded as unknown - the cause and degree of the injury, and the treatment received, if any);
- References to related documents in other systems, if any;
- Attached files, if any; and
- Changes to the report audit logs.

CBP uses the data collected in AUFRS to create a report for each incident. The data in the AUFRS incident report can be printed out as an AUFRS Incident Report, and labeled with a unique report ID number. If an assault on USBP personnel is involved, Form G725, *Report of Assault on Service Employee*, may also be printed out.

Aggregate statistical data reports, such as the distribution of assaults across CBP locations, may be generated from the system for analysis. These do not contain any personal or incident-specific data.

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

The primary sources of the incident information in AUFRS are CBP employees involved in the incident and their supervisors. The information is either manually entered into the system by CBP employees (usually one of the involved employees or his/her supervisor) or attached in relevant files (involved CBP LEO or supervisor memos, photographs, etc.). AUFRS may also import information from E3,[15] Border Patrol Enforcement Management System 2 (BPETS2),[16] and WebTELE, CBP's internal personnel directory.[17]

[15] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT and subsequent update, *available at* www.dhs.gov/privacy.
[16] CBP intends to publish a PIA for the Border Patrol Enforcement Management System 2 (BPETS2) in August 2017. When published, the PIA will be available at www.dhs.gov/privacy.
[17] For more information about WebTELE, please *see* DHS/CBP/PIA-043 CBPnet, *available at* www.dhs.gov/privacy.

Users creating an AUFRS record may import some information from E3 via an internal web service. This is a one-way, one-time data pull, with no further crosschecks or updates between E3 and AUFRS once the data is imported. Such information includes minimal subject data, including: name, height, weight, date of birth, immigration status, and country of citizenship; and CBP employee data only consisting of the employee's Hash ID. This information is imported for ease of use and to ensure that incident data is consistent across both systems. The E3 system is the primary system for USBP to record enforcement actions, and thus most AUFRS incidents that involve USBP will have an associated E3 event. Importing the subject and CBP employee data from E3 helps prevent errors that might otherwise occur if attempting to copy information manually between systems.

When a user accesses AUFRS, information is imported from BPETS2 and WebTELE, to determine the user's assigned area of responsibility. If a user has a BPETS2 account, the duty location in BPETS2 is used as the area of responsibility. For all other CBP employees, the WebTELE duty location will be documented as their area of responsibility. This is done to ensure that users will only have access to the data required to properly document and report any incident that should be reported within AUFRS.

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, the project does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

To ensure the accuracy of information in the system, incident reports are usually created by the CBP LEO involved, or someone else with knowledge of the incident. He or she controls the information initially entered into the report. Further, as the creator of the report, only he or she may enter and edit the report's qualitative "Narrative" data field, which is a text description of what took place in the incident.[18] The creator may also attach files to the report, such as CBP employee memos and photographs, which only the creator may detach later. Other CBP employees with edit access to the report (involved CBP employees and supervisors) may comment on the Narrative through an Addenda field, and may also add attachments of their own. The exception is for incidents involving the use of deadly force, where only a supervisor may create or edit the report. In such instances, involved employees will have read-only access to the report. Information

[18] Only employee and subject names are included in the narrative. The purpose of the narrative is to lay out the actions of the participants, not their particulars. The contents reflect the memos that agents and officers provide relative to such incidents. Additional training is not relevant, as these memos may be attached in lieu of a typed-in narrative.

recorded in AUFRS reflects information already reported in other venues, such as involved CBP LEO and supervisor incident memos, the E3 system, and Significant Incident Reports (SIR).[19] Narrative information, such as that found in the memos, may be attached directly to the AUFRS incident report and limited CBP employee/subject information may be imported from E3 to avoid errors in adding this information to AUFRS. References to other systems with applicable documentation, such as SIRs, are collected through one of the AUFRS tabs. While some of the information collected in AUFRS can be looked up in other systems, there is no technical verification that occurs within the system to determine if the information is accurate. Some of the information (such as height and weight) can vary slightly and is considered to be approximate. However, the fields may still be required for submission of an incident.

AUFRS employs a comprehensive set of business rules to help ensure that users only enter data that is complete, necessary and relevant to document assaults, use of force incidents, reportable firearms discharges, and vehicle pursuits. These business rules include: required completion of compulsory fields before users are allowed to submit information; cascading logic that will activate certain fields based on answers to previous fields; and cross-checks and navigation warnings that alert the user to specific areas of the application that are missing required information.

