Privacy Impact Assessment
for the

# Workbench 2.0

**DHS/CBP/PIA-042**

**May 8, 2017**


**Contact Point**
**Dalia Putnam**
**Chief, Communications Center of Operations**
**National Law Enforcement Communications Center (NLECC)**
**(407) 975-2100**

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

## Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) Workbench 2.0 is a web-based application used by CBP, Office of Information and Technology, Sector Enforcement Specialists (SES) at the National Law Enforcement Communications Center (NLECC) to provide secure radio, email, and telephonic services and support to more than 70,000 federal law enforcement officers. Once these subscribers are registered in Workbench 2.0, they are authorized by CBP to submit verbal and written requests for information for law enforcement purposes. CBP is conducting this Privacy Impact Assessment (PIA) because Workbench 2.0 processes personally identifiable information (PII) on DHS employees and contractors, personnel from other federal agencies, and members of the public.

## Overview

CBP Workbench 2.0 ("Workbench") is a web-based application used by Sector Enforcement Specialists (SES) staff at the National Law Enforcement Communications Center (NLECC), part of U.S. Customs and Border Protection's (CBP) Office of Information and Technology located in Orlando, Florida, to provide secure radio, email, and telephonic services and support to more than 70,000 federal law enforcement officers (also known as subscribers). These subscribers require NLECC services when they are away from their desks (*e.g.*, out in the field) and require information on active cases. The NLECC Land Mobile Radio (LMR) Network is designed to provide radio coverage along the perimeter of the United States and other areas frequented by authorized subscribers. The subscribers using the NLECC do not have local radio dispatch facilities and SES staff monitor calls 24 hours a day, 7 days a week, as a means of providing the emergency support required by the subscribers. To avoid the significant costs required to acquire the infrastructure for radio networks, at least 30 external agencies have signed agreements with the NLECC to provide law enforcement support and radio monitoring for authorized subscribers within their agency.

CBP permits Workbench subscribers to submit verbal (*i.e.*, phone and radio) and written (*i.e.*, email) requests for information for law enforcement purposes. These subscriber requests could include: coordinating tasks with other law enforcement officers, sending out administrative messages for lookouts, and entering fugitive and lost/missing/stolen federal property information in the National Crime Information Center (NCIC). In addition to radio, email, and telephonic services, Workbench stores the data collected from subscribers and search parameters used by SES staff when the following actions are conducted: 1) criminal history queries, 2) informant calls, 3) Be-Alert Program hotline calls, 4) private vessel/small boat entries, 5) vehicle registration checks, and 6) financial database queries. The NLECC is a centralized source for support and information to various subscribers located in the field that require emergency or other law enforcement

information and support.

**Criminal History Checks**

SES staff may conduct the law enforcement queries at the request of Workbench subscribers and respond back with the information found by searches of the separate law enforcement systems listed below. Appendix A includes a brief description of each system.

- TECS
- National Crime Information Center (NCIC)
- National Law Enforcement Telecommunications System (Nlets)
- Computer Linked Application Information Management (CLAIMS)
- Enforce Alien Removal Module (EARM)
- Central Index System (CIS)
- Student Exchange and Visitor Information System (SEVIS)
- Automated Targeting System (ATS) Passenger (ATS-P) and Land (ATSP-L)
- Analytical Framework for Intelligence (AFI)
- National Insurance Crime Bureau (NICB)
- Department of State Consular Consolidated Database (CCD)
- LexisNexis (ACCURINT)
- State Systems:
    - Florida Crime Information Center ((FCIC)/E-Agent)
    - Florida Driver and Vehicle Information Database (DAVID)
    - Pennsylvania Criminal Justice Network (PA CJNET)
    - Texas Law Enforcement Telecommunications System (TLETS)

**Informant Calls**

The NLECC is responsible for relaying information received from informants as necessary. Officers typically direct their informants to call into the NLECC to leave messages for them if they are in the field or unreachable. Often, these calls are diverted to U.S. Immigration and Customs Enforcement (ICE), CBP, and other law enforcement agencies within and outside of DHS. SES staff attempt to collect and record at least the name and callback number for these individuals in order to pass along to their respective officers.

**Be-Alert Hotline**

The purpose of the tip line is to provide citizens with a method to report violations of federal law enforced by CBP and ICE or the location of fugitives. The toll-free number established for this purpose is 1-800-BE ALERT (1-800-232-5378). The telephone number is routed into a telephonic voice mail system located at the NLECC and options allow callers to either leave recorded voice messages or speak with SES staff at the NLECC. A primary function of CBP and ICE is to initiate investigative or enforcement actions in response to violations of federal law enforced by their respective agencies. One of NLECC's functions is to ensure that information received that may be of investigative or enforcement interest is forwarded to CBP or ICE in a timely manner, and to support CBP and ICE law enforcement efforts regarding investigations and enforcement of federal law.

