Privacy Impact Assessment
for the

Border Patrol Enforcement Tracking System (BPETS/BPETS2)

DHS/CBP/PIA-046

August 28, 2017

Contact Point
Antonio J. Trindade
U.S. Border Patrol
Strategic Planning and Analysis Directorate
U.S. Customs and Border Protection
(202) 344-1446

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

Abstract

The Border Patrol Enforcement Tracking System (BPETS) is a Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) U.S. Border Patrol (USBP) web-based application that allows USBP to analyze incident data and manage the deployment of personnel and resources. BPETS is a legacy system, once maintained by the Department of Justice (DOJ) Immigration and Naturalization Service (INS), and is now maintained by CBP. The BPETS2 system is an enhancement to the legacy BPETS system, which adds advanced technologies and improved system integration. Currently, BPETS and BPETS2 operate in conjunction with one another, but the BPETS2 system will eventually replace the legacy BPETS system. CBP is conducting this Privacy Impact Assessment (PIA) because BPETS and BPETS2 both collect, maintain, and disseminate personally identifiable information (PII).

Overview

The priority mission of U.S. Customs and Border Protection (CBP) is to prevent terrorists and their weapons, including weapons of mass destruction, from entering the United States at or between ports of entry. The U.S. Border Patrol (USBP) is responsible for interdicting persons attempting to illegally enter or exit the United States between ports of entry and for deterring and preventing the illegal entry of terrorists, terrorist weapons, and contraband between ports of entry. Together with other law enforcement agencies, USBP helps maintain border security and facilitate the flow of legal immigration and goods while preventing the illegal trafficking of people and contraband. USBP is specifically responsible for patrolling nearly 6,000 miles of Mexican and Canadian international land borders located between the ports of entry, and over 2,000 miles of coastal waters surrounding the Florida peninsula and the island of Puerto Rico. Agents work around the clock on assignments, in all types of terrain and weather conditions, and in many isolated communities throughout the United States.

To allocate personnel and resources across a vast operation, USBP uses BPETS/BPETS2, a web-based system containing multiple modules each with specific user roles, to track the deployment of USBP personnel and operational assets to analyze enforcement incident data (such as apprehensions and seizures); to manage and deploy assets; to create and approve operational orders; and to generate reports and statistics to ensure that USBP is efficiently deploying resources to meet enforcement needs along the U.S. borders. Access to BPETS/BPETS2 data and the functions that users can perform are limited by the roles assigned to the individual user. Users are assigned specific roles in each module. These roles control whether a user can view, edit, or create data in that module. In addition, USBP personnel use BPETS/BPETS2 to maintain their time and attendance, create leave requests, and manage other general schedule requests.

BPETS/BPETS2 is used by both supervisors and non-supervisors of USBP, including

contractors assigned to support USBP. Through BPETS/BPETS2, employees are able to search for contact information of other USBP personnel, and employees conversely have some ability to limit who can search for their information.[1] Supervisors use BPETS/BPETS2 to view and update their assigned staff information, create and maintain work schedules for the pay period, view and approve their assigned employees' timesheets, run staffing and scheduling reports, and perform system administrative tasks (such as setting up profile defaults). With the release of BPETS2, when a user updates his or her staff profile, containing address and phone numbers, the information is synchronized with WebTELE, CBP's web-based telephone directory.[2]

Most of the personally identifiable information (PII) within BPETS/BPETS2 is manually entered by users, (*e.g.*, USBP personnel information, deployment schedules, and statistical information related to incident reports). BPETS/BPETS2 also contains aggregated statistical data (calculated numbers, not transactional records) from database snapshots of CBP data in the U.S. Immigration and Customs Enforcement (ICE) Enforcement Integrated Database (EID)[3] for incident and enforcement trends and reporting.

Currently, the Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW)[4] pulls BPETS information regarding scheduling of manpower within specific locations as entered in the G-259 and G-481 Scheduling modules. The data is used for replicating the reports within BPETS, specifically related to the total number of personnel deployed within zones. Many of the legacy reporting functions within BPETS have now transferred to the Border Patrol Enterprise Reporting Tool (BPERT) reporting dashboard within EMIS-EDW.