Additionally, online training and reference documents are available to guide individuals on the use of the system. These training tools are updated on an as needed basis, and when functionality is added or changed within the system. They are readily available to all AUFRS users, and a link to them is provided through the "Help" option on the AUFRS menu. There is also a training site available to all users for self-guided training and exploration of the system in a non-production environment; this link is also available through the "Help" option. LESC also maintains a branch dedicated to reviewing the statistics and integrity of the data and the proper business requirements of the system. AUFRS includes contact information to reach this group directly for questions and comments regarding the system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that inaccurate information may be entered in AUFRS.

Mitigation: This risk is partially mitigated. CBP LEOs receive training in law enforcement legal matters during basic training. Criminal law courses teach CBP LEOs to recognize violations of federal criminal statutes and either take appropriate action, with regard to laws under DHS purview, or make referral to another federal agency of primary jurisdiction. CBP LEOs are trained on the requirement to accurately document any incident, as well as evidentiary standards and

[19] *See* DHS/CBP/PIA-039 CBP Situation Room (SITROOM) (February 27, 2017), *available at* https://www.dhs.gov/privacy.

collection of evidence. LESC provides training in how to describe what transpires during an incident or arrest to CBP LEO instructors. In addition, the AUFRS interface breaks out specific data points to be recorded, so the CBP employee is not left to decide what to include in the AUFRS record. An objective narrative account of the event is collected, which should reflect information already captured in CBP employee or supervisor memos. CBP employees retain access to their involved reports and may edit them until they have been submitted. Subsequent to submission, employees retain viewing access to the reports in order to discuss such reports with supervisory staff. Each report is reviewed and approved by a supervisor familiar with the incident, but not directly involved, and then undergoes a subsequent review by LESC staff to ensure completeness and compliance with CBP reporting policy. There remains some risk that information in AUFRS may be inaccurate, since it relies on manual data entry. The impact of this risk is mitigated by the fact that CBP uses information in AUFRS for tracking and reporting purposes, and not as the sole source of information for taking action against an individual involved in an incident.

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.

CBP uses the data in AUFRS to analyze individual incidents and overall trends related to the threat environment facing CBP employees, and the likelihood of employing use of force in that environment. CBP uses this analysis to adapt policy on weaponry, tactics, and training, as necessary and appropriate. For example, if a less-lethal device initially introduced in one area is shown to be effective in neutralizing a situation with minimal negative effects, that device may be deployed throughout the field. Conversely, if a less-lethal device is shown to be ineffective, additional training might be developed to make it more effective or its use might be terminated. Because incident information is recorded in AUFRS after it is initially recorded elsewhere (*e.g.*, through CBP employee and supervisor memos and, if applicable, in SIRs and in the E3 system), AUFRS incident reports are not considered to be primary sources, although they may be discoverable in a legal proceeding.

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.

CBP may analyze AUFRS records related to incidents involving assaults on CBP employees, use of force incidents, reportable firearms discharges, and vehicle pursuits; however, the system does not conduct electronic queries, searches, or analyses.

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

No. Access to AUFRS is limited to CBP employees only and that access is limited by their area of responsibility and assigned access level within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: The primary risk to the PII in AUFRS is the interception of the data or misuse of the data by CBP employees.

Mitigation: To minimize this, AUFRS has a security module that limits the access of users based on an access role, area of responsibility, and involvement in a particular incident. Access to the security module is controlled by LESC and system access roles beyond default CBP employee access are granted only as needed. CBP components may grant access to information above default level to their own employees and only for their own incidents. The system database also uses an audit log that tracks changes made to incident reports, including who made those changes, the nature of the changes, and a time-stamped snapshot of the incident report following each session of changes.

Reports containing data from the system are provided in standard formats and are denoted with "For Official Use Only" or other applicable statement.

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.

CBP employees are generally aware of their information in AUFRS since they are the source of the record, or are provided the opportunity to review the record. Although subjects and witnesses involved in the incidents are typically aware that CBP is collecting their information after an incident, they may not have specific notice that their information is maintained in AUFRS. CBP is publishing this PIA to provide general notice to the public that AUFRS may maintain information related to use of force events.

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

By policy, involved CBP employees may be required to enter information into the system for incidents not involving the use of deadly force. For deadly force incidents, a supervisor will be responsible for creating the incident report. Local chain of command sometimes creates its own procedures for incident recording as well.

Information collected regarding subjects may not be available for individuals who abscond or otherwise are not available for questioning. While information fields for subjects may be required, "unknown" is an available option for all such fields if the subject is not available or declines to provide the information.

Information collected regarding witnesses is entirely voluntary. If added to AUFRS by a CBP employee, none of the fields other than last name of the witness(es) are required.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that involved CBP employees and members of the public may not be aware that their data is in AUFRS if they are not the creator of or contributor to an incident report.