As the primary after-hours point of contact for many CBP and ICE offices, including Office of Professional Responsibility (OPR) offices, the NLECC often receives information from the public that may be accusatory in nature concerning the integrity of CBP or ICE employees, or other law enforcement personnel who may be working directly with CBP and ICE. SES staff attempt to obtain sufficient information to forward allegations to the Joint Intake Center (JIC)[1] for further action. These types of calls have restricted entries in the Master Station Log (MSL) and any reports or written records pertaining to these types of allegations are disposed of per agency guidelines. Once saved, these restricted entries are no longer accessible to any SES staff including the individual who documented the call; the entries are only accessible by supervisors who have a "need to know" in the performance of their official duties.

**Private Vessel/Small Boat Entries**

The NLECC provides after-hours support to certain seaports and records activity such as small boat entries. The SES staff gather all applicable information from the boater required for input into the Pleasure Boat Reporting System (PBRS) module in TECS[2] including: name, date of birth, citizenship, gender, address, estimated date and time of arrival, vessel name, manufacturer, registration/vessel identification number, length, decal number if available, foreign port of departure, port of arrival, name and number of pier where vessel is docked, and cruising permit number and date issued. The information on passengers includes: name, passport type and number, date of birth, and citizenship.

The above information is used by CBP officers to determine admissibility when they

[1] The Joint Intake Center (JIC) serves as the central "clearinghouse" for receiving, processing, and tracking allegations of misconduct involving personnel and contractors employed by CBP and U.S. Immigration and Customs Enforcement.

[2] For more information about the information input into the Pleasure Boat Reporting System (PBRS) module in TECS, please *see* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* https://www.dhs.gov/privacy.

meet the arriving vessels and conduct inspections.

### Vehicle Registration Checks

Subscribers may call the NLECC for information on vehicle registration. The NLECC's response to the subscriber of registration checks on conveyance (*i.e.*, vehicle, aircraft, boat) will be limited to the information requested unless additional information is obtained during the course of the checks that may affect officer safety, such as NCIC wants or possible TECS matches. Upon validating the requestor is an authorized NLECC subscriber with a "need to know" in the performance of his or her duties, SES staff will then only provide law enforcement information from systems such as the NCIC, Nlets, or federal, state, or local law enforcement systems. TECS information may only be disseminated to authorized users in accordance with TECS security guidelines.

### Financial Database Queries

ICE is tasked with investigating violations of federal statutes pertaining to financial regulations. An important source of this information is the Financial Database, which is a Dun & Bradstreet report found in TECS. Since many investigations are conducted outside normal office business hours, access to the information by ICE agents, criminal investigators, and other law enforcement officers may be of importance. Per legacy Customs Directive 4352-06, dated December 1, 1986, NLECC personnel are granted authorization to access the financial database for the purpose of providing after-hours access to this information to ICE.

## System Administration and Auditing

### SES Staff Onboarding and Training

SES staff are subjected to single-scope background investigations (SSBI) and receive their security clearances once on-boarded to the NLECC. SES staff are only government employees and are not contractors or detailed from CBP or any other agency. SES staff trainees must complete training and review multiple standard operating procedures (SOP)[3] before they are able to respond to subscriber's requests. The duration of role-based training depends on the previous background of each SES member. The average training period is four to eight months and includes three phases of training, each lasting several months. The first phase involves shadowing and observation of a senior SES member. In phase two, the trainee is assigned to a different senior SES member and starts taking calls under his or her guidance. In the third phase of training, the trainee works semi-independently under the supervision of a team leader.

[3] These SOPs include: a) Master Station Log; b) NCIC Criminal History Queries and Protection of Information; c) NCIC Procedures; d) Financial Database Queries; e) Registration Checks; f) Informant Calls; g) Receipt & Reporting Allegations of Misconduct; h) Be-Alert Hotline Procedures; i) Transmission of Personally Identifiable Information; j) Release of TECS Lane Crossing Information; and k) Private Vessel Reporting.

**Workbench Subscribers Onboarding and Authentication**

Several DHS components register each of their field agents into Workbench using Personnel Entry Data Sheets; the data is used to create subscriber profiles. These data sheets are completed and emailed into the NLECC, from government email addresses, in order to register users and then the data sheets are deleted. For non-DHS law enforcement agencies that request radio, email, and telephonic support for field agents, CBP completes Memoranda of Understanding (MOU). Like DHS, the agents of these offices/agencies also complete the Personnel Entry Data Sheets for creation of subscriber profiles. The agency name is captured in the "Office" tab. An "Office" tab is created in order to add subscribers to Workbench; this tab shows the subscriber permissions[4] for information that is releasable to them.

For confidentiality and brevity during radio communications, SES staff assign subscribers a "callsignID." NLECC develops callsignIDs based on factors such as the individual subscriber's job series and location. Subscribers are authenticated by SES staff via their: 1) callsignID; 2) last five digits of their Social Security number (SSN); or 3) credentials/badges. If requests are received via email, the subscriber's email is used to authenticate the NLECC user.

**Workbench Master Station Log (MSL)**

Given the sensitive subject matter provided, SES staff are required to document all of their actions in the MSL. The MSL consists of daily work logs for each 24-hour day. The log data is used for numerical analysis purposes to respond to audits, to measure analytical work conducted by SES staff, to determine the number of calls received from a particular agency, and to define the staffing requirements for any given date or time.

