



Privacy Impact Assessment
for the

Enterprise Geospatial Information Services (eGIS)

DHS/CBP/PIA-041

May 2, 2017

Contact Point

Antonio J. Trindade

Strategic Planning and Analysis Directorate

U.S. Customs and Border Protection

(202) 344-1446

Reviewing Official

Jonathan R. Cantor

Acting Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) 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, 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 conducting this Privacy Impact Assessment (PIA) to assess the privacy risks of this information technology system and to notify the public of the collection, storage, retention, use, and dissemination of information within eGIS belonging to members of the public.

Overview

The U.S. Customs and Border Protection (CBP), specifically the U.S. Border Patrol (USBP or Border Patrol), plays a critical role in securing the Nation's borders between Ports of Entry (POE) against all threats. USBP 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, USBP objectives include:

- Preventing terrorists and terrorist weapons from entering the United States 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 USBP.

The Enterprise Geospatial Information Services (eGIS) application enables USBP agents in meeting the overarching strategic goals to secure the border. Agents use eGIS to conduct patrol, surveillance, and interdiction functions, and to conduct enforcement and apprehension processing,



adjudication, and resolution. eGIS increases CBP geospatial data availability to improve real-time decision making that is necessary for the protection of personnel and key resources.

eGIS is a national, web-based application designed to display data from multiple data sources spatially (i.e., on a browser-based map). Initially designed to support USBP requirements, eGIS provides services to well over 20,000 USBP agents and analysts and staff members to support all CBP components. eGIS facilitates the integration of multiple CBP enforcement systems to expose previously-unrecognized spatial patterns and trends. eGIS provides numerous mission-critical role-based features including real-time intrusion sensor alerts; arrest and interdiction locations; assault and significant incident tracking; facility and infrastructure data; field information reports; and recidivist arrest analysis.

Presenting data on a map assists USBP, Joint Task Force - West (JTF-W),¹ and Office of Field Operations (OFO) Agents/Officers in identifying trends in border incidents 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 all CBP personnel 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 of the eGIS features include:

- Browser-based application available to all Border Patrol agents;
- 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 Border Patrol enforcement operations);
- Search for ENFORCE events,² and select a point on a map to store apprehension coordinates; and
- Display events from the ENFORCE application.

eGIS consists of two applications: the eGIS Portal, which extracts data from other source systems, and the eGIS Map Viewer (eMap), which displays the data on maps. These visual aids

¹ Joint Task Force - West (JTF-W) is part of a DHS effort to coordinate and optimize DHS component authorities in a partnership to combat prioritized threats to the homeland with a specific focus on Transnational Criminal Organizations. The JTF-W structure focuses cross-department operations on strategic objectives across four geographical corridors: JTF-W California Corridor, JTF-W Arizona Corridor, JTF-W New Mexico/West Texas Corridor, and JTF-W South Texas Corridor, while simultaneously strengthening existing structures within each area.

² 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 DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT (July 25, 2012), available at <https://www.dhs.gov/privacy>.



use geographic coordinates to monitor border vulnerabilities, corrective actions, border incidents, and relevant events such as arrests and seizures that contain geographic data.

eGIS Portal

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; share links to GIS applications; and share map and layer packages for users' individual desktops. The eGIS Portal includes the following modules:

1. eGIS Map Viewer - An application for designing and saving web maps. Users can create, save, and share maps with other users.
2. Web AppBuilder - Permits users to design and build web applications from web maps. Web AppBuilder allows users to build applications without writing code. Web AppBuilder comes with a variety of themes that can be customized and widgets that allow for delivery of advanced functionality such as high-quality printing, geoprocessing, editing, and search.
3. 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.
4. ArcGIS applications - The eGIS Portal also supports geospatial applications that allow people to interact with web maps.

eGIS Map Viewer³

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 (Border Patrol Agents and OFO Officers) with additional privileges are able to view the locations of illicit activity 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:

³ The eGIS Map Viewer can be accessed through the eGIS Portal or on its own.