BPETS Functions

BPETS consists of the following modules:

- **Staffing Module** contains USBP employee information that forms the basis of employee profiles for staffing and timesheet purposes.
- **G-259 and G-481 Scheduling Modules**[5] allows supervisors to schedule staffing/manpower on a bi-weekly (G-259) and daily (G-481) basis. Supervisors assign days off, activities, vehicles, and work locations. Additional functions exist for setting up

[1] Agents cannot prevent supervisors from searching for their contact information, but can withhold this information from other agents.
[2] WebTele receives a one-way push of information from BPETS/BPETS2. For more information about WebTELE, please *see* DHS/CBP/PIA-043 CBPnet, *available at* www.dhs.gov/privacy.
[3] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at* www.dhs.gov/privacy.
[4] *See* DHS/CBP/PIA-034 Enterprise Management Information System - Enterprise Data Warehouse (EMIS-EDW), *available at* www.dhs.gov/privacy.
[5] Supports the requirements to maintain biweekly (G-259) and daily (G-481) schedules. A batch process is used to initialize the G-259 that is maintained with staff work status by pay period. The finalized G-259 is used to initialize the G-481 that is maintained daily. Finally, actual time worked and leave time taken are entered into the Timesheet module.

the duty location schedules, such as creating assignments, creating a workgroup hierarchy, and grouping staff members onto schedules.

- **Timesheet Module** allows the user to add information related to his or her time and attendance record (*e.g.*, scheduled and taken leave). The module provides the user with a print-out that contains his or her schedule (as scheduled by a supervisor) and the non-scheduled items that the user entered.
- **Vehicle Tracking Module** captures information on USBP vehicles at the specific duty locations. These vehicles are entered into the system at the duty locations, and are available to be assigned to agents within the Scheduling modules. There is no location tracking or monitoring of vehicles. The Vehicle Tracking module tracks which vehicle is assigned to each agent.
- **Checkpoint Module** captures information on USBP checkpoints. The checkpoint profile includes specifics about the checkpoint, such as the number of lanes, number of cells, and the location, as well as the type of facility (fixed or tactical). Enforcement incident data is not captured in the Checkpoint module.
- **Detail Management Module** was consolidated under the G-259 and G-481 Scheduling modules within BPETS2. The module provides a means to transfer staff to a different duty location on a temporary basis. In addition, the module contains reports on the total number of temporary duty assignments. The module was created to allow staff (employees and contractors) to appear on the bi-weekly schedule and the daily schedule. Additionally, this allows employees' (not contractors) supervisors/timekeepers to view their timesheets.
- **Operations Orders Module** tracks past and ongoing operations that occur within a sector. The Operations Order module contains information on the mission, purpose, and cost associated with the operation. Operations Orders do not contain PII; rather they contain text fields that describe the Situation, Mission, Execution, Administration, and Command/Control elements of the operation.
- **Border Safety Initiative Tracking System (BSITS) Module** tracks the number of deaths encountered by, and rescues made by, USBP while on patrol.[6] The module tracks the disposition of the individual, and type and location of the event.
- **GPRA Module**[7] is a reporting module which enables USBP to automatically generate

[6] This module does not include use of force incidents, but rather includes information about individuals that are rescued or already deceased when encountered by USBP.

[7] On January 4, 2011, the GPRA Modernization Act of 2010 (GPRAMA) became law. The acronym "GPRA" in the act's short title refers to the Government Performance and Results Act of 1993 (GPRA 1993), a law that GPRAMA substantially modified. When GPRA 1993 was enacted, it was regarded as a watershed for the federal government. For the first time, Congress established statutory requirements for most agencies to set goals, measure performance, and submit related plans and reports to Congress for its potential use.

mandatory standardized reports. This module enables USBP to generate reports by zone activity, narcotics seizures, personnel assigned to zone, technology (permanent and fixed) deployed by zone, vehicles assigned to personnel and deployed by zone, and summary statistical reports on enforcement activities within a specific area or operation (AOR). Statistics include: the number of narcotics seizures, personnel, technology, and vehicles assigned to an AOR.

- **Intelligence Reports Module** (summary reporting function only; this module does not contain PII) contains various reports, such as the Apprehension,[8] National Guard,[9] and Canine Assists[10] reports. Intelligence reports are broken down by various attributes. Some reports contain a daily snapshot of enforcement activities, such as the number of apprehensions and total amount of narcotic seizures. Other reports compare the number of apprehensions that were made within a specific location with total resources and manpower deployed nearby. This functionality is slowly being transferred to the BPERT reporting dashboard within the EMIS-EDW.
- **Security Module** is a system administration environment used to provision access for a user to specific modules and to roles within those modules. Roles vary by module, but typically they include self-service employee, supervisor, or administrative roles for managing time, attendance, and scheduling. Operational modules have role-based access by station, sector, and headquarters, as well as administrative roles.