All OPR/Internal Affairs (IA) request-related log entries will be entered in the MSL with callsignIDs associated with subscribers in those offices. Once these log entries are saved, the MSL automatically hides these entries that relate to OPR/IA. While the entries are hidden to SES staff, they are visible to supervisors who have a "need to know." If these log entries are needed at a later date, requests have to be made to NLECC supervisors, ensuring that OPR/IA log entries are only available to those that have a "need to know."

The information captured in the MSL includes: 1) log entry date/time (auto-generated), 2) SES member name, 3) time activity occurred, 4) requestor (or subscriber) name, 5) action code(s),

[4] Permissions that can be assigned to subscribers of Workbench are: (1) LexisNexis (ACCURINT); (2) Border Crossing (ATS queries for DHS, CBP, and ICE only); (3) Emergency Services; (4) Immigration System Queries; (5) Local State System Queries; (6) NCIC Entries; (7) NCIC Queries; (8) Nlets Queries (*e.g.*, Driver's License, Registration, Criminal History); (9) OTAR (Over-the-Air-Rekeying) of radios; (10) TECS Authorized Subscriber; (11) TECS Financial (Currency and Monetary Instrument Reports (CMIR) Only); (12) TECS Financial (ICE Homeland Security Investigations (HSI), ICE Office of Professional Responsibility (OPR), CBP OPR, and DHS Office of Inspector General (OIG) only); (13) TECS Financial Not Authorized; and (14) TECS Not Authorized.

and 6) narrative. The narrative is a clear text field in which all pertinent information concerning an activity is described or commented upon. Results of actions or queries, elaboration of data entered in previous fields, and the narration of the sequence of events are examples of text that may be entered in this field.

The Workbench action codes consist of the following categories:

- Telephone/Radio;
- Workbench Actions (*e.g.*, actions taken by SES staff);
- Be-Alert Tip Line Actions;
- Administrative Actions (*e.g.*, SES member documenting when he or she was on break, SES staff training a newly hired SES staff trainee);
- Enforcement Actions (relates to actions taken by SES staff during an officer safety or emergency situation (*e.g.*, prisoner transport, vehicle pursuit, surveillance, evidence transport));
- TECS (relates to the different types of queries that are run (*e.g.*, car registration, criminal history));
- Automated Targeting System (relates to the different types of queries that are run (*e.g.*, person or vehicle));
- Immigration Actions;
- NCIC Actions;
- Nlets Actions;
- Florida (FL) State System;
- Massachusetts (MA) State System;
- New York (NY) State System;
- Pennsylvania (PA) State System;
- Texas (TX) State System;
- Canadian Nlets (CPIC);
- Communications Duty Officer (CDO) Actions; and
- Miscellaneous/Other Actions (includes LexisNexis (ACCURINT).

# 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 maintain Workbench under the following authorities: 5 U.S.C. § 301; 6 U.S.C. § 202; 8 U.S.C. §§ 1103, 1185, 1225, 1357, 1365a, 1365b, 1379, and 1732; 18 U.S.C. § 27; 19 U.S.C. §§ 482, 1461, 1496, 1581, and 1582; 44 U.S.C. §§ 3101 and 3534; Homeland Security Act of 2002 (Pub. L. 107-296); Justice for All Act of 2004 (Pub. L. 108-405); Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458); Secure Fence Act of 2006 (Pub. L. 109-367); 8 CFR part 287; the Tariff Act of 1930, as amended; the Immigration and Nationality Act; and Executive Order (EO) 9397 (SSN), as amended by EO 13487.

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

The Border Patrol Enforcement Records (BPER) System of Records Notice[5] (SORN) provides coverage for subject, officer, and informant-related biographic and enforcement data contained in Workbench.

The TECS System of Records Notice[6] provides coverage for tracking individuals who have violated or are suspected of violating laws or regulations that are enforced by CBP.

The General Information Technology Access Account Records System (GITAARS) System of Records Notice[7] provides coverage for account information required for approved access to Workbench as well as the collection, review, and maintenance of any logs, audits, or other such security data (*e.g.*, the MSL) regarding the use of Workbench.

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

Workbench 2.0 is currently under its second Interim Authority to Operate (IATO), which expires in late April 2017. Workbench 1.0 was replaced by Workbench 2.0 when the latter became operational.

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

There is not currently a records retention schedule approved by the National Archives and

[5] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records, 81 FR 72601 (October 20, 2016).
[6] *See* DHS/CBP-011 TECS System of Records, 73 FR 77778 (December 19, 2008).
[7] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) System of Records, 77 FR 70792 (November 27, 2012).

Records Administration (NARA). CBP is in the process of drafting a records retention schedule for NARA review based on the retention requirements outlined in the BPER SORN and in Section 5.1 of this PIA.

### 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.

Workbench does not collect data directly from members of the public and therefore is not subject to the Paperwork Reduction Act. While the system contains information on informants and subjects of law enforcement in addition to emergency contact information provided by users and subscribers, these are executed as a part of the Workbench services and not designated collections of information from the public. The system typically collects member of public information provided by law enforcement officers and their informants for purposes of conducting searches and providing other support.

