Privacy Impact Assessment

for the

Enterprise Geospatial Information Services (eGIS)

DHS Reference No. DHS/CBP/PIA-041

December 2, 2022

Homeland Security

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) Enterprise Geospatial Information Services (eGIS) displays data on maps to monitor activities along the U.S. border for potential border vulnerabilities, corrective actions, border incidents, assets, and relevant events (such as arrests and seizures) using geographic data. eGIS presents visual displays of current and historical data from various DHS source systems to provide situational awareness for making critical organizational decisions. CBP is republishing and restructured this Privacy Impact Assessment (PIA) to assess this information technology system's privacy risk and to notify the public of previously published and new Portals that may collection, storage, retention, use, and dissemination of information within eGIS belonging to members of the public.

Overview

U.S. Customs and Border Protection (CBP) plays a critical role in securing the Nation's borders at and between the Ports of Entry (POE) against all threats. CBP approaches this mission from a risk-based approach, allowing the agency to apply information, integration, and rapid response in the most targeted, effective, and efficient manner. In securing the U.S. border, CBP objectives include:

- Preventing terrorists and terrorist weapons from entering the United States at and between POEs through improved and focused intelligence-driven operations, as well as operational integration, planning, and execution with law enforcement partners;
- Managing risk through the introduction and expansion of sophisticated tactics, techniques, and procedures. These include methods of detecting illegal entries such as using "change detection" techniques, increased mobile-response capabilities, and expanded use of specially trained personnel with "force multiplying" skills and abilities;
- Disrupting and degrading Transnational Criminal Organizations by targeting enforcement efforts against the highest priority threats and expanding programs that reduce smuggling and crimes associated with smuggling;
- Expanding CBP's situational awareness at and between POEs and employ a comprehensive and integrated "whole-of government" approach; and
- Increasing community engagement by participating in community programs and engaging the public to assist CBP.

The Enterprise Geospatial Information Services (eGIS) application enables CBP to meet the overarching strategic goals to secure the border. CBP uses eGIS to conduct patrol, surveillance, and

interdiction functions and conduct enforcement and apprehension processing, adjudication, and resolution. eGIS increases CBP geospatial data availability to improve real-timedecision making necessary for the protection of personnel and key resources. eGIS is a national, web-based set of applications designed to display data from multiple data sources spatially (i.e., on a browser-based map). Initially designed to support USBP's border security mission and primarily used by USBP, eGIS may provide maps and services to all CBP including support to Air and Marine Operations (AMO) and Office of Field Operations (OFO). eGIS facilitates the integration of multiple CBP enforcement systems to expose previously unrecognized spatial patterns and trends which can be used to better inform staffing and event responses. eGIS uses data to create maps from multiple data sources, identify patterns and trends, and enhance traditional tabular reporting capabilities. eGIS depicts border resources and activities to facilitate situational awareness. eGIS provides CBP personnel with an approved need the ability to view agency-specific data; personnel with additional privileges are able to view the locations of illicit activities and resource deployments within their area of responsibility. Some ofthe eGIS features include:

- Browser-based application available to all CBP employees and contractors;
- Ability to display and filter multiple map layers;
- Layers for Operation Waypoint data (a nationwide GPS gathering effort by USBP, ongoing since 2003 to precisely locate and inventory geographic features, both natural and man-made, that are specific to USBP enforcement operations); and
- Search for and display events from the e3 application.[1]

eGIS consists of two main applications and some geospatial services: eGIS Map (Legacy) viewer (eGIS Map Next Gen),[2] the mapping application available across the CBP enterprise providing users with a consistent, comprehensive depiction of CBP resource deployment and activities, and eGIS Portal, which allows users to create their own maps with their own data, and control sharing of those products. Both applications can include data uploaded by the user.

eGIS Portal

[1] An "event" within ENFORCE/EID or the E3 portal includes subject records on individuals arrested on suspicion of violating federal or state law, including federal immigration law. For more information on ENFORCE/EID, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates) and DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT (2012 and subsequent updates), U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3) TO ENFORCE, DHS/CBP/PIA-012 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy.

[2] eGIS Map NextGen is the evolution of eGIS Map (Legacy), delivering 3D visualization, a more modern interface, and an improved overall user experience. Development continues as we migrate over all functionality from eGIS Map.

The eGIS Portal is designed to increase geospatial visualization sharing across CBP. The eGIS Portal provides users the capability to search, discover, and access maps through a web browser; create and host web mapping applications; create groups for sharing geographic information system (GIS) information with coworkers or partners outside of CBP on an ad-hoc basis; share links to GIS applications; and sharemap and layer packages for users' desktops. The eGIS Portal includes the following modules:

1. Web AppBuilder - Permits users to design and build web applications using web maps without writing code. Web AppBuilder comes with various themes that can be customized and widgets that allow for deliveryof advanced functionality such as high-quality printing, geoprocessing, editing, and search.
2. Scene viewer - Enables users to view 3D geospatial content. The scene viewer works with desktop web browsers that support WebGL, a web technology standard for rendering 3D graphics.
3. ArcGIS applications - The eGIS Portal also supports geospatial applications that allow people to interact with web maps.

eGIS Map viewer[3]

The eGIS Map viewer is a web-based mapping application that depicts border resources and activities to facilitate situational awareness for agents and officers in the field. The eGIS Map viewer is a custom, internal CBP application that allows users to establish a customized map view area based on their area of responsibility or mission need. Users can turn on or off data content map layers to display using any web-enabled computer connected to the CBP intranet (CBPnet).

Basic features within eGIS are available to anyone with access to the CBP intranet. CBP law enforcement personnel (including, agents and officers from USBP, AMO, and OFO) with additional privileges can view the locations of illicit activity (e.g., illegal crossings) and resource deployments within their area of responsibility. Detailed information, including personally identifiable information (PII), is displayed when law enforcement users click on map dots if they have access to the underlying enforcement databases that supply the PII to eGIS. The eGIS Map viewer includes the following modules:

1. Map Contents - Allows users to add, remove, display, and organize map data layers of interest.
2. Base Maps - Allows users to select from over ten different map backgrounds (e.g., imagery, roads topographic) to enhance situational awareness.
3. Analysis Tools - Provides access to a number of analytical tools, such as creating an

[3] The eGIS Map viewer can be accessed from the eGIS Homepage or from the eGIS Portal.

activity heat map,[4] displaying personnel deployment, performing temporal analysis,[5] facilitating quality assurance reviews of activity data, and displaying detection viewsheds.[6] Additional tools include the ability to view Officer Safety Data information on fallen agents, draw graphics, measure distance/areas, and format coordinate display. This tool also allows users to query and export/download data.

4. Location tool – Allows users to upload a file with street address or latitude/longitude to find a geographic location.
5. Print and export – Allows users to print and download the results of queries they can run on some layers.
6. Bookmarks – Allows users to name and save a particular view of a map including the extent and layers they want to see again easily.

Types of Information Displayed by eGIS

eGIS allows authorized users to view the geographic location of data from various source systems as features on a map. eGIS is used to display information *already available to law enforcement users* through their access to various enforcement systems on a map for ease of use and identity patterns and trends of illicit activity. Users can click on the features to view attribute information of the event, which may include PII. Generally, the types of attribute information within eGIS include:

1. Historic Enforcement Data - Information pertaining to arrested subjects, including biographic and biometric information related to apprehensions and seizures.
2. Surveillance Data Feeds - Alert information from surveillance assets.
3. Intelligence Data - Location and type of reports logged in the Intelligence Reporting System (IRS).[7]
4. Officer Safety Data - Location of an assault and any weapons used by subjects on a CBP Officer or Agent; real-time location of CBP agents/officers using the mobile Team

[4] "Heat maps" display the density of historical spatial events, in practice meaning a large display of dots in an area where frequent apprehensions or seizures occur(ed). eGIS does not attempt to predict future events beyond displaying published weather forecasts. Rather, it serves as one of the input sources intelligence analysts use in their predictive analysis.
[5] Temporal data includes time and date information for geographic locations, which allows users to track real-time and previously documented observations. These observations can be discrete, such as lightning strikes, or continuous, such as trucking routes and flight paths. These observations do not include the tracking of individuals.
[6] A viewshed is the geographical area that is visible from a location. It includes all surrounding points that are inline-of-sight with that location and excludes points that are beyond the horizon or obstructed by terrain and otherfeatures (e.g., buildings, trees).
[7] A PIA for IRS is forthcoming.

Awareness Kit (TAK).[8]

5. Human Resources Data - Work and residence location of CBP personnel.[9]
6. Publicly available geospatial information - Locations of geospatial data within the open public domain to support CBP preparedness and resiliency. This data does not contain PII.

eGIS Sources of Information

eGIS does not store information from source systems. Rather, eGIS displays information from the CBP Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW) or directly from source systems.[10] Through EMIS-EDW, the eGIS Map viewer, and eGIS Portal leverage data from operational source systems for mapping capabilities (fully described in Section 3.0). EMIS-EDW serves solely as a data repository and reporting system and, therefore, does not update operational data. Therefore, eGIS cannot update or change the operational source systems, either. Rather, eGIS is a tool to visualize information in a geospatial manner that is already managed by CBP.