BPETS2

On March 11, 2012, BPETS2 was released. BPETS2 was developed and is maintained by the Border Enforcement and Management Systems Division (BEMSD). BPETS2 is comprised of the Staffing, Scheduling, Timesheet, and Vehicle Tracking modules. Legacy data in these BPETS modules was converted to BPETS2. The BSITS, Operations Order, and Checkpoint modules, as well as several reports, are currently maintained in legacy BPETS. The functionality in these modules is slowly being transitioned off of the legacy BPETS application to BPETS2.

[8] Apprehension reports contain aggregate statistics only. No PII is included in this report or any report generated by the Intelligence Reports module.
[9] The National Guard reports include the total number of National Guard deployments to the border. These reports are no longer used, but are available for historic uses and trend reporting. No PII is included in these reports.
[10] The Canine Assist report shows activity by a specific canine. These reports are still active but do not contain information about Canine handlers.

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 data that is stored in BPETS/BPETS2 (including operational, resource, and scheduling information) in furtherance of CBP's border security responsibilities. See, *e.g.*, 6 U.S.C. § 211; 8 U.S.C. § 1103(a)(5); 8 U.S.C. § 1357. Additional data collection, such as budgeting and resource allocation, serves to meet the mission accountability requirements imposed through the Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62.

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

BPETS/BPETS2 maintains employee personnel and medical records, employee time and attendance records, enforcement and incident records, and limited emergency contact information for USBP employees. USBP employee and medical records are covered by OPM/GOVT-1 General Personnel Records[11] and OPM/GOVT-10 Employee Medical File System Records,[12] respectively. Time and attendance records are covered by DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records.[13] Enforcement and incident records are covered by DHS/CBP-023 Border Patrol Enforcement Records (BPER).[14] Emergency contact information is covered under DHS/ALL-014 Personnel Emergency Contact Information System of Records.[15]

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

Yes. BPETS/BPETS2 has undergone the Security Authorization process in accordance with DHS and CBP policy, which complies with federal statutes, policies, and guidelines. BPETS/BPETS2 is part of the Enforcement Support Systems security authorization boundary and will receive a renewed Authority to Operate upon completion of this PIA.

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

Yes. BPETS/BPETS2 maintains several different types of records with different retention periods. See Section 5.0 of this PIA for a detailed description per module.

---

[11] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[12] OPM/GOVT-10 Employee Medical File System Records, 75 FR 35099 (June 21, 2010).
[13] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records, 80 FR 58283 (September 28, 2015).
[14] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).
[15] DHS/ALL-014 Personnel Emergency Contact Information System of Records, 81 FR 48832 (August 25, 2016).

In accordance with NARA General Records Schedule 2.4, Item 30, USBP time and attendance records are destroyed after a Government Accountability Office audit or when three (3) years old; whichever is sooner. These records include the data extract received bi-weekly from the U.S. Department of Agriculture (USDA) National Finance Center (NFC), known as the USDA Bi-Weekly Examination Analysis and Reporting System (BEAR) feed. In accordance with NARA General Records Schedule 2.4, Item 40, individual employee payroll records are destroyed when fifty-six (56) years old.

For enforcement records, CBP is in the process of drafting a proposed record retention schedule for the information maintained under the BPER SORN. CBP anticipates retaining records of arrests, detentions, and removals for seventy-five (75) years. Investigative information that does not result in an individual's arrest, detention, or removal, is stored for twenty (20) years after the investigation is closed, consistent with the NARA Job No. N1-563-08-04-02.

For user account management records, CBP will store records for ten (10) years following an individual's separation of employment from federal service; statistical records for ten (10) years; audit files for fifteen (15) years; and backup files for up to one (1) month. Records replicated on other DHS or CBP unclassified and classified systems and networks will follow the same retention schedule.

Emergency contact records relating to current and former DHS employees, and individuals designated as emergency points of contact, will be destroyed when superseded or obsolete, or upon separation or transfer of employee, in accordance with NARA General Records Schedule 5.3, Item 20.

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.

All information maintained in BPETS/BPETS2 is either a) collected directly from employees, or b) collected as part of a law enforcement action, and therefore the PRA is not applicable.

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.

Within the Staffing module, the following PII related to USBP employees is collected and stored in BPETS or BPETS2. These categories, and the specific data collected in each category, are listed in the following sections.