## Section 2.0 Characterization of the Information

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

Workbench collects, maintains, and disseminates information for different groups of individuals as outlined below.

**SES Members and Subscribers**

- First, middle, and last name;
- Last five digits of the SSN;
- Badge and credential number;
- CallsignID;
- Phone and fax numbers;
- Government email address;
- Emergency contact number[8] (member of the public);

[8] This is a voluntary data field in the Personnel Entry Data Sheets, but coverage for the collection of this information is covered by DHS/ALL-014 Personnel Emergency Contact Information System of Records, 81 FR 48832 (August 25, 2016).

- Duty station;
- Supervisor name; and
- Agency name.

**Informants (members of the public)**

- First and last name;
- Phone number; and
- Free form text field to include message to be relayed.

**Subjects (members of the public)**

- First, middle, and last name;
- Date of birth;
- Gender;
- Country of birth;
- SSN;
- Driver's license number;
- Alien Registration Number;
- Passport number;
- Email address;
- Home address;
- Business name; and
- Source system identifiers and tracking numbers.

**Vehicle, Vessel, and Aircraft Information**

- License plate information (number and state);
- Vehicle identification number (VIN);
- Vessel name;
- Vessel registration number;
- Boat hull number;

- U.S. Coast Guard (USCG) document number (provides evidence of nationality for international purposes, facilitates commerce between the states, and admits vessels to certain restricted trades, such as coastwise trade and fisheries);
- Aircraft tail number; and
- Aircraft registration year.

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

The sources of information collected and stored in Workbench are the subscribers and individual informants. Subscribers are typically field officers who request for SES staff to conduct searches on various criminal suspects or investigations. While the searches are conducted in systems outside of Workbench, the search criteria, and general search results are stored in Workbench. Any information provided by informants to assist with law enforcement operations and/or federal investigations (*e.g.*, terrorism, counterfeit products, narcotics smuggling) is also captured in the system.

## 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. Workbench does not directly use information from commercial sources or publicly available data. Workbench is used to document queries from subscribers and does not directly access commercial databases. Some of the databases searched by SES staff on behalf of subscribers may contain publicly available information on individual subjects.

## 2.4 Discuss how accuracy of the data is ensured.

While some information provided by subscribers and informants may be incomplete or incorrect, the input data can be corrected or modified by SES staff based on search results from the different systems outside of Workbench. Further, because Workbench is a tool for information sharing and not the repository for critical case or investigatory data, the information contained in it is not used for operational decision making; accordingly, the risk posed by inaccurate data in the system is minimal.

## 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk:** There is a risk that Workbench may be collecting more information than needed on members of the public.

**Mitigation:** This risk is partially mitigated. Workbench only collects and stores data provided by subscribers (law enforcement officers) and their respective informants. The information is captured in the appropriate fields in Workbench (*i.e.*, license plate information, date of birth, first name, last name) and only high-level activities performed with this information are captured in the system records. All searches are conducted external to Workbench and no specific search results are documented in the system. No information is solicited directly from the public, or recorded in other systems. The SES staff collects the least amount of information necessary to validate the information and relay it to the officer in the field. No information received by the SES is recorded outside of Workbench.

**Privacy Risk:** There is a risk that information in Workbench provided by subscribers used to conduct searches of source systems may be incomplete or inaccurate.

**Mitigation:** This risk cannot be fully mitigated. While the information maintained in Workbench may be incomplete or inaccurate, SES staff can confirm the data using results of searches in various other systems. In addition, if information is found to be incorrect after SES staff are able to validate it against other sources, SES staff contact the source agency responsible for the incorrect data to make them aware of the inaccuracy. SES staff also make the subscriber aware of the issue and annotate all actions taken in the MSL.

Further, because the information contained in Workbench is used for query purposes only and is not used operationally, the privacy risks posed by inaccurate inputs are reduced. There is a small risk that an inaccurate input (for example, the wrong middle initial) may lead subscribers and SES staff to identify the wrong individual. This risk is mitigated by the fact that SES staff and law enforcement partners are trained to take all necessary steps to positively identify the individual, and use additional data for corroboration when necessary. The information maintained by Workbench is not the sole means for which an enforcement or operational decision is made.

**Privacy Risk:** There is a risk that PII inadvertently entered in free form text fields in Workbench cannot be removed after log entries are saved to the MSL.

**Mitigation:** This risk is partially mitigated. SES staff complete the CBP Cyber Security Awareness and Rules of Behavior trainings. Both courses are designed to inform CBP employees of their responsibilities in protecting systems and data from threats. The courses also describe key provisions of the Privacy Act and provide guidelines for safeguarding and properly disclosing sensitive information.

In addition, if an SES member is found to have inadvertently included PII in free form text fields, he or she counseled by his or her supervisors and offered additional training as needed. If there is intentional inclusion of PII in these fields, the SES member is penalized in accordance with CBP Table of Offenses and Penalties, which can include termination of employment.