Typical eGIS User Transaction

eGIS provides authorized users with the ability to view specific attribute information through four tools:

- Identify: Users can click on a feature in the map to view attributes of that feature.
- Query: Users can structure queries to return information (excluding PII) on a specific data layer by user-defined location, timeframe, or specific attribute (e.g., how many seizures included firearms last year).
- Export: Users with export role access to specific layers can also download the results of their queries and save as a .csv file to view in Excel or as a geodatabase for use in commercial GIS software.
- Recidivist: Users can query subjects by the number of CBP recidivists counts and display them through the eGIS interface.[11]

[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE TEAM AWARENESS KIT (TAK), DHS/ALL/PIA-090 (2021), *available at* https://www.dhs.gov/privacy.
[9] This information is only available to the individual user and select Incident Management individuals.
[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE MANAGEMENT INFORMATION SYSTEM-ENTERPRISE DATA WAREHOUSE, DHS/CBP/PIA-034) (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy.
[11] Users enter two parameters, the number of arrests and a date range. The tool will return a list of subjects that have been arrested at least as many times specified in the defined date range. This list is sortable, containing the subject name, date of last arrest, etc. Users can "Zoom to Selection" to see the location of the last arrest as a dot on the map.

Access to non-sensitive data[12] in the eGIS Map viewer and eGIS Portal is granted within DHS through the DHS-wide Trusted Identity Exchange (TIE).[13] Access to sensitive data is managed through eGIS administration of user roles by verifying a user's identity and organization using the Border Patrol Enforcement Tracking System (BPETS)[14] and the DHS Active Directory.[15] eGIS administrators assign access or user roles based upon the particular user, organization, or geographic location, and the official need to know the information. In addition, administrators recertify eGIS users annually, view audit logs containing user logins and logouts and all administrative actions and send routine and emergency messages to users.

PIA Structure

CBP is republishing this PIA to provide transparency and evaluate any privacy risks associated with CBP's use of eGIS to collect and some use cases to display PII data on members of the public to authorized users.

This PIA describes the approved use cases for eGIS. All use cases are consistent with CBP border security and law enforcement authorities and conform to the purpose for which the data was originally collected. A comprehensive list of eGIS portal apps that collect or display PII is found in Appendix B of this PIA.

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's law enforcement jurisdiction is highly complex and derives authority from a wide spectrum of federal statutes. The information collected and maintained in eGIS and its source systems are used in furtherance of CBP's law enforcement authorities and responsibilities. Relevant authorities include:

- 5 U.S.C. § 301;
- Homeland Security Act of 2002, as amended, 6 U.S.C. § 101, et seq., including but not limited to 6 U.S.C. §§ 202, 211;
- The Immigration and Nationality Act ("INA"), 8 U.S.C. § 1101, et seq., including 8

[12] The table in Section 2.2 designates what data is non-sensitive/sensitive. Generally, the non-sensitive data is just geographic information without any PII/enforcement information.
[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS Trusted Identity Exchange, DHS/ALL/PIA-050 (2015), *available at* https://www.dhs.gov/privacy.
[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE Border Patrol Enforcement Tracking System (BPETS/BPETS2), DHS/CBP/PIA-046 (2017), *available at* https://www.dhs.gov/privacy.
[15] The DHS Active Directory attributes to the requesting agency/component which may be shared outside of the DHS network for purposes of authenticating users.

U.S.C. §§ 1103, 1185, 1225, 1324, and 1357;

- The Tariff Act of 1930, as amended, including but not limited to 19 U.S.C. §§ 482, 1461, 1496, 1581, and 1582;
- Enhanced Border Security and Visa Reform Act of 2002 (Pub. L. 107-173);
- Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (Pub. L. 104-208, Division C);
- Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458);
- Secure Fence Act of 2006 (Pub. L. 109-367);
- Security and Accountability for Every Port Act of 2006 (Pub. L. 109-347);
- Trade Act of 2002 (Pub. L. 107-210);
- 8 C.F.R. § 287.2; and
- 19 C.F.R. § 162.6.

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

eGIS displays information based on location. The information is also searchable by unique identifiers such as name, Alien Number (A-Number), or other biographic information from subject records. eGIS users can display Privacy Act-covered subject records. In addition, several eGIS Portal applications display and, in some cases, collect location and PII on members of the public. eGIS users can display Privacy Act-covered landowner contact information, and collect information following vessel encounters, 911 emergency calls in response to missing migrant inquiries, as well as information on known stash houses. These use cases and the specific PII collected will be discussed in detail in Appendix B.

For transparency, eGIS displays records covered by the following SORNs:

Historic Enforcement Data (including apprehensions, seizures, and other adverse actions):

- DHS/CBP-023 Border Patrol Enforcement Records (BPER),[16] which covers records related to securing the border between Ports of Entry. The BPER SORN covers eGIS records originating from the Border Patrol Enforcement Tracking System (BPETS) and e3 Biometrics System.
- Certain enforcement records may also be related to inspections or enforcement actions

[16] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 Fed. Reg. 72601 (October 20, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

taken at official POEs and are covered under DHS/CBP-010 TECS.[17]

- Records related to seizures are maintained in accordance with DHS/CBP-013 Seized Asset and Case Tracking System (SEACATS).[18]
- Enforcement information from the U.S. Immigration and Customs Enforcement (ICE) Enforcement Integrated Database (EID) is covered under DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER).[19]

Surveillance Data Feeds (Blue Force Tracking,[20] marine vessel tracking sensors, and surveillance):

- DHS/CBP-023 Border Patrol Enforcement Records (BPER).
- DHS/CBP-019 Air and Marine Operations Surveillance System (AMOSS)[21] which contains surveillance event and operations data. AMOSS supports domestic operations in conjunction with other domestic law enforcement agencies by tracking domestic flights, as well as providing air traffic monitoring for air defense purposes. By processing a collection of external data imposed over a zooming-capable screen, AMOSS provides a real-time picture of air activity over a wide portion of North America, thus allowing system operators to discriminate between normal and suspicious air, ground, and marine vehicle movement. Much of the external data processed by AMOSS does not contain PII and is supplied to AMOSS by means of networked external sources. For instance, GPS from CBP vehicles or law enforcement investigations, maps, datasets from radar plot data, track data, and flight plan data are all incorporated to enhance the system operator's ability to differentiate between normal and suspicious aviation movement.
- Marine Vessel Tracking information is imported from commercial vessel tracking

[17] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (December 19, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[18] *See* DHS/CBP-013 Seized Assets and Case Tracking System, 73 FR 77764, (December 19, 2008), *available at* www.dhs.gov/system-records-notices-sorns.
[19] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016), *available at* www.dhs.gov/system-records-notices-sorns.
[20] Blue Force Tracking is a term for a GPS-enabled system that provides location information about other law enforcement vehicles and aircraft.
[21] *See* DHS/CBP-019 Air and Marine Operations Surveillance System (AMOSS), 78 FR 57402 (September 18, 2013), *available at* www.dhs.gov/system-records-notices-sorns. AMOSS is a sophisticated radar processing system that supports the concerted and cooperative effort of air, land, and sea vehicles; field offices; and command and control centers staffed by law enforcement officers (LEO), detection enforcement officers (DEO), pilots, crew, and Air and Marine Operations Center (AMOC) support staff inmonitoring approaches to the U.S. border to detect illicit trafficking and direct interdiction actions, as appropriate.

services and is therefore not covered by a Privacy Act system of records.[22]

Intelligence Data:

eGIS does not display finished intelligence information but displays the location and type of reports logged in the Intelligence Reporting System (IRS).[23] While finished intelligence information does not contain PII, some eGIS Portal applications display PII on members of the public. See Appendix B for detailed information on these eGIS Portal applications.

- DHS/CBP-024 Intelligence Records System (CIRS) System of Records.[24]

Encounter Data (vessel encounters, 911 emergency call data, and missing migrant inquiries)

- DHS/CBP-023 Border Patrol Enforcement Records (BPER), covers records related to securing the border between Ports of Entry.[25] The BPER SORN covers eGIS records originating from the Border Patrol Enforcement Tracking System (BPETS) and e3 Biometrics System.
- DHS/CBP-010 TECS covers certain enforcement records that may also be related to inspections or enforcement actions taken at official POEs.[26]
- DHS/CBP-013 Seized Asset and Case Tracking System (SEACATS) covers records related to seizures.[27]
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) covers enforcement information from the U.S. Immigration and Customs Enforcement (ICE) Enforcement Integrated Database (EID).[28]
- DHS/CBP/PIA-075 Intelligent Computer Assisted Detection (ICAD) System

Officer Safety Data (use of force and assaults):

- DHS/ALL-020 Department of Homeland Security Internal Affairs, which covers records related to internal investigations.[29] Use of force incidents may also be

[22] Commercial services aggregate the marine automatic identification system (AIS), an automatic tracking system used for collision avoidance on ships and by vessel traffic services (VTS). For an example, please *see* https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4.
[23] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198, *available at* https://www.dhs.gov/privacy.
[24] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198, *available at* https://www.dhs.gov/privacy.
[25] *See supra* note 16.
[26] *See supra* note 17.
[27] *See supra* note 18.
[28] *See supra* note 19.
[29] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361, *available at* https://www.dhs.gov/privacy.

documented in relation to an enforcement record and would receive coverage under the SORNs listed above.