Mitigation: All CBP LEOs are trained on the requirement to report incidents. Involved CBP employees will either be the creator of the incident report or contribute to it, except for deadly force incidents. Nevertheless, CBP LEOs will no doubt be aware of the AUFRS incident report and will have access to it. All information collected regarding CBP employees is either collected directly from the employee, the employee's supervisor, or imported from another system (minimal E3 imported information). However, the report will show up in each involved CBP employee's "Home" screen when they access AUFRS. All CBP government employees have access to the system, but that access is limited to their area of responsibility, involvement in specific incidents, and role in the system as determined by their component. Subjects and witnesses may not be aware of the AUFRS system specifically, but they are aware that CBP has gathered their information (which for witnesses is typically voluntarily provided) pursuant to an incident.

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.

Incident reports are retained indefinitely in AUFRS because the system's purpose is to look for trends in threats and responses to those threats across as long a time span as possible. CBP is in the process of working with NARA to establish an appropriate records schedules for AUFRS.

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: This risk cannot be mitigated until a records retention schedule is in place. CBP is in the process of working with NARA to establish an appropriate records schedules for AUFRS. Consistent with the BPER SORN, CBP intends to retain records in AUFRS relating to arrests, detentions, and removals for 75 years.

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.

The AUFRS owning organization, LESC, does not routinely share PII or incident specific information outside DHS or with other government components or outside entities as part of normal operations. There are occasional Freedom of Information Act (FOIA) and other requests that require sharing on an as-needed bases, but such requests are normally handled through other CBP offices that are responsible for the redaction of PII and other sensitive information (*e.g.*, law enforcement tactics, weapons, and other sensitive information as appropriate to each request). Aggregate numeric statistical information is routinely published by the Office of Public Affairs, but this does not include any PII or incident specific information other than overall incident locations (sectors, stations, field offices, ports of entry, etc.) and assault and use of force types.

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

Any sharing of data will occur in accordance with the provisions of the Privacy Act (5 U.S.C. § 552a). This sharing will typically involve FOIA requests or law enforcement disclosures. To that extent that information is shared compatible to the SORNs listed in Section 1.2, the information will be shared pursuant to the routine uses of the applicable source systems.

6.3 Does the project place limitations on re-dissemination?

Because PII and incident specific information from AUFRS is not shared outside of DHS as a part of the normal agency operations, specific limitations have not been set, other than existing agency, Department, and U.S. Government-wide existing limitations.

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

LESC does not routinely share information outside of DHS; there is no direct access to AUFRS outside CBP; and information released by other CBP components must follow accounting for disclosure requirements.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no privacy risk to AUFRS information sharing. LESC does not routinely share information outside of DHS, there is no direct access to AUFRS outside CBP, and information released by other CBP components is subject to redaction. Therefore, there are no particular privacy risks confronting the system project, nor is additional mitigation required.

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?

AUFRS is only available through the internal CBP website, CBPnet, and only to CBP employees as they log onto the web. The CBP employee's existing level of access to AUFRS controls what he or she may see and do in the system. Level of access is governed by each user's roles, which may be set by each of the CBP components in accordance with its own needs and requirements. Details of these roles are included in Section 8.3.

Subjects and witnesses will not be aware of the system but must rely on this PIA and the

CIRS SORN to determine if their PII exists in AUFRS.

The CIRS SORN asserts exemption from the access, correction, and amendment provisions of the Privacy Act. However, such exemptions are reviewed in the context of each request. To seek access to information collected through AUFRS, U.S. Citizens and Lawful Permanent Residents may request information about themselves, pursuant to the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)) or pursuant to FOIA (5 U.S.C. § 552).

Any individual, regardless of citizenship or immigration status, may seek notification of or access to any CBP record contained in AUFRS pursuant to procedures provided by FOIA, and can do so by visiting https://www.cbp.gov/site-policy-notices/foia, or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, DC 20229

When seeking records about one's self from any of the system of records listed in Section 1.2 of this PIA or any other Departmental system of records, the request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information. The individual must first verify his or her identity, meaning that the requestor must provide his or her full name, current address, and date and place of birth. The requestor must sign his or her request, and the signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While an inquiry requires no specific form, forms may be obtained for this purpose from the Chief Privacy Officer and Chief FOIA Officer, https://www.dhs.gov/freedom-infomration-act-foia or 1-866-431-0486. In addition, the request should:

- Explain why the requestor believes the Department would have information on him or her;
- Identify which component(s) of the Department the requestor believes may have the information about him or her;
- Specify when the requestor believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

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

The originating CBP employee and all involved employees retain access to each report, even after it has been submitted and approved as completed. Should the CBP employee take issue with subsequent edits to the report, he or she may discuss that with a supervisor or others in the chain of command. Subjects and witnesses are unlikely to be aware of any inaccurate information in the system; however, if they do suspect CBP's records related to them are inaccurate, they may seek redress under the Privacy Act and FOIA request processes.