Finally, CBP Privacy will conduct a CBP Privacy Evaluation (CPE) within one year of publication of this PIA to verify that PII is not being stored in any free form fields. The results of the CPE will be shared with the DHS Privacy Office.

# Section 3.0 Uses of the Information

## 3.1 Describe how and why the project uses the information.

Officers of CBP, other DHS components, and external agencies subscribe to Workbench to address the fact that, when away from their desks, they need administrative support to obtain information on individuals suspected of criminal conduct. SES staff are available 24 hours a day, 7 days a week in order to adequately support the needs of these subscribers. Additionally, informants calling into the NLECC are looking for their law enforcement contacts (who may be away from their desks) can leave messages for them with SES staff containing information on subjects of investigation.

## 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. Workbench does not conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

No other DHS components or personnel have assigned roles and responsibilities within Workbench as this is a CBP system manned by NLECC staff.

The following DHS components have personnel who are subscribers to or clients of the NLECC and use Workbench services:

- U.S. Immigration and Customs Enforcement
  - Homeland Security Investigations
  - Enforcement and Removal
  - Office of Professional Responsibility
- Transportation Security Administration, Office of Investigations
- U.S. Coast Guard, Coast Guard Investigative Service

- U.S. Department of Homeland Security, Office of Inspector General

The agents of these DHS components complete the Personnel Entry Data Sheets for creation of their Workbench subscriber profiles. Once registered in the system, the subscribers are able to call in for information and other search queries upon successful authentication by SES staff. However, these agents do not have roles or responsibilities within the system and cannot access, view, or edit any data in the system.

### 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk:** There may be unauthorized uses of information outside of the authorized law enforcement-related queries.

**Mitigation:** This risk is partially mitigated because subscribers can only be helped by an SES member if they have existing user profile in the system, and are authenticated using valid credentials. SES staff are trained to only assist registered subscribers of Workbench. In terms of using information for unauthorized purposes, all activity by SES members is logged in the MSL, which contains fields to record information such as name of subscriber, name of SES member, time/date of occurrence, and info/narrative field to describe activity. SES members complete the log record for each transaction per their training. Any activity outside of these guidelines would be non-sanctioned.

## Section 4.0 Notice

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

The Workbench system deals with two categories of individuals: 1) the subjects of investigations, informants, individuals calling in tips, and private vessel owners; and 2) the SES staff and subscribers of the system. When Workbench subscribers call into SES staff with information for subject queries, they are providing data gleaned from second- and third-party sources. CBP obtains information from the subscriber, which may or may not have been collected directly from the subject, to conduct queries of other law enforcement systems. When individuals are questioned or arrested on charges, their information is recorded in various law enforcement systems. When informants, private vessel owners, and other individuals call in on the tip line, their information is recorded in Workbench. While all of these individuals are aware that their information is being collected, they will not have specific notice that their information may be housed in Workbench. Accordingly, CBP is providing notice through this PIA.

CBP provides notice to SES staff and subscribers for creation of their user profiles in Workbench. A Privacy Act Statement at the top of the Personnel Entry Data Sheets explains purpose of information. This text is as follows: "This data sheet is required by the Operations Branch for the entry of personnel into the User Authentication System. The User Authentication System is the primary tool used by the Sector Enforcement Specialist to identify an authorized subscriber of operational services. Validation of a subscriber is required in order to provide law enforcement queries."

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

The subscribers or field officers calling into the NLECC are actively working cases and pursuing suspects, which is why they may need assistance with gathering additional information while in the field. They will not receive the assistance unless they are listed as authorized users in the Workbench system. These subscribers are not required to register in Workbench unless they plan to call the NLECC for law enforcement purposes. If they choose to opt-out of providing information, they need alternative means of obtaining information when away from their desks as they are not able to be validated via the Workbench system.

Information received from an informant or any other private citizen is provided to the NLECC voluntarily. They are generally calling the NLECC to connect with an agent or officer with whom they are working or to report suspicious activity. If these individuals want to opt-out of providing their information, they can choose to have the agent or officer call them so they can relay information directly to them; report the suspicious activity to another agency; or decline to report.

In addition, there is no notice to a subject at the time of collection that his or her information may be stored in Workbench in association with a law enforcement query; however, this PIA provides notice of this collection.

## 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** There is privacy risk to notice in that members of the public are not aware that their information may be retained as part of a Workbench query record, and that there have been no opportunities for the individuals in question to opt-out or decline participation in the collection.

**Mitigation:** This risk is partially mitigated. Workbench processes do not require collection of data directly from members of the public; any processes to opt-out or decline providing personal information would be completed at the source of collection. In many of these instances (such as cases in which CBP has a record of inspection on an individual that led to an enforcement action), the individual would have been provided notice through direct participation in the event. There is

no notice to the individual at the time of collection that their information may be stored in Workbench in association with a law enforcement query; however, this PIA provides notice of this collection.

## Section 5.0 Data Retention by the project

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

CBP is in the process of drafting a records retention schedule for the information maintained in Workbench, consistent with the BPER SORN. CBP is currently retaining information indefinitely until the formal records retention schedule is completed, but anticipates retaining user account management records for ten (10) years following an individual's separation of employment from federal service; audit files (including user activity logs) for fifteen (15) years; and backup files for up to one (1) month.