CBP Human Resources Data:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) covers records related to the provision of access to information technology resources.[30]
- DHS/ALL-014 Department of Homeland Security Emergency Personnel Location Records System covers work and residence location of CBP personnel.[31]

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

Yes. eGIS has undergone the Security Authorization process in accordance with DHS and CBP policy, which complies with federal statutes, policies, and guidelines. The eGIS program has an ongoing Authority to Operate eGIS Cloud has an Authority to Operate that expires March 4th, 2025. All of eGIS will eventually move to eGIS Cloud. During the implementation, eGIS will continue to operate concurrently.

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

eGIS does not ingest, store, or extract source information from EMIS-EDW. EMIS-EDW retains all source information in accordance with the record retention requirements of those source systems. eGIS uses the eGIS Map Viewer and eGIS Portal to display records from EMIS-EDW. Some eGIS Portals collect and retain personally identifiable information on members of the public.

The eGIS Map Viewer does create and retain information about users, roles, and access requirements. It also stores user bookmarks and preferences, as well as logging and auditing data. The eGIS Map Viewer also retains local data uploaded by end users and the eGIS Portal retains data that is created by eGIS Portal users. The CBP Records Office is currently drafting a Records Retention Schedule for data specific to the eGIS Portal. CBP has proposed to retain data specific to eGIS for seven years and then archive it for up to 40 years. Cost and performance impact of data retention may lead to retention periods of less than 40 years.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number

[30] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, *available at* https://www.dhs.gov/privacy.
[31] *See* DHS/ALL-014 Department of Homeland Security Emergency Personnel Location Records, October 17, 2008, 73 FR 61888, *available at* https://www.dhs.gov/privacy.

for the collection. If there are multiple forms, include a list in an appendix.

The Paperwork Reduction Act (PRA) does not apply to eGIS because it does not collect information directly from members of the public.

Section 2.0 Characterization of the Information

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

Historic Enforcement Data

Most of the subject records displayed by eGIS come from the E3 portal, which collects and transmits encounter records to ENFORCE-EID and IDENT.[32] Enforcement information from E3 includes biographic, biometric, encounter, border violence, and prosecution-related data obtained from individuals during encounters. The information listed below is not exhaustive; other data may be collected that is consistent with the general categories listed below.

- Biographic data includes: name, aliases, date of birth, phone numbers, addresses, nationality, Social Security number, A-Number, employment history, educational history, immigration history, criminal history.
- Biometric data includes: height, weight, eye color, hair color, fingerprints, iris scans.
- Encounter data includes: location of apprehension/encounter; subject name; place of birth; date and time of apprehension; citizenship; matches to information in screening databases, identification numbers of documents found on the individual, including but not limited to State ID number, driver's license number, A-Number, or Travel Document Number; Fingerprint Identification Number (FIN); violations.
- Border violence data (see Officer Safety Records data below).
- Prosecutions (case management) data.
- Static and video images from surveillance assets.
- Location and type of reports logged in the Intelligence Reporting System (IRS). This data does not contain PII.

Officer Safety Records

[32] For more information about the E3 portal, please *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3) TO ENFORCE, DHS/CBP/PIA-012 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy.

- CBP Officers/Agents: name, Hash ID, business phone number, email address, duty location, incident location, weapon make/model/serial number.
- Subjects: name, gender, height, weight, date of birth/age, immigration status, assault charge, injury information (if applicable), medical facility address and phone number (if applicable).
- Witnesses: name, phone number and address (if available), testimony, country of origin.
- Incident data: title/description of incident, incident ID number, date/date range of incident, time of incident, reporting organization/agency, location of incident, type of premises, property damage information (property type, description, value), weapon make/model/serial number.

CBP Human Resources Data

In eGIS, authorized users can display PII on CBP personnel. The WebTele employee database is the only map layer that displays PII of CBP employees. Within eGIS, authorized users may be permitted to display the following fields on CBP personnel: government or contractor employee, Hash ID, name (first, middle, last), agency code, title, work address, work phone number, home address, home phone number, emergency contact name,[33] alternative contact name, emergency address, emergency phone number, home info last update date/time, alternative phone number, alternative phone number relation, emergency phone number relation, emergency city name, emergency doctor name, geographic location.

Publicly Available Geospatial Information

eGIS displays a vast amount of sensor and satellite imagery, most of which is publicly available.

PII on Members of the Public

In addition, some eGIS Portal applications collect, retain, disseminate, or maintain data on members of the public, including but not limited to name, cellphone number, address, license plate number, date of birth, vessel information, driver's license number, and passport number. Detailed information on these collections and their use are discussed in Appendix B.

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

eGIS data sources are continually being updated and expanded. Much of the information within eGIS is raw video, photograph, audio, ground sensor, and radar data using border

[33] Emergency contact information is not retrieved by unique identifier, and therefore no SORN coverage is required.

surveillance systems in rural and populated areas at or near the U.S. border.[34]

PII on members of the public are only displayed within eGIS and covered in further detail within Appendix B. This information is collected and entered by CBP personnel during encounters with members of the public or during investigations. For example, CBP personnel enter PII when investigating suspected immigration violations, during 911 emergency calls for assistance, or in response to inquiries related to missing migrants.

In the case of landowner parcel and contact information, eGIS does not ingest, store, or extract information from the contract vendor source. During the eGIS user's session, landowner parcel and contact information will be displayed using the eGIS Map Viewer. The data is retained in the contract vendor source system and will not persist in eGIS when the eGIS user session ends. The eGIS Map Viewer does create and retain information about CBP users, roles, and access requirements. It also stores user bookmarks and preferences, as well as logging and auditing data. The eGIS Map Viewer retains local data uploaded by end users, and the eGIS Portal retains data that is created by eGIS Portal users. USBP is currently working with the CBP Records Office in drafting a Records Retention Schedule for data specific to the eGIS Portal.

In addition to collecting and displaying data directly in eGIS Portal applications, eGIS ingests information from numerous data sources. Refer to Appendix A for a complete list of data sources ingested or used by eGIS.

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

Yes. The eGIS platform ingests information from commercial and publicly available data sources to enhance situational awareness, agent safety, and emergency preparedness/response. Examples of publicly available data that eGIS uses include earthquake, flooding, wildfire, and tropical storm data feeds provided by the National Oceanic and Atmospheric Administration (NOAA), United States Geological Survey (USGS), and other sources. Further, publicly available infrastructure locations are included in eGIS from the Homeland Infrastructure Foundation-Level Data (HIFLD) sources. Examples of these include emergency services (hospitals, fire stations, evacuation routes) and transportation infrastructure (bus stations, railroads, mass transit). The eGIS platform also ingests commercial weather data from Weather Underground (The Weather Company, IBM) to provide users with more detailed weather conditions in more local areas. The eGIS platform also leverages geospatial data services such as traffic conditions, landscape

[34] For a detailed description of all CBP Border Surveillance Systems, and the privacy risks associated with them, please See U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE BORDER SURVEILLANCE SYSTEMS, DHS/CBP/PIA-022 (2014 and subsequent updates), available at https://www.dhs.gov/privacy.

elevation, base maps, and more to support situational awareness.

In addition, there are access-controlled applications in eGIS Portal that display landowner parcel and contact information collected from a contract vendor source. This is only used to assist CBP during the Rights of Entry (ROE)[35] and Right of Way (ROW)[36] negotiations.

2.4 Discuss how accuracy of the data is ensured.

While the majority of datasets available within the eGIS platform originate from external (non-eGIS) data sources, multiple data quality measures have still been implemented to improve data accuracy throughout the system. For example:

- A Data Review tool was developed and integrated directly within the eGIS Map Viewer application to identify potential geospatial errors.[37]
- Detailed annual system access training, documentation, and quality checks have been put in place to ensure that data accuracy is maintained.
- USBP maintains a Statistics and Data Integrity Unit within the headquarters office that is specifically tasked with monitoring and ensuring data integrity represented within the eGIS system, among others. This unit follows standard operating procedures (SOP) to periodically and systematically review data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of over-collection of public PII because eGIS displays information from publicly available sources.

Mitigation: This risk is partially mitigated. CBP mitigates this risk associated with overcollection by ensuring that data is only temporarily cached during the user's session and is purged upon completion.

Privacy Risk: Because eGIS obtains landowner parcel and contact information from a subscription service, there is a risk that information within eGIS may be outdated or inaccurate.