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

Types of Information Displayed by eGIS

eGIS provides authorized users with the ability 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 to identify 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 This data does not contain PII elements.
4. Officer Safety Data - location of an assault and any weapons used by subjects on a CBP Officer or Agent. This data does not contain PII elements.

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.

⁶ A viewshed is the geographical area that is visible from a location. It includes all surrounding points that are in line-of-sight with that location and excludes points that are beyond the horizon or obstructed by terrain and other features (e.g., buildings, trees).

⁷ A PIA for IRS is forthcoming.



5. Human Resources Data - work and residence location of CBP personnel.⁸
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 ingest or extract information from source systems. Rather, eGIS displays information from the CBP Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW).⁹ 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:

1. Identify: Users can click on a feature in the map to view attributes of that feature (may also be accessed by right-clicking on the feature in the map).
2. Query: Users can structure queries to return information on a specific data layer by user-defined location, timeframe, or specific attribute (e.g., how many seizures included firearms last year).
3. 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.
4. Recidivist: Users can query subjects by the number of recidivist counts and display them through the eGIS interface.¹⁰

Access to non-sensitive data¹¹ in the eGIS Map Viewer and eGIS Portal is granted within DHS through the DHS-wide Trusted Identity Exchange (TIE).¹² Access to sensitive data is

⁸ This information is only available to the individual user and select Incident Management individuals.

⁹ See DHS/CBP/PIA-034 Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW) (September 7, 2016), available at <https://www.dhs.gov/privacy>.

¹⁰ 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.

¹¹ 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.

¹² See DHS/ALL/PIA-050 DHS Trusted Identity Exchange (April 2, 2015), available at



managed through eGIS administration of user roles by verification of a user's identity and organization using the Border Patrol Enforcement Tracking System (BPETS)¹³ 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 recertify eGIS users annually, view audit logs containing user log-ins and log-outs and all administrative actions, and send routine and emergency messages to users.

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. eGIS is authorized to collect and maintain records pursuant to the following authorities granted to the source systems:

- 5 U.S.C. § 301;
- 6 U.S.C. § 202;
- The Immigration and Nationality Act ("INA"), 8 U.S.C. § 1101, et seq., including 8 U.S.C. §§ 1103, 1185, 1225, 1324, 1357, 1365a, 1365b, 1379, and 1732;
- 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582, and 2075(b)(2)(B)(3);
- 49 U.S.C. § 44909;
- Enhanced Border Security and Visa Reform Act of 2002 (Pub. L. 107-173);
- Homeland Security Act of 2002 (Pub. L. 107-296);
- 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);
- Justice for All Act of 2004 (Pub. L. 108-405);
- 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); and

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

¹³ BPETS is a web-based application that allows USBP to analyze incident data and manage the deployment of its personnel and resources. A PIA for BPETS is forthcoming.



- 8 CFR 287.

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 not searchable by unique identifier such as name, Alien File Number (A-Number), or other biographic information from subject records. However, based on location, eGIS users can display Privacy Act-covered subject records. 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),¹⁴ 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 taken at official POEs and are covered under DHS/CBP-010 TECS.¹⁵
- Records related to seizures are maintained in accordance with DHS/CBP-013 Seized Asset and Case Tracking System (SEACATS).¹⁶
- 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).¹⁷

Surveillance Data Feeds (Blue Force Tracking,¹⁸ marine vessel tracking, sensors, and surveillance):

- DHS/CBP-023 Border Patrol Enforcement Records (BPER).
- DHS/CBP-019 Air and Marine Operations Surveillance System (AMOSS)¹⁹ which contains surveillance event and operations data. AMOSS supports domestic operations

¹⁴ DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).

¹⁵ DHS/CBP-011 TECS, 73 FR 77778 (December 19, 2008).

¹⁶ DHS/CBP-013 Seized Asset and Case Tracking System (SEACATS), 73 FR 77764 (December 19, 2008).

¹⁷ DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016).