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

All CBP employees have access to an AUFRS training and reference document that describes fully system access and usage. They may also contact LESC AUFRS staff directly with any questions regarding those or any other aspect of the system. For subjects and witnesses, this PIA and the CIRS SORN provide notice of FOIA and Privacy Act procedures to request access to or correction of their records.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for records in AUFRS.

Mitigation: This risk is partially mitigated. CBP employees have the ability to view all AUFRS records in which they have been a party to an assault and therefore can amended the record or work with their supervisor to amend the record. Members of the public who may have been named as witnesses or subjects of the assault, may reference this PIA and the CIRS SORN.

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

In addition, providing individual access or correction of AUFRS records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in AUFRS, regardless of a subject's citizenship, could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or

evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Privacy Risk: Due to the law enforcement nature of the information within AUFRS, there is a risk that individuals will not be able to access, correct, or amend their records.

Mitigation: This risk is partially mitigated. Information from certain CBP source systems may be amended as indicated in the CIRS SORN. For AUFRS records, individuals can seek access, correction, and amendment of information from the underlying source system SORNs, depending on the location of the incident (TECS for incidents at a Port of Entry and BPER for incidents between Ports of Entry).

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

Section 8.0 Auditing and Accountability

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?

Access to AUFRS is limited to CBP users, who must be trained on their responsibilities regarding incident reporting and the appropriate use of the system. AUFRS features built-in access controls that govern each user's assigned roles. CBP does not share information from AUFRS outside of the agency and accordingly, does not need special procedures governing use of the information outside of CBP.

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

All CBP employees must take annual privacy awareness training, which includes training in need to know and other aspects of information handling. There is no requirement for AUFRS-specific privacy training, due to the controlled access to and lack of information sharing from the system. Each screen in the system is Sensitive But Unclassified (SBU) / For Official Use Only (FOUO).

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

AUFRS is only available through the internal CBP website, CBP.net, and only to CBP employees. Access is governed by each user's roles, which may be set by each of the CBP components in accordance with its own needs and requirements. By default, all federal CBP employees have basic access to AUFRS, since any CBP employee may potentially be required to report an incident during the execution of his or her duties. This basic AUFRS access allows employees to create an incident report. Any other CBP employees involved in the incident may also access and edit the report, as may anyone assigned the AUFRS Supervisor role whose area of responsibility covers that of the report. Only the CBP employee creating the report may enter and edit the report's qualitative Narrative data field, which is a text description of what took place in the incident. The creator may also attach files to the report, such as employee memos and photographs, which only the creator may detach later. Other CBP employees with edit access to the report (*i.e.*, involved employees except for incidents involving the use of deadly force and supervisors) may comment on the Narrative through an Addenda field accompanying the Narrative field and may also add attachments of their own.

CBP employees may be given read-only access to reports within their components' organizational hierarchy outside their own areas of responsibility, on a need to know basis, as determined appropriate by the employees' chain of command. For example, one may be able to see all incidents within his or her sector in read-only mode (that is, with no ability to make changes) to gain an understanding of the changing threats occurring along neighboring sections of the border.

These roles are assigned by an AUFRS Administrator, whose assignment as an Administrator is managed by his or her local or component's chain of command. AUFRS Administrators may be limited to a particular location or to a hierarchical tree of locations at any level within their component.

LESC AUFRS System Administrators are assigned to review all reports for data integrity and to help the components and individuals utilize the system on an as needed basis. These System

Administrators can grant Administrator access to component personnel as necessary, for example, to establish an Administrator at HQ level within a component who may then assign additional Administrators and Supervisors throughout the component's organizational hierarchy.

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?

CBP does not plan to offer access to AUFRS to external users, but if that occurs in the future, memoranda of understanding (MOU) will be reviewed by the program owner, the CBP Privacy Office, and the CBP Office of the Chief Counsel prior to sharing information outside of CBP. In addition, CBP would implement changes to the structure of CBP system security and system access to accommodate external users.

Responsible Officials

Jaron Monholland
Law Enforcement Officer/Agent Safety and Compliance Directorate
U.S. Customs and Border Protection
(304) 724-5842

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

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security