Mitigation: This risk is not mitigated. CBP relies on the contract vendor source to ensure the accuracy of the landowner parcel and contact information, and the contract vendor source relies

[35] Right of Entry (ROE) refers to the legal right to enter upon real property of another for a special purpose without being guilty of trespass.
[36] Right of Way (ROW) is an easement, a privilege to pass over the land of another, whereby the holder of the easement acquires only a reasonable and usual enjoyment of the property, and the owner of the land retains the benefits and privileges of ownership consistent with the easement.
[37] The Data Review tool identifies events with latitude/longitude anomalies for further review. For example, if an arrest is identified as occurring in a station's area of responsibility (AOR), the Data Review tool assists in verifyingthat eGIS is displaying the correct AOR.

on publicly available local county tax records for data accuracy. Landowner parcel and contact information in eGIS are updated or refreshed when the information in the public record source system is updated. However, USBP Sectors and Station points of contact, specifically Ranch Liaisons, help verify that the information made available from the contract vendor source is accurate. USBP will notify the contract vendor source of any data discrepancies.

Privacy Risk: There is a risk that CBP may incidentally collect information from individuals who are complying with the law and are not subjects of interest.

Mitigation: This risk is partially mitigated. CBP may deploy sensors, cameras, and surveillance technology in areas that are trafficked by members of the public who are not the target of CBP's investigative efforts. For example, CBP uses sensors that may detect and track members of the public engaged in recreational boating. Due to the covert nature of the placement of this equipment, CBP cannot provide appropriate markings or signage that would allow individuals to avoid the area to prevent CBP's collection of their information. CBP partially mitigates this collection risk by strictly controlling the collection, use, and retention of information it collects through BSS[38] and the publication of this PIA.

Privacy Risk: There is a risk that individuals are not aware their information is stored in the eGIS Portal.

Mitigation: This risk is partially mitigated. When appropriate, CBP provides notice at the time of collection. Regardless of the law enforcement or border security reasons for the information collection, CBP has published SORNs for all information types, available at https://www.dhs.gov/system-records-notices-sorns.

Privacy Risk: There is a risk of over-collection because eGIS imports information from Border Surveillance Systems, which may capture information about individuals or activities that are beyond the scope of CBP's authorities. Video cameras can capture individuals entering places or engaging in activities as they relate to their daily lives because the border includes populated areas. For example, eGIS may collect video of an individual entering a doctor's office, attending public rallies, social events or meetings, or associating with other individuals.

Mitigation: eGIS provides a snapshot in time view for authorized users. It does not provide real-time surveillance but rather displays historical encounter data. At the point of collection, cameras, radar, and other border surveillance tools are oriented toward the border and away from communities and places of worship and commerce frequented by local residents when operationally feasible. While CBP records lawful activity at or near the border, these recordings are automatically overwritten unless an authorized user determines the recording is needed for an

[38] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE BORDER SURVEILLANCE SYSTEMS, DHS/CBP/PIA-022 (2014 and subsequent updates), *available at* https://www.dhs.gov/privacy.

approved purpose. Specifically, CBP copies and retains information only when relevant to an active case file for law enforcement or border security purposes. Additionally, CBP does not associate the recorded video or other data with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation.[39]

Privacy Risk: There is a risk of over-collection because eGIS consolidates many different sources of information into one information technology system.

Mitigation: To facilitate and further the overall CBP goal to secure the U.S. border, CBP uses information within eGIS to collect, store, and retrieve geolocation imagery and coordinates, biographic, and biometric records about individuals, vehicles, vessels, property, or aircrafts encountered, apprehended, or seized at or between POEs. These records include encounters of individuals (including U.S. citizens and non-U.S. citizens) related to border crossing events and activities, and information associated with individuals that are detected, apprehended, detained, or involved with surveillance technologies. These encounters can also include information about Border Patrol Agents and assaults made against them, as well as the use of force that may be necessarily exercised during an encounter.

Therefore, this risk is mitigated because, despite the amount of information that eGIS can access, all of the data sources listed in Section 2.2 support the same purpose for the collection. All eGIS data has a nexus to the CBP law enforcement and border security missions, particularly most data sources are tailored to support Border Patrol, as well as Air and Marine, operations along the southwest border. Any human resource or personnel information stored by eGIS is used strictly to facilitate the border security mission and allocate resources and manpower.

Privacy Risk: Because eGIS aggregates information from various source systems through EMIS-EDW, there is a risk that information within eGIS may be outdated or inaccurate.

Mitigation: Information displayed in eGIS from EMIS-EDW is collected from the source systems and updated one or more times a day. EMIS-EDW relies upon the source systems to ensure that data used by eGIS is accurate and complete. Discrepancies may be identifiedin the context of a CBP Agent or Officer's review of the data, and when discovered, the CBP Agent or Officer will take action to correct that information in the source system. When corrections are made to data in source systems, the updated information is uploaded into EMIS-EDW at the established intervals, ensuring that only the most current data is used for reporting within EMIS-EDW.

eGIS extracts data from systems identified in Section 2.2. Procedures for correcting inaccurate or erroneous information will be handled by those source systems as appropriate. eGIS incorporates the procedures of the source systems with respect to error correction. Once any updates or corrections are made in the source systems, they are transmitted to EMIS-EDW and

[39] *See supra* note 29.

displayed in eGIS. Corrected data becomes available to EMIS-EDW via regularly scheduled refresh processes. The refresh processes detect updated records in the source systems and appropriately update the same records in EMIS-EDW. EMIS-EDW monitors source systems for changes to the source system databases. When corrections are made to data in source systems, EMIS-EDW and eGIS reflect these updates to data, accordingly.

In addition, most of the information within eGIS is used to geospatially visualize existing operational data. It is not used to make real-time operational decisions or adverse actions about a specific individual, but rather is used to identify trends and patterns based on the type(s) and location(s) of activities.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

eGIS is used to identify border security trends and provide geospatial analysis of incidents and events using web-based maps. These maps monitor border vulnerabilities, corrective actions, border incidents, and events that contain geographic data. Displaying data on a map assists CBP personnel in identifying trends in border incidents for staffing and event responses. Other mapped data assists CBP in identifying areas of weakness in its border management mission.

Within the eGIS Portal, users can access featured content, HIFLD Open-Source Public Data, link to the eGIS Map Viewer application, information on data sources, and get help from the eGIS helpdesk. Users can use the "Feedback" form at the bottom of the homepage to provide feedback and help improve the eGIS Portal. Within the "Gallery" section of the eGIS Portal, users can browse featured maps, web mapping applications, and any new datasets available to the CBP enterprise, as long as they have access to the source system from which the data is pulled. Additionally, users can create a custom list of favorites. Using the "Map" function, users can build interactive web maps and share them with others in their organization based on geographic area and mission. Users can choose a base map and area of interest,[40] and add information layers. Once a user has finished building a map, he or she can refine it, save it to a personal workspace, or share it with other eGIS users.

eGIS also features "Groups" and "My Content." "Groups" permits users to create a collection of items (maps or layers), usually related to a specific topic of interest. Group owners choose settings for whether the group is searchable if others can request to join, and who can contribute content. "My Content" allows users to add and share web maps and applications, files from their computer,[41] and content from the web. eGIS Portal enables users to upload additional

[40] User defined. Typical boundaries include a city, street, sector, etc.
[41] Multiple file types can be uploaded from a user's workstation. If formatted properly, authorized users can uploadPII from their workstation.

file types such as image and document files and share their content to members of groups in the portal. All members of a group are permitted to view content that has been shared to the group. Data collected and displayed in these user defined portals are discussed in detail in Appendix B.

A select group of DHS, U.S. Immigration and Customs Enforcement (ICE), and United States Coast Guard (USCG) users can access the eGIS Map Viewer and eGIS Portal according to the user's authorized role access. These external eGIS users will not have access to the landowner parcel and contact information.

All uses of information are discussed in detail in Appendix B.

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. eGIS displays data elements, such as apprehensions and seizure data to identify illegal border activity trends and to allocate appropriate resources. It is not used for data mining.

While the system provides heat maps that display the density of historical spatial events, eGIS does not attempt to predict future events beyond displaying published weather forecasts. Rather, it serves as one of the input sources intelligence analysts use in their predictive analysis.

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

ICE and USCG users can access the eGIS Map Viewer and eGIS Portal according to the user's authorized role access.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PII within eGIS, including CBP employee data, may be inappropriately used or exploited.

Mitigation: Several controls are in place to mitigate the risk of inappropriate use of the information: 1) users of eGIS are required to pass a background investigation before being granted access to the system; 2) access is restricted to individuals with an official need to know to perform their duties; 3) audit logs are used to track all system activity, including the user, the date, time of action, and what action was performed; 4) all eGIS users must complete the Privacy at DHS: Protecting Personal Information training class annually; and 5) upon entry into eGIS, the user is presented with a reminder/disclaimer on the home page of the eGIS Portal website regarding the type of data permitted on the site. In addition, eGIS limits access to the layer by with information is viewed through strict access and role management controls.

Privacy Risk: There is a risk that PII within eGIS, including members of the public, may be inappropriately used or exploited.