### 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** Workbench may be storing information beyond appropriate retention timeframes.

**Mitigation:** The free form text fields in Workbench are not used to store detailed search result information (based on training provided to SES staff, including safeguarding PII). They should be used to summarize any action an SES member took that cannot be derived from the action codes he or she used. For instance, SES staff can state all checks in databases were negative, or they coordinated an event with an officer, or they updated a subscriber's contact information. That said, CBP is working on records disposition schedules, so relevant information stored in the system will subsequently need to comply with these requirements.

## Section 6.0 Information Sharing

### 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Appendix B contains a list of non-DHS federal agencies with agents who are subscribers of the NLECC and use Workbench services as part of their normal agency operations. For the non-DHS law enforcement agencies that request radio, email, and telephonic support for field agents, CBP completes MOUs prior to including their personnel in the Workbench system. As with DHS components, the agents of these offices/agencies also complete the Personnel Entry Data Sheets in order to have their user profiles created in Workbench.

The NLECC provides law enforcement information from national systems (like NCIC and Nlets) to all registered Workbench users. For any other system, such as TECS, the subscriber has to already be an active (registered) user of the system (*e.g.*, TECS) in order for the NLECC to provide information that is only available in that system.

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

The NLECC only shares information with non-DHS federal agencies that enter into MOUs with CBP. Users are not registered until a signed MOU and current Interagency Agreement is signed. Agency personnel are registered users of Workbench and use NLECC services when they are in the field and require information on subjects of an investigation. Two purposes of the BPER SORN are to: a) record the detection, location, encounter, identification, apprehension, and/or detention of individuals who commit violations of U.S. laws enforced by DHS between the points of entry; and b) support the identification and arrest of individuals who commit violations of federal criminal laws enforced by DHS.

NLECC may share information with Workbench subscribers pursuant to routine uses in the BPER SORN,[9] including:

> H. To appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, when DHS/CBP believes the information would assist in the enforcement of applicable civil or criminal laws; and
> M. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate in the proper performance of the official duties of the officer making the disclosure.

Additionally, all activity by the SES staff on behalf of their law enforcement subscribers is logged in the MSL as it could be needed for OPR/IA or OIG audits. The NLECC is mandated to produce activity-related information upon request by these departments.

## 6.3 Does the project place limitations on re-dissemination?

Information sharing is based on the results obtained from the various law enforcement queries requested by NLECC subscribers. Additionally, information may be requested for audits or investigations conducted by agency OPR/IA or OIG departments and also by other federal agencies needing to reconcile their office personnel records.

[9] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records, 81 FR 72601 (October 20, 2016).

Neither the MOUs with non-DHS agencies nor any standard operating procedure of the NLECC currently place any restrictions on re-dissemination of information obtained through the NLECC queries. The registered subscribers receiving information are restricted on unauthorized sharing of this data via the Third Agency Rule, which states that information accessed cannot be disclosed by the accessing agency without approval from the agency that owns the data being accessed. When sending any border crossing information to non-DHS subscribers via email, SES staff annotate the following statement:

> *This information is being provided only for the purpose stated in your request, it should not be employed for any other use that is not consistent with said request, in addition this information must not be further disseminated to a third party without the express written consent of the United States Customs and Border Protection. However, the released information may be presented in any court proceedings related to the matter for which the information was sought.*
>
> *By accepting this information, you agree that in the event of any unauthorized release of the information, outside of presenting this information in court, your agency will intercede on CBP's behalf to assume full responsibility for any and all expenses, costs, or liabilities arising from such disclosure.*

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

The Workbench MSL provides the means to record all transactions performed at the NLECC in a database. Each entry in the MSL is essentially documentation of information sharing with registered users of the system. The MSL serves in lieu of DHS-191, Release of Information Subject to the Privacy Act, given the log entries document the release of information to other agencies. Any requests from field offices for a printed or hard copy of an MSL or individual entry must be approved for release by the NLECC's management prior to transmission.

## 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There could be unrestricted or unauthorized information sharing by SES staff and subscribers.

**Mitigation:** This risk is partially mitigated. MSL log extracts are provided to agency OPR/IA and OIG departments with prior authorization from the NLECC to execute these requests. Any Workbench subscribers and others with ad-hoc needs for this information have to submit requests to NLECC management for authorization.

SES staff only share information with registered Workbench subscribers. SES staff can check the subscribers' "Office" tab permissions to see what information is allowed for the office

in question. That is, when each agency's personnel are setup in Workbench, they are provided levels of permission related to the type of information that can be provided to them by SES staff. The MSL standard operating procedure governs the printed and verbal release of these MSL extracts.

Information sharing is governed by the Third Party Rule, which means that information accessed cannot be disclosed by the accessing agency without approval from the agency that owns the data being accessed. SES staff annotate the below statement when emailing border crossing information to non-DHS subscribers.