¹⁸ Blue Force Tracking is a term for a GPS-enabled system that provides location information about other law enforcement vehicles and aircraft.

¹⁹ DHS/CBP-019 Air and Marine Operations Surveillance System (AMOSS), 78 FR 57402 (September 18, 2013). 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 in monitoring approaches to the U.S. border to detect illicit trafficking and direct interdiction actions, as appropriate.



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 services and is therefore not covered by a Privacy Act system of records.²⁰

Intelligence Data: eGIS does not display finished intelligence information, but displays the location and type of reports logged in the Intelligence Reporting System (IRS). This data does not contain PII elements.²¹

Officer Safety Data (use of force and assaults):

- DHS/ALL-020 Department of Homeland Security Internal Affairs,²² which covers records related to internal investigations. Use of force incidents may also be 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)²³ covers records related to the provision of access to information technology resources.
- DHS/ALL-014 Department of Homeland Security Emergency Personnel Location Records System²⁴ covers work and residence location of CBP personnel.

²⁰ 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>.

²¹ Intelligence records are covered by the forthcoming DHS/CBP-024 Intelligence Records System (CIRS), which covers intelligence products containing raw intelligence, public source information, and information collected by CBP pursuant to immigration and customs authorities.

²² DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014).

²³ DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).

²⁴ See DHS/ALL-014 Department of Homeland Security Emergency Personnel Location Records, 73 FR 61888 (October 17, 2008).



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 is currently finalizing the re-certification of its Authority to Operate prior to its expiration on May 8, 2017.

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.

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 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 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.²⁵ Enforcement information from E3

²⁵ For more information about the E3 portal, please *see* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT (July 25, 2012), available at <https://www.dhs.gov/privacy>.



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.

Surveillance Data Feeds

- Static and video images from surveillance assets.

Intelligence Records

- Displays the location and type of reports logged in the Intelligence Reporting System (IRS). This data does not contain PII.

Officer Safety Records

- 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,²⁶ 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

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

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 surveillance systems in rural and populated areas at or near the U.S. border.²⁷ PII within eGIS is either related to CBP personnel or subject records from enforcement actions.

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	Air and Marine (AMO) Points	Treasury Enforcement Communication System (TECS) and Case Management Air and Marine Targets (CMAR)	Approx. every 15-30 min.
	Air Marine Tracks	TECS and CMAR	Approx. every 15-30 min.
	Apprehensions*	Enforcement Integrated Database (EID)	Approx. every 30 min.

²⁶ Emergency contact information is not retrieved by unique identifier, and therefore no SORN coverage is required.

²⁷ For a detailed description of all CBP Border Surveillance Systems, and the privacy risks associated with them, please see DHS/CBP/PIA-022 Border Surveillance Systems (August 29, 2014), available at <https://www.dhs.gov/privacy>.



	Apprehensions - UAC (Unaccompanied Children) (USBP)*	EID	Approx. every 30 min.
	Apprehensions – OTM (Other Than Mexican)*	EID	Approx. every 30 min.
	Assaults	Assaults and Use of Force Reporting System (AUFRS)	Approx. every 15-30 min.
	Border Safety Initiative*	Border Patrol Enforcement Tracking System (BPETS) and BSI Tracking System (BSITS)	Approx. every 15-30 min.
	Entries	EID	Approx. every 30 min.
	G166* (Investigative Reports)	EID	Approx. every 30 min.
	High Risk Encounter Area* (HREA)	USBP Sector Intel Units	As Needed
	I44 - Appraised Values* (Report of Apprehension or Seizure)	EID	Approx. every 30 min.
	Intelligence*	Intelligence Reporting System (IRS) Manager Service	Approx. every 30 min.
	Seizures*	EID	Approx. every 30 min.
	Significant Incident Reports (SIR) (USBP, OFO and AMO)*	SIR	Approx. every 30 min.
	Use of Force*	BPETS 2 Use of Force	Approx. every 15-30 min.
	TSM* (Turn-backs and Got-aways)	TSM (Tracking, Sign-Cutting and Modeling) Application	Continuous
	AMO BFT*	AMO	5 Seconds