Mitigation: Several controls are in place to mitigate the risk of inappropriate use of the information: 1) users of eGIS are required to pass a background investigation before being granted access to the system; 2) access is restricted to individuals with an official need to know to perform their duties; 3) audit logs are used to track all system activity, including the user, the date, time of action, and what action was performed; 4) all eGIS users must complete the Privacy at DHS: Protecting Personal Information training class annually; and 5) upon entry into eGIS, the user is presented with a reminder/disclaimer on the home page of the eGIS Portal website regarding the type of data permitted on the site. Access to data in eGIS Portal applications is restricted to groups with a need to know.

Privacy Risk: There is a risk that the missing migrant PII shared outside of DHS may not be handled appropriately by the entity receiving the information.

Mitigation: This is risk is mitigated. CBP implements a rigorous approval process for sharing information with external entities. A Memorandum of Understanding (MOU) or an Interagency Service Agreement (ISA) is completed between the two entities (i.e., CBP and the external entity) outlining strict guidelines for how the information should be handled. In the event of a request for information or ad hoc information disclosure, CBP has robust internal procedures governing the disclosure of information to external entities.

Privacy Risk: There is the risk that CBP personnel may enter inaccurate information into eGIS.

Mitigation: The training and interviewing techniques employed by USBP agents and CBP Law Enforcement Communication Assistants (LECA) reduce the risk of inaccurate information being entered in the system. While CBP cannot fully mitigate the accuracy risks, USBP agents use all information available to assess whether the information provided is accurate and warrants further investigation.

Privacy Risk: There is a risk that eGIS may capture information about individuals, locations, vessels, or activities that are beyond the scope of CBP's authorities. Sensors can capture information about individuals entering places or engaging in activities as they relate to their daily lives because the U.S. border includes populated areas. For example, sensors may collect images of an individual hiking or boating along the border.

Mitigation: While sensors may record lawful activity at or near the U.S. border, CBP does not associate the sensor data with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation. Sensors are oriented toward the U.S. border and away from communities and places of worship and commerce frequented by local residents as much as operationally feasible.

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.

All persons entering the United States are subject to data collection requirements and processes, including providing biometric data. Individuals are made aware of the information collection requirements by signage posting at POEs. Individuals encountered between ports of entry attempting to enter the United States unlawfully may not be provided advanced notice; such persons are provided notice at the time the information is collected (i.e., during the apprehension), except in circumstances where providing notice would compromise theoperation. All persons are provided general notice through this PIA and the applicable SORNs listed in Section 1.2.

CBP employees and contractors are required to submit and keep current certain personal information as a condition of employment. When an individual accesses eGIS, his or her username and profile from Active Directory is displayed. Therefore, while employees and contractors do not have advance notice that their information is used by eGIS, it is implied that their user profile from WebTele and Active Directory will be shared to access CBP information technology.

In general, eGIS does not collect any information directly from individuals. Most of the information that is used in eGIS comes from the CBP or government data sources identified in Appendix A, or from publicly available data sources (See Appendix B).

Some eGIS Portal applications display publicly available data while others display PII from members of the public. In some instances, PII is provided voluntarily to assist CBP in performing their law enforcement duties while in other instances it is collected during a law enforcement interaction with members of the public.

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

For law enforcement records, individuals do not have an opportunity to provide consent or decline to provide information. CBP employees and contractors are required to submit and keep current certain personal information as a condition of employment. Individuals are made aware that their chain of command may see this personal information but are given the option to hide personal information from users outside of their chain of command. Employees and contractors who decline to provide this information may be denied employment or continued employment.

Members of the public do not have an opportunity to provide consent or decline to provide this information. Some data displayed is from public sources while other data is voluntarily provided during an interaction with CBP.

In addition, this PIA and the DHS/CBP-024 Intelligence Records System (CIRS) System of Records provides public notice of CBP's use of publicly available landowner data.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that CBP may use information in eGIS without providing notice or without the consent of the individual.

Mitigation: Individuals encountered between ports of entry and are therefore attempting to enter the United States unlawfully, may not be provided advanced notice; such persons are provided notice at the time the information is collected (i.e., during the apprehension), except in circumstances in which providing notice would compromise the operation. Additionally, all persons are provided general notice through the publication of this PIA and the publication of the relevant SORNs noted in Section 1.2. Any individual with additional questions or concerns about how his or her information is collected or handled may contact the CBP INFOCENTER at (877)-227-5511, the search bar at https://help.cbp.gov/s/?language=en_US, or follow the procedures in Section 7 of this PIA.

Section 5.0 Data Retention by the project

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

As described above, eGIS Map viewer *displays* information from EMIS-EDW, which follows the retention period established by the underlying source systems for the data. Whenever EMIS-EDW is refreshed, eGIS will reflect the updated information. Therefore, whatever changes are made at the source system level are then transmitted to EMIS-EDW and displayed by eGIS.

For information stored within the eGIS Portal, such as user-created maps and preferences, CBP is proposing a retention period for the eGIS Portal of seven years and then the data is archived for up to 40 years. Cost and performance impact of data retention may lead to retention periods less than 40 years.

5.2 Privacy Impact Analysis: Related to Retention

With the exception of some limited public data, eGIS does not ingest, store, or extract any source system information. See Appendix A and B for source system and details related to collection, use, and retention.

Privacy Risk: The primary risk associated with retention is retaining the publicly available information longer than necessary. This would increase the risk of unauthorized access, use, and loss of the data.

Mitigation: eGIS mitigates this risk by not ingesting or retaining publicly available information in eGIS. This information will only be displayed using eGIS Map Viewer in a special-

access layer. The information will be viewed during the user's session but only retained in the original data source. No information used in the eGIS Map viewer will be retained in eGIS once the user's session is closed.

The eGIS program manager will continue to work with the CBP Records Information Management Office to identify and/or develop a record retention schedule for each type of record collected and retained in eGIS. Until an approved record retention schedule is approved, all eGIS records will be retained for the purposed 40-year retention. Storing these records for a long period of time is necessary to provide CBP the ability to view law enforcement and investigation patterns.

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.

Reports and maps may be shared outside of DHS on an *ad hoc* basis. These maps and reports are vetted through USBP Headquarters prior to being shared with external organizations.

These reports do not include PII.

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

Ad hoc maps and reports do not contain PII.

6.3 Does the project place limitations on re-dissemination?

Sharing with external organizations is limited to sharing non-PII reports and maps on an *ad hoc* basis and vetted by USBP Headquarters prior to sharing. There are no limitations to re-dissemination for PII reasons, however these maps and reports may be marked as Law Enforcement Sensitive or other classification.

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

CBP does not maintain a record of disclosures from eGIS pursuant to the Privacy Act because no PII is included in the reports or maps.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no risk to information sharing. eGIS does not share PII outside of DHS and has no external users.

Section 7.0 Redress

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

eGIS is a geospatial visualization reporting tool that extracts data from various databases but, in most cases, does not actively collect the information in those respective databases. In some situations, eGIS Portal applications are created and used to collect and retain information on members of the public. These eGIS Portals are discussed in detail in Appendix B. When an individual is seeking redress for other information analyzed in eGIS, he or she must locate the database that directly collect that information and request access, correction, or amendment of his or her information by following the access procedures outlined in the PIAs and SORNs of the source systems.

Individuals seeking notification of and access to information contained in CBP records may gain access to certain information by filing a Freedom of Information Act (FOIA) request with CBP at https://foia.cbp.gov/ 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, D.C., 20229
Fax Number: (202) 325-1476

U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information. CBP will refer requests for information contained in immigration systems maintained by other DHS components or by United States Department of Health and Human Services or United States Department of Justice to those agencies for additional processing.

All Privacy Act and 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. Requests for information are evaluated by CBP 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.

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

Individuals may seek redress and/or contest a record through two different means. Both will be handled in the same fashion. If the individual is aware the information is specifically handled by CBP, requests may be sent directly to CBP FOIA (via the procedures described above). If the individual is uncertain what agency is responsible for maintaining the information, redress

requests may be sent to DHS Traveler Redress Inquiry Program ("TRIP"), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

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

Upon request, CBP officers may provide a fact sheet that provides information on appropriate redress. The redress procedure provides the ability to correct data in the source systems; however, as discussed earlier in this document, it may not be clear to the requestor that his or her information is retained in eGIS. Additional information is available on DHS's website. The source system SORNs also provide information on accessing and amending information collected through those systems.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals are unable to correct their information directly in eGIS.

Mitigation: This risk is partially mitigated by the frequency with which information is updated or refreshed in EMIS-EDW. EMIS-EDW and eGIS are updated or refreshed when the information in the source system is updated. These updates occur every day, ranging from every 15 minutes to once a day. As a result, when a record is modified or corrected in the source system, it also is modified or corrected in EMIS-EDW and then within eGIS. However, some privacy risk remains because the information contained in finished reports generated by eGIS is not refreshed, and eGIS users may not be aware that the information in the report is out of date or inaccurate.

Privacy Risk: Due to the amount of aggregated information within eGIS, there is a risk that individuals will be unable to locate the relevant SORN or redress procedures for accessing, correcting, or amending their information.

Mitigation: This risk is mitigated because CBP is publishing this PIA, which lists all of the eGIS source system SORNs in Section 1.2.