General employment information:

- First name, last name, middle initial (and nickname, if applicable);
- Hash ID;[16]
- Job title;
- Sector and station;
- Date of birth (DOB);
- Gender;
- Enter on Duty (EOD) date and service computation date;
- Border Patrol and station EOD dates;
- Academy class;
- Job classification;
- Pay information (GS-scale grade, step, quality step increases, and relevant dates);
- Driver's license state, number, and expiration date;
- Home and mailing addresses (street address, city, state, ZIP code);
- Phone numbers (home phone, mobile phone, unlisted, and pager);
- Email address;
- Emergency contact information (name, relationship, phone numbers, and address);
- Emergency Patrol Agent contact information (name, phone number);

[16] The Hash ID is a unique identifier assigned to CBP employees, derived from the individuals Social Security numbers.

- Work information (address; phone numbers; supervisor; assigned canine);
- Medical information (including doctor name and phone number, medical alerts, health plan name and code, blood type); and
- Special skills.[17]

In addition to BPETS2 data, legacy BPETS also collects and stores a limited amount of data related to subjects of border incidents. This information is captured only in the BSITS module and is not used in any other module. Eventually the BSITS module data elements will be captured in the Tracking, Sign-cutting, and Modeling module within E3[18] and the existing data in the BSITS module will be maintained in legacy BPETS for historical purposes only. PII captured in legacy BPETS related to incident subjects includes:

- Full name (first, middle, last) of the individual encountered during the border safety event);
- DOB;
- Nationality;
- Gender;
- Citizenship status; and
- For some individuals (specifically, non-U.S. citizens subject to an immigration enforcement action), there is a link to the subject of an E3[19] event (EID database):[20]
  - Event number; and
  - FIN (Fingerprint Identification Number).

[17] Special skills may include: All Terrain Vehicles; Bike Patrol; Border Patrol Search Trauma and Rescue; Border Patrol Tactical Unit; Border Patrol Explorers; Horse Patrol; Canine Handler; Recruitment; Scope Skills; Union Steward; Boat Handler; Boat Instructor; BPETS; Bus Driver's License; CBP Automated Travel System; Chaplain; Critical Incident Investigation Team; Class B Driver's License; Commercial Driver's License; Confined Spaces; Customs Overtime Scheduling System; Collapsible Steel Baton/Oleoresin Capsicum Spray Instructor; Designated Marksman; Driving Instructor; E3; Emergency Medical Training; Enforce; Firearms Instructor; FITS; FN303 (less lethal device); Hazardous Materials Training; Honor Guard; Intel; Languages; Law Instructor; Light Unit Maintenance Officers; Mobile Response Team; Mobile Surveillance System Instructor; MSS Operator; Operational Requirements Based Budgeting Program; Peer Support; Pepper-ball Launching System; PT Instructor; Pursuit Interdiction Technique; Radiation Isotope Identification Device; RECON; Sensor Installation/Maintenance; Sign Cutting; Significant Incident Report; Snow; Snowmobile; Spanish Instructor; Special Response Team; TECS-TPX (system); TELE/WebTELE (system); Vehicle Maintenance Officer; Welding; Z Backscatter Van).
[18] *See* DHS/CBP/PIA-012(a) CBP Portal (e3) to EID/IDENT and subsequent update, a*vailable at* www.dhs.gov/privacy.
[19] *Id.*
[20] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at* www.dhs.gov/privacy.

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

BPETS/BPETS2 data is either provided directly by the employee (*e.g.*, Staffing and Timesheet modules) or relates to enforcement information obtained from encounters with the public (*e.g.*, BSITS module). BPETS/BPETS2 does not capture employee information from any specific form; however, individual duty locations may capture employee related information via an employee locator sheet, email, or verbal report. Other modules are regularly updated directly by the employee (*e.g.*, Timesheet module). The enforcement information is primarily captured within E3 on forms I-213 and I-44, which are used to report and process removable alien apprehensions and seizures. Information entered in the BSITS module is often captured via a tracking sheet specific to the individual duty location. Employee or resource information includes employee personnel information, technology or equipment details, and assignment scheduling data. Enforcement related information includes significant apprehension information, seizure information, and daily aggregations of the totals of this data.

BPETS/BPETS2 uses a combination of manually entered data and data imported from other CBP or DHS systems, such as ICE EID.[21] Data is imported whenever possible in order to minimize processing time, eliminate duplicate data collections, and minimize errors in manual data entry. This information is used for summary reports which compare the total apprehensions within an area to the number of personnel assigned to that location. Additionally, the EID data is used, in some cases, for linking BSITS (deaths and rescues) subjects to an enforcement event.