Blue Force Tracking (BFT)	USBP BFT - Trial	Infrastructure Maintenance Support (OTAR)	Streaming
CBP Boundaries	AMO and USBP AOR (no PII)	United States Border Patrol Geospatial Information Systems (USBP-GIS)	Weekly - Mondays
Charts	Federal Aviation Administration (FAA) Sectional Charts (no PII)	FAA	Varies - As Needed
Facilities	CBP Real Property Locations (no PII)	FM&E (Facilities Management & Engineering) Division	As Needed
General References	Publicly available location information such as boundaries, infrastructure, law enforcement, and transportation (no PII)	HSIP (Homeland Security Infrastructure Program)	Annually
Intelligent Computer Assisted Detection (ICAD)	Alarm Events*	ICAD	
	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	Streaming
ICE	ERO Detentions	ICE	Approx. every 30 min.
	Offices and Facilities	ICE	As needed
Live Traffic	Traffic Alerts (no PII)	HERE.com through ESRI (Environmental Systems Research Institute) Service	Every 5 minutes
Manpower	Manpower*	BPETS	Hourly
Marine Vessel Traffic Feed	Top Risk Vessels*	TASPD (Targeting and Analysis Systems Program Directorate)	Streaming



	All Vessels*	TASPD	Streaming
Natural Events	Radar View	Wunderground	Streaming
	Satellite View	Wunderground	Streaming
	Tropical Storms (ESRI)	National Oceanic and Atmospheric Administration (NOAA)	Varies
	US Weather Radar (NOAA)	NOAA	Streaming
	Floods, Quakes Fires (USGS)	USGS (United States Geological Survey)	Streaming
	Watches and Warnings (NOAA)	NOAA	Streaming
Office of Information Technology (OIT) Outages	Non-Intrusive Inspection (NII)	Maximo	Daily
	Radiation Portal Monitors (RPM)	Maximo	Daily
	Border Security Dev. Pgm (BSDP)	Sentrillion	Daily
Seizures (OFO)	Cargo	Seized Asset and Case Tracking System (SEACATS)	Daily
Seizures (IPR)	IPR (Intellectual Property Rights)	SEACATS	Daily
Tactical Communications (TACCOM)	Communications base stations, receivers, repeaters and other devices (no PII)	Multiple CBP (OIT, USBP, AMO), ICE	Infrequent
Targeting Framework	Shift Logs	TASPD	Approx. every 30 min.
Technology	Aerostats*	USBP-GIS and USBP Sources	As needed
	ICAD Repeater*	ICAD	Daily (Approx. 0830 EST)
	ICAD Sensors*	ICAD	Daily (Approx. 0830 EST)



	Integrated Fixed Towers (IFT) Sites (Planned)*		
	License Plate Readers - LPR (USBP)*	Passenger Systems Program Directorate (PSPD) ²⁸	Streaming
	MSS* (Mobile Scope Surveillance)	Tucson Sector MSS Website	Approx. every 60 min.
	RVSS* (Remote Video Surveillance System)	Remedy	Approx. every 60 min.
	RVSS Feeds*	Big Pipe	Streaming
	U-UGS* (Unattended Ground Sensors)	ICAD	Daily
UAC	Apprehensions - UAC (USBP)*	e3 EID	Approx. every 30 min.
	Detention Facilities: Detentions - UAC (USBP)	e3 EID	Approx. every 30 min.
USBP Reference	Geographic references used by Border Patrol Agents	Sectors/Stations Op. Waypoint - Trimble GPS	Weekly
USBP Tactical Infrastructure (TI)	Geographic references used by Border Patrol Agents	Sectors/Stations Op. Waypoint - Trimble GPS	Weekly

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

²⁸ CBP collects license plate information during vehicle crossings at primary inspection. License plate numbers (as read and forwarded by the license plate reader system or manually entered by the CBP Officer) for all vehicles entering and leaving the United States are queries against TECS and then transferred to EMIS-EDW. eGIS reads the LPR data from EMIS-EDW. For a detailed description of primary and secondary processing, please *see* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (December 22, 2010), *available at* <https://www.dhs.gov/privacy>.



tropical storm data feeds that are 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 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 elevation, base maps, and more to support situational awareness.