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

Mitigation: This risk is partially mitigated. Information from certain CBP source systems may be amended as indicated in the applicable SORN. However, providing individual access and/or correction of eGIS records may be limited for law enforcement reasons, including as expressly permitted by the Privacy Act. Permitting access to the records contained in eGIS could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with

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

Section 8.0 Auditing and Accountability

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

eGIS has a robust set of access controls that restrict individuals' access to only the data they should have access to. Misuse of data accessed through eGIS is prevented or mitigated by maintaining audit trails of user role access provisions and by requiring that users: 1) conform to appropriate security and privacy policies, 2) follow established rules of behavior, and 3) are adequately trained regarding the security of the system.

Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity.

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

CBP process owners and all system users are required to complete annual security training including: 1) "CBP Sensitive Security Information," 2) "CBP IT Security Incident Response Training," and 3) "CBP IT Security Awareness and Rules of Behavior Training." Each annual security training addresses the appropriate use of PII. If an individual does complete training, that individual will lose access to all computer systems. All eGIS users must also complete the annual DHS privacy awareness training.

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

Access to non-sensitive data in the eGIS Map viewer and eGIS Portal is granted within DHS through the DHS-wide Trusted Identity Exchange (TIE).[42] Access to sensitive data is managed through eGIS administration of user roles by verification of a user's identity and organization using BPETS and Active Directory. eGIS administrators assign access or user roles based upon the particular user, organization, or geographic location, and the official need to know the information. In addition, administrators can recertify eGIS users annually, view audit logs containing user logins and logouts and all administrative actions and send routine and emergency messages to users.

[42] *See supra* note 11.

The default role for new eGIS Portal users is read-only. eGIS administrators can authorize users to upload content, including photograph files and document files, and share their content with members of groups within the portal. All eGIS users must complete the Privacy at DHS: Protecting Personal Information training class annually and are presented with the following disclaimer on the home page of the eGIS Portal website: "*The following SPII ALLOWED on this site. Material posted on eGIS Portal may be Sensitive But Unclassified, to include For Official Use Only, Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), or Sensitive Security Information. This environment WILL NOT house Classified, Secret, or Top-Secret Information. Content owners are responsible for ensuring appropriate access controls.*"

Users who require access to eGIS to perform their duties must first complete a full field background investigation. The requirement for gaining access to eGIS is documented.

Each sensitive layer in eGIS has individual access control so that access can either be granted or removed at the layer level. Once access to the eGIS application is granted, the system administrator controls additional access that allows users to view and/or edit data in those areas of the application that are required to perform their job.

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?

eGIS does not share information externally. However, should eGIS expand its user base to non-DHS users, the eGIS system and program owners will coordinate with the CBP Privacy Officer for review.

Contact Official

C. Taylor Ray
Director, Systems Division
U.S. Border Patrol
U.S. Customs and Border Protection

Responsible Official

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

Privacy.cbp@cbp.dhs.gov

Approval Signature

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

_____

Lynn Dupree
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Appendix A: Data ingested or used by eGIS

eGIS ingests information for the following types of information (note that fields marked as * require special access permissions):

Category/Group	Data Type	Source	Update Frequency
Activity	Apprehensions *	U.S. Immigration and Customs Enforcement (ICE) Enforcement Integrated Database (EID)	Approx. every 30 min.
	Apprehensions– UAC (USBP) *	EID	Approx. every 30 min.
	Apprehensions – OTM *	EID	Approx. every 30 min.
	Assaults *	E-STAR (previously known as Assaults and Use of Force Reporting System (AUFRS)	Approx. every 15-30 min.
	Border Safety Initiative *	Border Patrol Enforcement Tracking System (BPETS/BPETS2) and Border Safety Initiative Tracking System (BSITS) Module	Approx. every 15-30 min.
	Entries *	EID	Approx. every 30 min.
	G166 *	EID	Approx. every 30 min.
	High Risk Encounter Area (HREA)*	USBP Sector Intel Units	Biannually
	I44 – Appraised Values *	EID	Approx. every 30 min.
	Seizures *	EID	Approx. every 30 min.
	Significant Incident Reporting System (SIR) (USBP, OFO and AMO) ***	SIR	Approx. every 30 min.
	Use of Force *	BEPTS 2 Use of Force	Approx. every 30 min.
	Tracking, Sign-cutting, and Modeling (TSM) (Turn-backs, Got-aways and Checkpoints) *	TSM	Near real time
Blue Force Tracking	AMO Blue Force Tracking (BFT) * (All, Radar Only (Exclude MX), and Transponder Only (Exclude MX))	AMO	5 Seconds
	Team Awareness Kit (TAK)*	TAK	Near real time
	USBP Blue Force Tracking (BFT)	National Law Enforcement Communications Center (NLECC)	Near real time

Category/Group	Data Type	Source	Update Frequency
CBP Boundaries	AMO Air Branch Areas of Responsibility (AOR)	USBP-GIS	Weekly - Mondays
	OFO Field Office AOR	USBP-GIS	Weekly - Mondays
	Office of Information Technology (OIT) Regions	USBP-GIS	Weekly - Mondays
	OIT Tactical Communications (TACCOM) Regions	USBP-GIS	Weekly - Mondays
	USBP Corridors	USBP-GIS	Weekly - Mondays
	USBP Law Enforcement Operations Directorate (LEOD) Corridors	USBP-GIS	As Needed
	USBP Sector AOR	USBP-GIS	Weekly - Mondays
	USBP Station AOR	USBP-GIS	Weekly - Mondays
	USBP Zones	USBP-GIS	Weekly - Mondays
Charts	Nautical Charts	National Oceanic and Atmospheric Administration (NOAA)/ National Ocean. Service (NOS) /Office of Coast Survey (OCS)	Varies – As Needed
Detentions	UAC (USBP) *	e3 EID	Approx. every 30 min.
	All (USBP) *	e3 EID	Approx. every 30 min.
Facilities	CBP Real Property (Facilities Management & Engineering (FM&E))	FM&E	Daily
	Integrated Border Enforcement Teams (IBETs) Stations	USBP-GIS	As Needed
	AMO Facilities	USBP-GIS	As Needed
	OFO Container Security Initiative (CSI) Ports	USBP-GIS	As Needed
	OFO Facilities	USBP-GIS and OFO-GIS	As Needed
	OFO Field Offices	USBP-GIS	As Needed
	OFO Incident Action Plans (IAP) Operations	USBP-GIS	As Needed
	OFO Preclearance Operations	USBP-GIS	As Needed
	USBP Camps	USBP-GIS	As Needed
	USBP Checkpoints	USBP-GIS	As Needed
	USBP Fwd Op Base (FOB)	USBP-GIS	As Needed

Category/Group	Data Type	Source	Update Frequency
	USBP Headquarters	USBP-GIS	As Needed
	USBP Stations	USBP-GIS	As Needed
General Reference	Boundaries	Homeland Infrastructure Foundation-Level Data (HIFLD)	As Needed
	Communications	HIFLD	As Needed
	Emergency Services	HIFLD	As Needed
	Energy	HIFLD	As Needed
	Government	HIFLD	As Needed
	Infrastructure	HIFLD	As Needed
	Law Enforcement	HIFLD	As Needed
	Public Venues	HIFLD	As Needed
	Transportation	HIFLD	As Needed
ICAD Events	Alarm Events **	Intelligent Computer Aided Detection (ICAD)	Near Real Time
	Historical Alarm Events **	ICAD	Temporal: 3-8 hours, 9-16 hours, 17-24 hours
	Historical Ticket Events **	ICAD	Temporal: 3-8 hours, 9-16 hours, 17-24 hours
	Ticket Events **	ICAD	Near Real Time
ICE	Enforcement and Removal Operations (ERO) Detentions	U.S. Immigration and Customs Enforcement's (ICE)	Approx. every 30 min.
	Offices and Facilities	ICE	As needed
Live Traffic	Road	HERE.com through ESRI Service	Every 5 minutes
Manpower	Manpower **	BPETS	Hourly
Marine Vessel Traffic	Top Risk Vessels *	Automated Indicator Sharing (AIS) via Targeting and Analysis Systems Program Directorate (TASPD)	Hourly
	All Vessels *	AIS via TASPD	Hourly
	Earthquakes – Last 7 days	U.S. Geological Survey (USGS)	Daily
	Fires	USGS	Hourly
	Lightning	NOAA	Approx. every 5 min.
	Observed River Stages	NOAA	Hourly
	Radar	IBM/Weather	Approx. every 5 min.