Typically, an employee's initial record is created by a user with administrative rights to the Staffing module. Once the record is created and PII entered, the employee can update/maintain his or her own PII. Employee information is separated into work and personal information. Work information includes work phone number and address information such as duty location. Employee work information is always visible to all BPETS users. Personal information, such as home address and home phone number are marked private and hidden by default. Supervisors can view personal information, but only that of their subordinates. Employees may choose to make their personal information available to others. When un-restricted, the personal information such as home address and home phone number are viewable to all other BPETS users, regardless of role. Data entered manually includes personnel information, deployment schedules, and some statistics related to incidents. Data pulled from other systems is used in the reporting functions of BPETS/BPETS2. This data includes statistical data from EID (number and type of cases resulting from USBP enforcement encounters).

[21] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at* www.dhs.gov/privacy, and DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016).

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

BPETS/BPETS2 does not use commercial or publicly available information.

2.4 Discuss how accuracy of the data is ensured.

Accuracy of the information available through BPETS/BPETS2 and entered by USBP personnel is ensured by training provided to USBP agents and other system support personnel, including supervisors, with respect to access and use of the system. Accuracy of the information obtained from other systems relies upon the integrity of those systems. USBP agents and support personnel who access information through BPETS/BPETS2 receive training in the use of the system as part of their basic training and periodic refresher training.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that BPETS may contain inaccurate information based on manual data entry.

Mitigation: BPETS/BPETS2 has controls built into the system to ensure data accuracy. Some examples of these controls include required fields to ensure completeness of records and format controls. Required fields include identifying information, such as first and last name and work address. Some fields require the data to be provided in an appropriate format to reduce errors, including date fields, time fields, and employee look-up fields. PII such as employment type, supervisor, EOD dates, service computation date, job class, title, and grade/step is populated by users with the role of Personnel.[22] This information is only viewable to the employee as well as users with the role of Supervisor[23] (for that employee) or Personnel. In addition to these system controls, access to each module of BPETS/BPETS2 is limited to personnel that are properly trained in the specific rules related to each module.

Additionally, USBP maintains a unit within the Headquarters Office that is specifically tasked with monitoring and ensuring data integrity in the BPETS/BPETS2 system. This unit conducts periodic reviews of BPETS/BPETS2 data.

[22] Personnel role is granted to administrative personnel and enables the administrator to change HR-related information such as EOD, job-classification, pay, etc.
[23] Supervisor role is granted to supervisors only and enables the supervisor to set/change work schedules, assignments, etc.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The information captured in the Staffing module is maintained primarily for the use of scheduling. However, the Staffing module is the backbone for the BPETS/BPETS2 applications, and information about USBP employees contained in the Staffing module is used throughout other modules. Reports within the Staffing module are also used as a tool for identifying and notifying employees in emergency situations. Information in the Staffing module is also used to identify the user who is making updates to, and who is authorized to approve, an operation within the Operations Order module.

The information captured in the BSITS module pertaining to subjects encountered during a safety event (death or rescue) is used primarily for statistical and reporting purposes by USBP. The PII collected and included for statistical and reporting purposes is typically originally collected as part of an E3 event and is used for identification of the subject and to aid in determining the final disposition of the event, such as cause of death as determined by a medical examiner, or providing information specific to USBP's response to the event. The subject information is also used to link the Border Safety Initiative (BSI)[24] event with an E3 event.

Information captured in E3 and pulled into BPETS/BPETS2 is used for reporting through the Intelligence Reports modules. These reports help to show the number of events that occur in a given location. These events can be apprehensions, seizures, or assists.

The GPRA module uses staffing, BSI, and apprehension information to display a situational analysis for USBP supervisors and managers. The GPRA module correlates staffing totals to enforcement events (apprehensions, seizures, deaths, and rescues). The GPRA module combines this information with other zone activities to display an estimated effectiveness for the area of responsibility. Additionally, the GPRA module displays the number of USBP agent staff to technology resources ratio in that area, and the number of enforcement event assists as a result of the assets. This information assists the duty location managers in making operational decisions (strategic or tactical) by giving an overview of both staffing/resource information and enforcement activity information available through BPETS/BPETS2.