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.²⁹
- Detailed 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 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

²⁹ 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 verifying that eGIS is displaying the correct AOR.



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 approved purpose. Specifically, CBP copies and retains information only when it is 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.³⁰

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 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, Air and Marine, and Joint Task Force-West 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 (see chart above). EMIS-EDW relies upon the source systems to ensure that data used by eGIS is accurate and complete. Discrepancies may be identified in 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

³⁰ For a detailed description of all CBP Border Surveillance Systems, and the privacy risks associated with them, please see DHS/CBP/PIA-022 Border Surveillance Systems (August 29, 2014), available at <https://www.dhs.gov/privacy>.



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 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 USBP, JTF-W, and OFO officers 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 Home Page 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. 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,³¹ 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

³¹ User defined. Typical boundaries include a city, street, sector, etc.



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,³² and content from the web.

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 United States Coast Guard 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 Personnel layer through strict access and role management controls.

³² Multiple file types can be uploaded from a user’s workstation. If formatted properly, authorized users can upload PII from their workstation.



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, 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 where providing notice would compromise the operation. 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.

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.

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 or follow the procedures in Section 7 of this PIA.

Privacy Risk: There is the risk that individuals may not be aware that their data is stored in eGIS.

Mitigation: This risk is partially mitigated for eGIS users, who understand that their personal and employment information is required to gain access to eGIS. This risk is not mitigated for other individuals whose information is entered into eGIS. These individuals may or may not have been provided general notice at the time of collection about the retention of their information in CBP systems, depending on the circumstances and the source system. For individuals who were provided notice at the time of collection, they may not be aware that their information now resides in eGIS. Notice may not be provided at the time of collection to individuals whose data is collected as part of an incident because of the law enforcement nature of the encounter.

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

Because eGIS does not ingest, store, or extract any source system information, there is no risk to record retention.

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 CBP 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 does not actively collect the information in those respective databases. When an individual is seeking redress for other information analyzed in eGIS, he or she must locate the databases 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.

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



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

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

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

If individuals are uncertain what agency or database manages the information, they may seek redress through the DHS Traveler Redress Program ("TRIP"), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

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 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.



Privacy Risk: With the recent cancellation of the DHS Mixed Systems policy³³ through DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*,³⁴ there is a risk that non-U.S. Citizens and non-Lawful Permanent Residents are now unable to access, correct, and amend their information as they were previously able to do.

Mitigation: This risk is partially mitigated. This PIA and source system SORNs describe how individuals can make access requests under FOIA or the Privacy Act. Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. However, these individuals still may seek notification of and/or access to records pursuant to procedures provided by FOIA. Additionally, to ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

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 to which they should have access. 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," 3) "CBP Safeguarding Classified National Security Information," and 4) "CBP IT Security Awareness and Rules of Behavior Training." Each security training addresses the

³³ For more information, please see Privacy Policy Guidance Memorandum 2007-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, available at <https://www.dhs.gov/privacy>.

³⁴ For more information about the recent cancellation of the DHS Mixed Systems policy, please see the DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*, available at <https://www.dhs.gov/privacy>.



appropriate use of PII. If an individual does not take 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).³⁵ 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 log-ins and log-outs and all administrative actions, and send routine and emergency messages to users.

The default role for new eGIS Portal users is a read-only role. 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.

³⁵ DHS/ALL/PIA-050 DHS Trusted Identity Exchange (TIE), (April 2, 2015), available at <https://www.dhs.gov/privacy>.



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.

Responsible Officials

Antonio J. Trindade
Strategic Planning and Analysis Directorate
U.S. Customs and Border Protection

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

Approval Signature

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

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