Category/Group	Data Type	Source	Update Frequency
Natural Events	Radar (NOAA)	NOAA	Approx. every 5 min.
	Satellite	IBM/Weather	Approx. every 5 min.
	Satellite (NOAA)	NOAA	Approx. every 5 min.
	Storm Surge Potential	National Weather Service (NWS)	Approx. every 30 min.
	U.S. Tropical Storms	NOAA	Every 15 min.
	Watches and Warnings	NOAA	Hourly
	Wind Animation	NOAA	Every 1 hrs.
	World Tropical Storms	ESRI National Hurricane Center (NHC)	Every 15 min.
OIT Outages	Non-Intrusive Inspection (NII) *	Maximo	Daily
	Radiation Portal Monitor (RPM) *	Maximo	Daily
	Border Security Deployment Program (BSDP) *	Sentrillion	Daily
Seizures (OFO)	Cargo *	Seized Assets and Case Tracking System (SEACATS)	Daily (Approx. 0900-1000 EST)
Seizures (IPR)	The National Intellectual Property Rights Coordination Center (IPR Center) *	SEACATS	Daily
Technology	ICAD Repeaters **	USBP-GIS and USBP Sources	As Needed
	ICAD Sensors **	ICAD	Daily (Approx. 0830 EST)
	License Plate Reader (USBP LPR) *	ICAD	Daily (Approx. 0830 EST)
	USBP Program Management Office Directorate (PMOD) Managed Assets*	PMOD	Daily
	Remote Video Surveillance System (RVSS). Feeds *	Remedy	Approx. every 60 min.
	Unattended Ground Sensors (U-UGS) *	Big Pipe	Hourly
	U-UGS *	ICAD	Daily (Approx. 0830 EST)
UAC (Unaccompanied Alien Children)	Apprehensions – UAC (USBP) *	e3 EID	Approx. every 30 min.
	Border Monuments	Operation Waypoint	Weekly - Mondays
	Bridges	Operation Waypoint	Weekly - Mondays
	Buildings	Operation Waypoint	Weekly - Mondays

Category/Group	Data Type	Source	Update Frequency
USBP Reference	Cameras (Non-RVSS)	Operation Waypoint	Weekly - Mondays
	Crossings	Operation Waypoint	Weekly - Mondays
	Fencing Non-Tactical Infrastructure (Non-TI)	Operation Waypoint	Weekly - Mondays
	Firearms Ranges – USBP Use	Operation Waypoint	Weekly - Mondays
	Gates	Operation Waypoint	Weekly - Mondays
	Geological Features	Operation Waypoint	Weekly - Mondays
	Houses	Operation Waypoint	Weekly - Mondays
	Landmarks	Operation Waypoint	Weekly - Mondays
	Layups	Operation Waypoint	Weekly - Mondays
	Lighting (Non-TI)	Operation Waypoint	Weekly - Mondays
	Line Watches	Operation Waypoint	Weekly - Mondays
	Marine Features	Operation Waypoint	Weekly - Mondays
	Mile Markers	Operation Waypoint	Weekly - Mondays
	Other Facilities	Operation Waypoint	Weekly - Mondays
	Pick-up Locations	Operation Waypoint	Weekly - Mondays
	Rescue Beacons	Operation Waypoint	Weekly - Mondays
	Roads (Non-TI)	Operation Waypoint	Weekly - Mondays
	Scope Sites	Operation Waypoint	Weekly - Mondays
	Technology	Operation Waypoint	Weekly - Mondays
	Towers (Non-Camera)	Operation Waypoint	Weekly - Mondays
	Trails	Operation Waypoint	Weekly - Mondays
	Transportation Checks	Operation Waypoint	Weekly - Mondays
	Water-Related	Operation Waypoint	Weekly - Mondays
USBP Tactical Infrastructure (TI)	Additional Features (Points)	Operation Waypoint	As Needed
	Additional Features (Linear)	Operation Waypoint	As Needed
	All-Weather Roads	Operation Waypoint	Weekly - Mondays
	Border Lighting	Operation Waypoint	Weekly - Mondays
	Brush Clearing	Operation Waypoint	Weekly - Mondays
	Pedestrian Fencing	Operation Waypoint	Weekly - Mondays
	Pedestrian Fencing Exceptions	Operation Waypoint	As Needed
	Vehicle Fencing	Operation Waypoint	Weekly - Mondays
	Vehicle Fencing Exceptions	Operation Waypoint	As Needed

Appendix B: eGIS Portal Apps that Collect or Display PII

1. Landowner Parcel & Contact Information Portal

CBP uses eGIS to display publicly available landowner parcel and contact information in association with CBP's need to seek expedited real estate Rights of Entry (ROE),[43] Right of Way (ROW),[44] and subsequent acquisition of land for the placement of proposed and approved border surveillance technology and infrastructure, including but not limited to sensor towers,[45] relay towers, command and control station sites, and future border barrier construction. While CBP can access landowner parcel information through a variety of methods, there is no widely available central service for this information in a CBP system.

CBP ranch liaison officers engage with property owners and have on-site knowledge of the property. Ranch liaison officers also supplement their knowledge by accessing local publicly available resources, such as local county tax records. Another source of landowner parcel and contact information is publicly available data that is collected by a contracted vendor source and maintained by CBP's Office of Facilities Management & Engineering (FM&E); however, FM&E's subscription to landowner parcel and contact information is not readily available to U.S. Border Patrol (USBP). Ranch liaison officers do not have a central repository for collecting, generating, or retaining landowner parcel and contact information.

In most cases, the landowner parcel and contact information made available to the public by the local county tax records office is only available in hard copies and not in a format that is readily accessible to USBP. USBP now accesses publicly available landowner parcel and contact information made available to USBP from a contract vendor source. This information includes latitude/longitude coordinates and shape files[46] detailing the land parcel area. This landowner parcel and contact information will be supplied to USBP by a contract vendor source and delivered to USBP using a subscription-based service and an Application Programming Interface (API). The data will reside only with the contracted vendor source (in the same manner as eGIS displays real-time weather data from the National Oceanic and Atmospheric Administration). The contracted vendor source data is updated as new landowner parcel and contact information becomes publicly available.

---

[43] Right of Entry (ROE) refers to the legal right to enter upon real property of another for a special purpose without being guilty of trespass.

[44] Right of Way (ROW) is an easement, a privilege to pass over the land of another, whereby the holder of the easement acquires only a reasonable and usual enjoyment of the property, and the owner of the land retains the benefits and privileges of ownership consistent with the easement.

[45] For more information on sensor towers, *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE BORDER SURVEILLANCE SYSTEMS, DHS-CBP-PIA-022 (2014 and subsequent updates), *available at* https://www.dhs.gov/privacy.

[46] A shape file is a simple, non-topological format for storing the geometric location and attribute information of geographic features. Geographic features in a shape file can be represented by points, lines, or polygons (areas).

USBP intends to temporarily use and visually display in eGIS the landowner parcel and contact information, which will be provided on-demand from the contract vendor source. The landowner parcel and contact information will be displayed using eGIS Map Viewer in a special-access layer. The landowner parcel and contact information will be viewed during the user's session but retained in the original data source. No landowner parcel and contact information will be retained in eGIS once the user's session is closed.

In order to identify proposed Remote Video Surveillance System Upgrade (RVSS-U) sites, USBP conducts gap analysis to identify the need for and placement of RVSS-U sensor towers, relay towers, and Command and Control (C2) station sites. The coordinates for the proposed site of the RVSS-U are then entered into eGIS. Once the site has been identified and the location entered into eGIS, the eGIS user will access the associated landowner parcel and contact information and use the information to assist USBP in securing a ROE to the associated site parcel and a ROW to access the land parcel from the nearest public access road from the landowner.

USBP will use the landowner parcel and contact information, specifically the parcel locations and shapes, to display the data on a new eGIS parcel layer, accessible only to those with the appropriate access. eGIS users with the appropriate access, primarily USBP project managers and analysts, will be able to right-click on a land parcel to display parcel detail information, including landowner name and address. Specific landowner parcel and contact information will not be retained in eGIS during the ROE and ROW negotiations but may be retained in a work product kept by negotiating personnel. At the end of the ROE and ROW negotiations, only the coordinates of the RVSS-U site will remain in eGIS. Access to the parcel layer will be controlled by the eGIS admin tool and granted by eGIS administrators.

Site location decisions, land parcel information, owner identification, and real estate acquisition tracking is a major factor in the successful deployment of RVSS-U. Landowner parcel and contact information will enable earlier identification of preferred sites, expedite ROE for survey and evaluation, construction, and provide actionable information to CBP personnel.

Landowner, parcel, and contact information collected from the contracted vendor source will include latitude/longitude coordinates and shape files detailing the parcel area as well as the following information:

- Parcel ID – unique identifier for linking to point and polygon features (source: local authorities);
- State and county code – uses the Federal Information Processing Standard Publication 6-4 (FIPS 6-4), a five-digit code which uniquely identifies counties and county equivalents in the United States, certain U.S. possessions, and certain freely associated states (source: local authorities);

- APN and APN2 – assessor parcel number (and secondary) (source: local authorities)
- Parcel owner name (source: local authorities);
- Parcel owner address (source: local authorities);
- Parcel location, including city, state, a zip code (source: local authorities); and
- Standardized address, city, state, and zip code (source: U.S. Postal Service).

None of the data will be retained in any eGIS database and the new layer(s) will provide parcel data "on demand" from the contracted vendor source. The landowner parcel and contact information data will be available to select users via the eGIS Map viewer. eGIS users with the appropriate access will be able to right-click on a parcel to display parcel detail information, including owner name and address.