All USBP employee information in the Staffing, Scheduling, and Timesheet modules is captured so that scheduling supervisors can assign manpower to specific locations within that duty location's area of responsibility. The schedule begins with an individual employee record. This employee record may have a schedule default; activity, sub-activity, and vehicle. If an employee

[24] The Border Safety Initiative (BSI) is held annually to promote messaging about the dangers migrants often face when illegally crossing the U.S./Mexico border. USBP works with consulates from various countries, media partners, and stakeholders to educate would-be immigrants about the risks associated with crossing the desert.

is assigned a vehicle; this vehicle information is maintained within the Vehicle Tracking module. The employee is identified as working a type of activity and sub-activity.[25] Activity types are used to determine whether the employee is operating in an enforcement or non-enforcement capacity (*i.e.*, agent or support). The employee is assigned to work in a specific location; these locations are defined in the zone management portion within the Scheduling modules. Once completed, this scheduling information identifies for the individual employee, a work schedule or shift, duties during that shift, which vehicle he or she will be driving, and in what area of the border he or she will be working. Additionally, these schedules are also used by radio dispatch as a guide for determining the agents that are working on a particular shift for the purpose of conducting safety checks over the radio.

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.

BPETS/BPETS2 aggregates enforcement data pertaining to encounters and types of seizures, as well as assists in rescues and deaths. This data helps to ensure proper staffing along the border to meet these threats and provide assistance when needed; the system does not conduct electronic searches, queries, or analyses to discover predictive patterns or anomalies.

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

BPETS/BPETS2 is not accessible by personnel outside of CBP.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is the risk that PII in this system may be used inappropriately or exploited.

Mitigation: All reports (obtained from the BPETS/BPETS2 applications, the USBP Statistics and Data Integrity Unit, or via the Business Object data query tools) are provided in standard formats that are clearly denoted with "For Official Use Only" or other applicable statement.

Legacy BPETS enforces access roles to limit what information is viewable by the authorized user. Additionally, BPETS2 mitigates this risk by enforcing stricter controls on what information authorized users are able to view. For example, users with the role of Supervisor can

[25] Sub-activity is another level of classification of the activities that agents perform. For instance, an activity would be Patrol Border, the sub-activity would provide more detail into what specific duties they were performing while Patrolling the Border, such as linewatch.

view and edit employee work schedules and assignments while users with the role of Personnel can view and edit HR-related data, such as EOD, job classification, and pay. All users of BPETS are required to pass a single scope background investigation before being granted access to the system, and access is restricted to the modules they need in order to perform their duties. An audit log is used to track all system activity, including the user, the date, time of action, and what action was performed. Users are required to take security and privacy training annually.

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.

USBP employees and contractors are aware that their personal information is collected in BPETS/BPETS2 by virtue of their access to the system, and their entry of personal information into the system. USBP employees and contractors understand that the personal and employment-related data collected into BPETS/BPETS2 is necessary for operational planning, the effective deployment of USBP resources, and congressionally mandated reporting of performance data. Individuals are made aware that their chain of command (supervisors) may see this personal information, but are given the option to un-hide their individual personal information from users outside of their chain of command.

BPETS/BPETS2 also uploads information related to incident subjects to populate BSITS reports and statistics. While the law enforcement nature of the encounter precludes CBP from providing prior notice, information is typically collected directly from the individual and either entered into the BSITS module by an agent at the local station/sector, or pushed to the BSITS module from E3 for reporting and statistical purposes. As described above, legacy BPETS stores PII related to subjects of border incidents. Eventually the BSITS module data elements will be captured in the Tracking, Sign-cutting, and Modeling module within E3,[26] and the existing data in the BSITS module will be maintained in legacy BPETS for historical purposes only.

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

As per the memorandum issued by Chief of the Border Patrol on April 8, 2005, titled "Use of Border Patrol Enforcement Tracking System," USBP employees and contractors cannot opt-out

[26] *See* DHS/CBP/PIA-012(a) CBP Portal (e3) to EID/IDENT and subsequent update, a*vailable at* www.dhs.gov/privacy.

of using BPETS/BPETS2 and are required to submit and maintain their personal information in the system.

Because the information collected about the individuals during an encounter is used for law enforcement purposes, subjects of incident events entered in the BSITS module do not have the ability to decline to provide the information or consent to particular uses.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is the risk that individuals may not be aware that their data is in BPETS/BPETS2.

Mitigation: This risk is only partially mitigated. Individuals whose data is collected as part of an incident cannot be provided advanced notice because of the law enforcement nature of an encounter. However, information is collected directly from the person to ensure accuracy, and consequently alerts the person to the collection of his or her information. This PIA provides additional notice.

USBP employees and contractors within CBP understand that the use of personal and employment related data collected in BPETS/BPETS2 is a condition of their federal employment in their capacity as agents. They are aware of their information is in BPETS/BPETS2 by virtue of their access to the system, and their entry of personal information into the system.