> *This information is being provided only for the purpose stated in your request, it should not be employed for any other use that is not consistent with said request, in addition this information must not be further disseminated to a third party without the express written consent of the United States Customs and Border Protection. However, the released information may be presented in any court proceedings related to the matter for which the information was sought.*
>
> *By accepting this information, you agree that in the event of any unauthorized release of the information, outside of presenting this information in court, your agency will intercede on CBP's behalf to assume full responsibility for any and all expenses, costs, or liabilities arising from such disclosure.*

In addition, CBP Privacy will work with NLECC to update all currently signed MOUs to include pertinent language regarding re-dissemination of DHS data. The updated language will be used in all future NLECC MOUs.

# Section 7.0 Redress

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

Any individual, regardless of citizenship or immigration status may seek notification of or access to any CBP record contained in Workbench through the procedures provided by the Freedom of Information Act (FOIA) and the access provisions of the Privacy Act of 1974, 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 this system of records 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.[10] 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,[11] 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 them;
- Identify which component(s) of the Department they believe may have the information about them;
- 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 procedures outlined in Section 7.1 can be used to access individual information in the system. However, since Workbench is generally not the source of the information, the individuals would need to go to the source systems to update or modify their information. A list of source systems for Workbench can be found in Appendix A of this PIA. Ultimately, Workbench is only a repository of actions performed by the SES. Any erroneous information provided by law enforcement officers (LEO) or the public will be rectified by the LEOs when reviewing search results provided to them or performing inspections (*i.e.*, private vessel/small boat entries, vehicles). Any modifications to individual information will be captured in the relevant investigative, case management, or source systems such as TECS and not in Workbench. While the SES attempts to validate information provided to them, the responsibility lies specifically with the LEOs to verify and revise in the appropriate systems of record.

[10] 6 CFR part 5.
[11] 28 U.S.C. § 1746.

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

As mentioned in Section 7.2, the source systems would have procedures available to the public as to how they can update their information in a particular system.

### 7.4 Privacy Impact Analysis: Related to Redress

**Privacy Risk:** Individuals may be unaware of inaccurate information about themselves in Workbench, and therefore be unable to remedy the inaccuracies.

**Mitigation:** Information on individuals is only collected and stored in Workbench as reported by NLECC subscribers looking for additional information on their subjects. The searches for information on these individuals are executed in law enforcement databases external to Workbench. While inaccuracies in Workbench may be rectified by these search results, individuals will need to follow specific procedures outlined by these source systems to rectify any errors and other issues regarding their respective information.

## Section 8.0 Auditing and Accountability

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

All actions taken by SES members are documented in the MSL for auditing and accountability purposes. This is to ensure that if there are questions as to why a certain query was made, SES staff can provide documentation that it was at the request of a law enforcement officer in the performance of his or her duties, or that additional queries were made on his or her behalf for officer safety reasons. First line supervisors review the MSL daily to ensure quality control. If administrative errors are identified, the SES member is counseled, provided refresher training if needed, and the log supplemented with the correct data. If it is discovered the SES member made the query for anything other than an official purpose, the SES member will be penalized in accordance with CBP Table of Offenses and Penalties, which can include termination of employment. Some system owners, for example the Federal Bureau of Investigation (FBI), which owns NCIC records, conduct routine audits to ensure compliance with their respective system policies. Agency OPR/IA or the OIG may request MSL extracts when they are investigating officers/agents to ensure they are running queries in the performance of their duties and have a "need to know." The NLECC is notified if violations are identified.

CBP Privacy will conduct a CPE within one year of publication of this PIA to verify that the NLECC is adhering to the privacy protections outlined in this PIA. The results of the CPE

will be shared with the DHS Privacy Office.

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

All SES are required to take annual privacy and security awareness training to maintain system access. In addition, there is a master training syllabus for SES staff. The training typically takes between four to eight months to complete depending on the previous background of the specialists being trained. This syllabus is in addition to state and other law enforcement system specific training that is required.

### 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 Communications Center of Operations for the NLECC determines the roles and responsibilities of users of Workbench. The MOUs and other agreements in place with non-DHS agencies dictate the personnel requiring the services of the NLECC. SES staff, field officers, and administrators have specific roles and permissions in Workbench.

### 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 only shares information with non-DHS agencies that have MOUs with the NLECC. Per CBP policy, domestic MOUs must be finalized in conjunction with the CBP Office of Privacy and Diversity as the lead. There is no access to Workbench by external agencies without MOUs in place.

Additionally, all agencies create user profiles for their respective officers in the system via the Personnel Entry Data Sheets, so these officers can request and receive information from SES staff.