2. Missing Migrant Program Portal

The eGIS Portal application for the Missing Migrant Program (MPP) collects data pertaining exclusively to missing non-U.S. citizens and deceased individuals encountered along the U.S. border between the ports of entry. This data includes information from 911 calls from migrants in need of rescue or individuals searching for a missing migrant. Rescue and search scenarios typically start with an individual in distress (or a witness) calling 911. If the 911 caller identifies that the individuals in distress are located along the U.S. border and between the ports of entry, the 911 operator/dispatcher will automatically transfer the call to USBP who has the resources and familiarity with the terrain to execute the rescue. To assist USBP, the 911 operator/dispatcher will provide the USBP agents with the triangulation coordinates received from the cellular tower connected to the cell phone making the 911 call.

USBP agents assigned to the MMP review each missing person inquiry. During the review process, USBP will identify the type of request being submitted.

These request types include:

- Category 1 - missing person;
- Category 2 - need for immediate rescue (911 callers);
- Category 3 - recovery of deceased person; and
- Category 4 - forensic assistance/logistical support by USBP in the identification of deceased person.

USBP intends to collect GPS location data and the cell phone number from these 911 calls and display the information on eGIS maps.

USBP will use the MMP 911 call information to display the data on a new eGIS Portal layer, accessible only to those with authorized access to view the data. Users with the appropriate access will be able to right-click on a map icon and display the captured data, including the name of the missing person, latitude, longitude, cell phone number, potential medical need of the individual making the 911 call, and search status. This will allow information to be shared between coordinating rescue entities within USBP. All calls are displayed for 2 years by default, users can filter date ranges. Active calls are displayed with large bright bold symbols, inactive and closed calls display much smaller symbols.

USBP MMP program managers comprise the primary user base. Their access to this eGIS layer will be controlled by the eGIS Admin Tool, granted by eGIS administrators.

MMP data intended to be retained in the eGIS database and displayed in a new layer will include latitude/longitude coordinates[47] as well as the following information pertaining to the individual placing the 911 call:

- Name of missing migrant;
- Cell phone number of individuals placing the 911 call (provided by caller);
- Potential medical need;
- Cellular phone battery level (optional and provided by caller). This information is obtained by asking the individual. Either the 911 call center or Rio Grande Valley Operational Center personnel has asked the individual or has obtained the information from a concerned entity/family member etc. If provided, cell phone battery information is used to assist in real time rescue efforts;
- Ambulatory status of the individual making the 911 call;
- Number of subjects in need of assistance;
- Group description;
- Search status;
- Originating agency;
- USBP Sector;
- USBP Station;
- Phase of coordinates;

[47] Coordinates are received from the 911 call centers or from identified landmarks. CBP currently has more than 22,000 landmarks in eGIS.

- MMP location Matrix ID;
- Tracking Sign-cutting Module (TSM) event number;
- Incident comments;
- Date closed; and
- Number of individuals rescued.

3. 911 Emergency Management Portal (9EMP)

Beginning fiscal year 2019 , CBP began purchasing and deploying 170 self-powered 911 cellular relay rescue beacons along the southern border of the United States and between ports of entry. When calling 911, if the caller identifies individuals in distress are located along the U.S. border and between the ports of entry, the 911 operator/dispatcher will automatically transfer the call to USBP who has the resources and familiarity with the terrain to execute the rescue. When a 911 call is placed from the individual's person cell phone, the 911 operator/dispatcher will provide USBP agents with the triangulation coordinates received from the cellular tower connected to the cell phone making the 911 call. Intelligent Computer Assisted Detection (ICAD) will provide location data for 911 call placed from rescue beacons.

Data from the 911 call is retained in the eGIS – 9EMP and displayed on a map. This data is primarily used by the Missing Migrant Program (MMP) to help locate individuals who have been reported missing. In addition, the data associated with these calls is analyzed to assist USBP in determining the placement of current and future rescue beacons and/or 911 placards.

If a caller uses a CBP rescue beacon to place a 911 call, the GPS location of the rescue beacon and sensor data (including images) is recorded in ICAD and the location data is displayed on the eGIS – 9EMP map. In contrast, if a caller uses a cellphone to place the 911 call, the location information may be provided by the 911-call center or USBP will use landmark information identified by the caller to pinpoint the GPS location of the caller. The map will display the GPS location and the cell phone number of the caller. For tracking purposes, information collected during the 911 call is manually entered in eGIS 9EMP, as well in a MMP database.

USBP will use the eGIS 9EMP call information to display the data on a new eGIS map layer, accessible only to those with authorized access to view the data. Users with the appropriate access will be able to right-click on a map icon and display 911 call related data. Displaying 911 information on a map allows it to be shared between coordinating rescue entities within USBP. All 911 calls are displayed for 2 years by default and users can filter by date range. Active calls are displayed with large bright bold symbols, while inactive and closed calls are displayed with much smaller symbols.

USBP MMP program managers comprise the primary user base. Their access to this eGIS

– 9EMP is controlled by the eGIS Admin Tool, granted by eGIS administrators. The following information concerning the 911 caller is collected and retained in the eGIS 9EMP and displayed in a new map layer:

- Name of missing migrant;
- Cell phone number of the 911 caller;
- Potential medical need;
- Cellular phone battery level obtained by asking the caller or concerned entity including family members). This information is helpful in real time rescue efforts.
- Ambulatory status of the individual making the 911 call;
- Number of subjects in need of assistance;
- Group description;
- Search status;
- Originating agency;
- USBP sector;
- USBP station;
- Latitude and longitude coordinates from 911 call centers; identified landmarks when the 911 emergency call is not placed from a rescue beacon; or from a CBP deployed rescue beacon;
- MMP Location Matrix ID;
- Tracking Sign-cutting Module Event number;
- Incident comments;
- Date closed; and
- Number of individuals rescued.

The following information is captured in ICAD and displayed on the map layer:

- Date;
- Time;
- Location;
- Sensor ID;
- TSM / Alarm ID; and

- Agent name / star number.

4. Northern Border (NB) Vessel Encounter

The eGIS – NB Vessel Encounter application is configured within the current design of the eGIS Portal system that collects and displays information on passengers on suspicious vessels operating along the Great Lakes region.

In response to observed and suspected illicit cross border activity, USBP agents operating in the lakes, rivers, and tributaries of the Great Lakes respond to suspicious maritime cross-border traffic of vessels. Agents may conduct vessel encounters and further investigate a suspicious vessel based on the responding agents' level of suspicion or probable cause. USBP agents conduct record checks themselves or with the help of Detroit Sector Law Enforcement Information Systems Specialists (LEISS). These record checks allow the agent to confirm the validity of the documentation presented such as Nexus cards, permanent resident documentation, or government issued identification. Using a CBP owned and issued hand-held tablet or laptop, the agent will manually log information into the eGIS – Northern Border (NB) Vessel Encounter application. The USBP Detroit Sector Special Investigations Unit uses the information collected to perform further analysis on the suspicious cross border activity to inform operations in the Detroit Sector Aera of Responsibility. Access to the NB Vessel Encounter eGIS Portal app is restricted to USBP Detroit Sector Special Investigations Unit personnel with an operational "need to know."

The eGIS NB Vessel Encounter Portal will collect and display the following data:

- USBP agent last name/first name;
- Vessel;
- Vessel registration number;
- Vessel registered state;
- Operator name
- Operator date of birth;
- Operator citizenship;
- Operator country of birth;
- Operator passport number;
- Operator driver's license/state identification number;
- Operator identification number - other government-issued identification;
- Passenger name;
- Passenger date of birth;

- Passenger citizenship;
- Passenger country of birth;
- Passenger passport number;
- Passenger driver's license/state identification number;
- Passenger identification number - other government-issued identification;
- Photo of vessel; and
- CBP email address.

5. Stash[48] House Enforcement Portal (SHEP)

The USBP Rio Grande Valley Sector will use the SHEP Portal to collect limited PII, regarding the location of the known stash house, as well as the e3 or Tracking & Sign-Cutting (TSM) event linked to that known address. Any PII associated with the e3 event will be maintain in e3. The address/location information is collected for display purposes only. Access to SHEP will be restricted to USBP management and the Rio Grande Valley Sector Intelligence Unit personnel with a need-to-know.

The eGIS SHEP Portal will collect and display the following data:

- Type of enforcement activity (stash houses);
- Operational status of enforcement activity;
- Date of initial intelligence;
- Source of initial intelligence;
- Station Area of Responsibility in which initial intelligence was obtained;
- Entity that provided the initial intelligence;
- Station Area of Responsibility in which stash house is located;
- Zone in which stash house is located;
- e3 event number associated with enforcement activities;
- TSM event number associated with enforcement activities;
- Street address of stash house;
- City of stash house;
- Description of address if multi-plex or multi-address property;
- Synopsis of intelligence relating to stash house;

[48] A stash house is a home or building used to smuggle people or drugs.

- Deconfliction number;
- Deconfliction date;
- Total number of principals apprehended;
- Total number of migrants apprehended;
- Total weight of marijuana seized;
- Total weight of cocaine seized;
- Total weight of heroin seized; and
- Total weight of methamphetamine seized.