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.

BPETS will retain all records while they remain active. The inactive records will be destroyed according to the following retention schedule, portions of which are awaiting submission to NARA for approval.

- Audit records (tracked changes, search/view logs, and login audits) are destroyed or deleted six (6) years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.[27]
- Scheduling information is retained consistent with the NARA-approved scheduled for time and attendance records: destroyed after a Government Accountability Office audit or when

[27] Records are securely retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 3.2, Item 31, "User Identification, Profiles, Authorizations, and Password Files."

three (3) years old; whichever is sooner. This information includes:

- Schedule requests/leave requests;
- Work assignments-status, activity, sub-activity, location;
- Vehicle assignments; and
- Duty assignment information.

- Staffing Information
  - Staffing information retrieved from other systems are retained consistent with the retention guidelines of the source system.
    - The U.S. Department of Agriculture (USDA) National Finance Center (NFC), known as the USDA Bi-Weekly Examination Analysis and Reporting System (BEAR) feed must be deleted after a GAO audit or three (3) years, whatever is sooner.
    - In accordance with NARA General Records Schedule 2.4, Item 40, individual employee payroll records are destroyed when 56 years old.
  - Medical information (including doctor name and phone number, medical alerts, health plan name and code, blood type) is retained until the employee separates from USBP.[28]
  - Work contact information is retained for one year after an employee separates from USBP (becomes "deactivated" in the system), consistent with NARA General Records Schedule 2.2, Item 80
  - Employee and emergency contact information is retained until superseded or obsolete, or upon separation or transfer of the employee from USBP (becomes "deactivated" in the system), consistent with NARA General Records Schedule 2.4, Item 40.
- Employee records pertaining to assignment of accountable property is retained for three (3) years after deactivation, consistent with NARA General Records Schedule 5.4.
- Enforcement records of arrests, detentions, and removals are retained for 75 years. Investigative information that does not result in an individual's arrest, detention, or removal, is stored for 20 years after the investigation is closed, consistent with the N1-563-08-04-02. Enforcement information includes the following types of records:
  - GPRA;

[28] *See* OPM/GOVT-10 Employee Medical File System Records, 75 FR 35099 (June 21, 2010).

- Checkpoint;
- BSITS; and
- Operations Orders.

- CBP retains SNAP[29] information consistent with the EID retention period of 99 years.
- Summary information (such as statistics and summary tables of number of employees deployed in various locations) will be retained for the life of the system. Summary tables (such as statistics) do not contain PII.

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: BPETS/BPETS2 maintains records that have variable records retentions requirements, which increases difficulty in ensuring that records are destroyed in a timely manner. Most of the records maintained within BPETS/BPETS2 are covered by the records retention schedules above, and the disposition requirements will be built into the system. At the time of the publication of this PIA, USBP has not deleted any records from BPETS/BPETS2, but will begin to align BPETS/BPETS2 records with the schedules above. USBP will provide a quarterly progress report to the CBP Privacy Officer.

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.

CBP does not use BPETS/BPETS2 to share PII external to DHS. Only aggregate statistical reports, which are vetted through USBP Headquarters before being shared, are available to external organizations (*i.e.*, Congress, the White House, or Freedom of Information Act (FOIA) requests) upon request. These reports do not include PII.

[29] SNAP is the BPETS Snapshot of the EID data. SNAP is where BPETS downloads EID tables as a summary view to calculate BPETS statistics.

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

CBP does not use BPETS/BPETS2 to share PII external to DHS. Only aggregate statistical reports, which are vetted through USBP Headquarters before being shared, are available to external organizations. These reports do not include PII.

6.3 Does the project place limitations on re-dissemination?

Statistical reports shared with external organizations are provided in standard, non-editable formats (*e.g.*, PDF) and are clearly denoted as "For Official Use Only" or other applicable statement. These reports do not include PII.

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

CBP does not use BPETS/BPETS2 to share PII external to DHS, therefore CBP has no disclosures for which to account from BPETS/BPETS2.

6.5 Privacy Impact Analysis: Related to Information Sharing

There are no privacy risks to information sharing. BPETS/BPETS does not share PII external to DHS.

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?

Only authorized USBP employee and contractor personnel are granted access to BPETS/BPETS2 and have the ability (and are required) to maintain accurate personal information in BPETS/BPETS2. Users have access to their own PII, and have a responsibility to keep the data current. Supervisors have access to PII related to their subordinates and may update the data if necessary. Former USBP personnel who wish to access their BPETS/BPETS2 records may follow the redress procedures outlined in Section 7.2. CBP has exempted access to law enforcement records retained in accordance with the BPER SORN from certain provisions of the Privacy Act. CBP will review requests submitted under the procedures outlined in Section 7.2, but may withhold records if they are determined to contain law enforcement information.