## Responsible Officials

Dalia Putnam
Chief, Communications Center of Operations
National Law Enforcement Communications Center (NLECC)
Enterprise Networks and Technology Support Directorate
U.S. Customs and Border Protection

Debra L. Danisek
CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection

## Approval Signature

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

_____

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

# Appendix A

DHS Systems:

- CBP TECS;[12]
- CBP Analytical Framework for Intelligence (AFI);[13]
- CBP Automated Targeting System (ATS) Passenger (ATS-P) and Land (ATSP-L);[14]
- ICE Enforce Alien Removal Module (EARM);[15]
- ICE Student Exchange and Visitor Information System (SEVIS);[16]
- USCIS Central Index System (CIS);[17] and
- USCIS Computer Linked Application Information Management (CLAIMS).[18]

Other Systems:

- National Crime Information Center (NCIC) is an FBI owned system that assists law enforcement in apprehending fugitives, locating missing persons, recovering stolen property, and identifying terrorists. Additional information on NCIC is available at https://www.fbi.gov/services/cjis/ncic.
- National Law Enforcement Telecommunications System (Nlets) is a non-profit organization owned by the states that allows state and federal law enforcement agencies, as well as select international agencies, to securely share law enforcement, criminal justice, and public safety related information. Additional information on Nlets is available at http://www.nlets.org/.
- National Insurance Crime Bureau (NICB) is a non-profit organization that partners with insurance companies and law enforcement to facilitate the detection, identification, and prosecution of insurance criminals. Additional information on NICB is available at www.nicb.org.

[12] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[13] *See* DHS/CBP-017 Analytical Framework for Intelligence System, 77 FR 13813 (June 7, 2012).
[14] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[15] *See* DHS/ICE/PIA-015(b) Enforcement Integrated Database (EID) ENFORCE Alien Removal Module (EARM 3.0) (May 20, 2011), *available at* https://www.dhs.gov/privacy.
[16] *See* DHS/ICE 001 Student and Exchange Visitor Information System, 75 FR 412 (January 5, 2010).
[17] *See* DHS/USCIS/PIA-009 Central Index System (CIS) (June 22, 2007), *available at* https://www.dhs.gov/privacy.
[18] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems (March 25, 2016), *available at* https://www.dhs.gov/privacy.

- Department of State Consular Consolidated Database (CCD).[19]
- LexisNexis (ACCURINT) provides legal, government, and business information compiled from a variety of sources. Additional information on LexisNexis is available at https://www.lexisnexis.com.

State Systems:

- Florida Crime Information Center ((FCIC)/E-Agent) provides access to certain records from Florida law enforcement agencies made public. Additional information on FCIC is available at http://www.fdle.state.fl.us/cms/Home.aspx.
- Florida Driver and Vehicle Information Database (DAVID) provides immediate access to Florida driver license and motor vehicle information. Additional information on DAVID is available at http://www.flhsmv.gov/courts/david/.
- Pennsylvania Criminal Justice Network (PA CJNET) provides public access to various aspects of court information, including appellate courts, common pleas courts, and magisterial district court docket sheets; common pleas courts and magisterial district court calendars; and PA ePay. In addition to the public information available on this site, specialized eServices are available to users with a secure login. These include secure docket sheets for the three levels of court; secure court calendars for common pleas courts and magisterial district courts; statewide warrants; and attorney registration. Additional information on PA CJNET is available at https://ujsportal.pacourts.us/.
- Texas Law Enforcement Telecommunications System (TLETS) provides intrastate interconnectivity for Texas criminal justice agencies to a variety of local, state, and federal data base systems. Additional information on TLETS is available at http://www.dps.texas.gov/director_staff/information_management/tlets.htm.

[19] *See* Privacy Impact Assessment: Consular Consolidated Database (July 17, 2015), *available at* https://www.state.gov/documents/organization/242316.pdf.

# Appendix B

- Environmental Protection Agency;
    - Office of Inspector General; and
    - Criminal Investigative Division.
- Export-Import Bank of United States - Office of Inspector General;
- Federal Deposit Insurance Corporation - Office of Inspector General;
- Federal Housing Finance Agency - Office of Inspector General;
- Federal Reserve Board - Office of Inspector General;
- National Aeronautics and Space Administration - Office of Inspector General;
- National Oceanic and Atmospheric Administration - National Marine Fisheries Service, Office for Law Enforcement;
- National Science Foundation - Office of Investigation;
- Office of Personnel Management - Office of Inspector General;
- Peace Corps - Office of Inspector General;
- Railroad Retirement Board - Office of Inspector General;
- Social Security Administration - Office of Inspector General;
- U.S. Department of Agriculture - Office of Inspector General;
- U.S. Department of Commerce - Office of Export Enforcement ;
- U.S. Department of Defense - Defense Criminal Investigative Service;
- U.S. Department of Education - Office of Inspector General;
- U.S. Department of Energy - Office of Inspector General;
- U.S. Department of Health and Human Services;
- Office of Inspector General;
- Food and Drug Administration - Office of Inspector General;
- U.S. Department of Labor;
- Office Labor Racketeering & Fraud Investigations - Office of Inspector General;
- Office of Inspector General (OSEC) (a.k.a. Division of Protective Services);

- U.S. Department of State - Office of Inspector General;
- U.S. Department of Transportation;
- National Highway Traffic Safety Administration;
- Office of Inspector General;
- U.S. Department of Treasury;
- Office of Inspector General;
- Treasury Inspector General for Tax Administration;
- Internal Revenue Service - Criminal Investigative Division; and
- U. S. Department of Veteran's Administration - Office of Inspector General.