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

To correct inaccurate data, current BPETS users can update their own basic contact information, or contact their immediate supervisor, personnel office, Border Enforcement and Management Systems Division (BEMS) user support, or the national help desk to request a change in their official personal information (such as grade/step). Additionally, there is a BPETS/BPETS2 email address where a user can request that BPETS system administrators review possibly inaccurate information.

Other individuals seeking notification of and access to records contained in BPETS/BPETS2, or seeking to contest its content, may submit a FOIA or Privacy Act request to CBP at https://foia.cbp.gov, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
1300 Pennsylvania Avenue, NW, Room 3.3D
Washington, DC 20002
Fax Number: (202) 325-1476

Requests for information are evaluated to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

All FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process.

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

Corrections to information regarding current USBP personnel are handled either directly by the individual or through his or her supervisor. Other individuals are advised of the procedures for correcting their information in this PIA, the applicable SORNs, as outlined in Section 1.2, and on the DHS and CBP public-facing websites.

7.4 Privacy Impact Analysis: Related to Redress

There is no risk to redress for inaccurate information stored within BPETS. All BPETS/BPETS2 records are covered by existing SORNs, which afford Privacy Act redress options, but all USBP employee and contractor personnel granted access to BPETS/BPETS2 are

required to maintain accurate personal information in the system. Any inaccurate subject, encounter, and seizure information is corrected, either automatically within BPETS/BPETS2 once the correction is made in E3, or manually in BPETS/BPETS2 by the assigned agent.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

The BPETS/BPETS2 application includes the following safeguards to prevent the misuse of data:

- Users are granted access to the system only when an authorized user creates their profile. Users cannot grant themselves access to the system.
- Users are granted roles to perform duties only when an authorized user who can set program access rights grants them permission. Users cannot grant roles to themselves unless they have been granted the role which allows them to set program access rights.
- Multiple concurrent active sessions for a user have been prevented by system security functions.
- Access privileges to BPETS/BPETS2, like all CBP systems, are deleted when the user no longer requires access to perform his or her job function.
- The system audit trail fully tracks the identity and activity of each person performing an action on the system, including the time and date of the access and logoff.
- The application software contains audit-logging routines that allow tracking activities of users that modify, bypass, or negate system security safeguards.
- Encryption algorithms, where implemented, are in compliance with Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules.*
- Data integrity controls (encryption, digital signatures) are used to ensure that tampering does not occur when transmitting or receiving data.

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

The CBP annual requirement for security training for information system users includes general principles of handling sensitive information, including privacy information. No additional privacy training specific to BPETS/BPETS2 is provided to users.

To mitigate the lack of BPETS/BPETS2 privacy-related training, access to PII is limited to the access needed to perform the user's duties. Further, accessing PII within BPETS/BPETS2 is a logged event.

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

USBP users who require access to BPETS/BPETS2 to perform their duties (*e.g.*, operations managers, human resource managers[30]) must first complete a single scope background investigation and receive the appropriate security clearance. BPETS is only accessible to individuals with access to the CBP network and who have completed a background investigation.

Each module of BPETS/BPETS2 has individual access controls to ensure that users only have access to modules they need to accomplish their specific mission functions. The system administrator controls[31] additional access to allow users to view or edit data in those areas of the application that are required to perform their job.

With the release of BPETS2, the majority of the PII is only accessible from within BPETS2. BPETS2 captures audit information for every user that views the personal information of another user. Legacy BPETS does not have as robust auditing capability.

[30] Once added to the system, all USBP employees and contractors have access to BPETS/BPETS2. USBP employees that perform HR-related work have access to the HR-related information in BPETS/BPETS2, such as grade/step/series.

[31] System administrator access is assigned to direct supervisors or above. If a user needs additional access, he or she will go to their direct supervisor for that access. If that supervisor cannot grant the access, he or she will go to a system administrator that can.

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?

It is not expected that BPETS/BPETS2 will be used by external users, but if that occurs in the future, memoranda of understanding will be reviewed by the program manager, the CBP Privacy Office, and the CBP Office of the Chief Counsel.

Responsible Officials

Tommy Smith
Operations Officer
U.S. Border Patrol
U.S. Customs and Border Protection
(202) 344-1794

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