Privacy Impact Assessment
for the

Geospatial Information Infrastructure (GII)

DHS/ALL/PIA-078

November 22, 2019

Contact Point
Lewis Summers
Geospatial Information Infrastructure Program Manager
Geospatial Management Office (GMO)
Information Sharing and Services Office (IS2O)
Office of the Chief Information Officer (OCIO)
Department of Homeland Security
(202) 603-6304

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

Abstract

The Department of Homeland Security (DHS) Geospatial Information Infrastructure (GII) is a major application infrastructure, maintained by the Geospatial Management Office (GMO), representing the physical and logical implementation of the Department's Geospatial Services Segment Architecture (GSSA). The purpose of the GII is to deliver a geospatial technology platform composed of geospatial enterprise applications, tools, and information to facilitate secure information-sharing between federal, state, local, tribal, territorial, private sector, international, and other non-governmental partners who support the homeland security mission. DHS is conducting this Privacy Impact Assessment (PIA) because the information viewed and shared in the GII may contain personally identifiable information (PII) on DHS personnel and members of the public.

Overview

The Department of Homeland Security (DHS) Geospatial Management Office (GMO) was created by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004[1] and established formally within the Office of the Chief Information Officer. The GMO leads the Department-wide development of the Geospatial Services Segment Architecture (GSSA) to steward geospatial governance and provide oversight into geospatial investments. The Geospatial Information Infrastructure (GII) information system was developed as the solution for the procurement of technical assets to support the Department's GSSA.[2] The GII also enables the GMO to support the long-term requirement of handling personally identifiable information (PII) contained in geospatial data provided within DHS, for other federal agencies, and through partnerships with state, local, tribal, territorial, and private organizations.

The GII is a body of enterprise data, application services, and infrastructure governed by the GSSA following DHS Enterprise Architecture principles to meet common geospatial requirements across the broad DHS mission space. The GII allows homeland security enterprise users to securely share geospatial information on critical infrastructure, natural hazards data, aerial imagery, and other user-defined geospatial data; as well as perform spatial analyses such as querying (searching and filtering by location), geocoding (translating street addresses to locations on a map), and proximity functions (creating buffers, finding nearest locations to a point of interest, planning routes). The GII acts as a service and platform provider and does not create or own the

[1] Pub. L. 108-458, available at https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf.
[2] The Department's geospatial investment requirements are outlined by DHS Management Directive for Information Technology & Management (MD 0007.1), *available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0007_1_information_technology_integration_and_management.pdf.

data managed and shared within. All data remains under the ownership of the users that provide it (i.e., Individual GII Users or GII Data Provider). The GII provides the following capabilities:

- Secure access to enterprise geospatial information (i.e., imagery, base maps);
- Mapping and visualization services;
- Geospatial tools and analytic services;
- Web application templates; and
- Training materials and tradecraft.

Future versions of the GII (e.g., hosted in a cloud environment) will provide a public/private cloud infrastructure and integration framework to supply standards-based geo visualization services, geoanalytics, common geospatial operating data, and geospatial content delivery services.

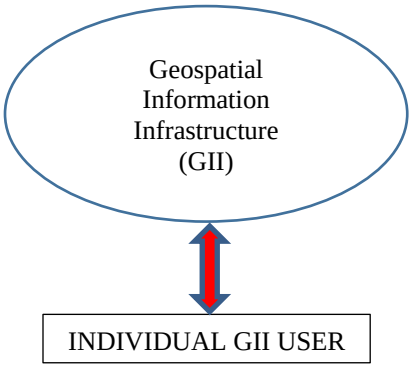
The GII leverages the Homeland Security Information Network (HSIN) Identity Management solution[3] to provision user access to its applications, data, and web services. There are three types of user/mission partner data relationships with GII:

1. An Individual GII User, that logs in to the GII;
2. A GII Data Provider (i.e., data owner), that owns and manages homeland security mission data and desires to provide it within the GII information system; and has a GII System Owner-approved memorandum of understanding or agreement (MOU/A) or interconnection security agreement (ISA) to share data within the GII. The data owner determines accessibility restrictions and data element types, and is responsible for the accuracy of the data provided to the GII;
3. A GII Data Consumer, that is an organization with an application or service that desires to use or consume GII data; and has an approved MOU/A or ISA with GMO to receive GII data.

[3] For more information about the HSIN Identity Management solution, please *see* DHS/ALL/PIA-061-1 HSIN Release 3 User Accounts: HSIN Enterprise Reporting Solution, *available at* https://www.dhs.gov/privacy. This GII PIA focuses on the information associated with the mission of GII and not the identity management portion of the GII. The HSIN Release 3 User Accounts PIA discuss the privacy risks and mitigations associated with HSIN's Identity Management solution being leveraged by the GII.

Individual GII User

Individual GII users, both from within DHS and external to DHS, are required to obtain HSIN authentication credentials to access the GII information system. The individual GII user has access to numerous geospatial capabilities to include web-based map viewing, map services for web and desktop use, and analytic services. Since the GII also supports the storage of a number of data files (e.g., Excel, Word, PDF, .txt) and mapping files (e.g., gpx, ArcGIS Server Web Service, Web Mapping Service (WMS)), individual GII users, as the owner of their data, can also upload content or access their GII content via applications; provision other approved users to download that data; and can create geospatial features and add features from text files, GPS files, and other files and develop data layers in support of their mission. All individual GII user content is private by default until it is shared by that user. Individual user content can be tagged with terms defined by the individual data owner. These tags can be used to help organize similar content items and provide a way to quickly search for related items.



- Requires HSIN Authentication

The GII is a geospatial information sharing platform made up of users (i.e., Individual GII User), groups, and content. A group is formed within the GII to facilitate the collaboration and the sharing of content managed by an individual GII user or GII Data Provider. Each group is maintained by a group owner (a lead point of contact) that has the authority to invite and remove GII users to and from the group. The group owner must obtain HSIN account credentials with which to access GII as an individual GII user and to request a group of GII users be created to share content.

Users have the ability to create, manage, and share their content with GII groups within which they are members. Every item (e.g., layer file, pdf, shapefile, map package) in the GII has a data Content Details page which consists of various metadata elements (e.g., title, description, owner providing the item to GII, terms of use for the item content, and credit attributed to the item's source). The user always retains control of the content; however, other users can view the content if they are members of the group with which the original user shared the content.

The ability to create a group in the GII is limited to GII administrators within the GMO. When GII administrators receive a request for a new group, they evaluate the validity of the request by collecting the below information. Additionally, the GMO team works with the DHS Privacy Office to ensure compliance with all applicable privacy regulations and policy (e.g., completing a Privacy Threshold Analysis (PTA)).

- Group Name
- High Level Requirement or General Purpose
- Requested Completion Date
- Mission Needs Statement
- Estimated Number of Users for this group
- Will the geospatial data in the group require special archiving?
- Will the geospatial data in the group contain PII or Sensitive PII?
    - If PII or SPII, please list data elements
- Stakeholders
- Customer Point of Contact Information
- Group/Site Owner Information

Mission partners, through their individual GII accounts, can select who will have permission to access the files and maps created within that mission partner's GII account. If the mission partner adds a data layer or content is created and saved to a map in the GII, the mission partner is able share it with:

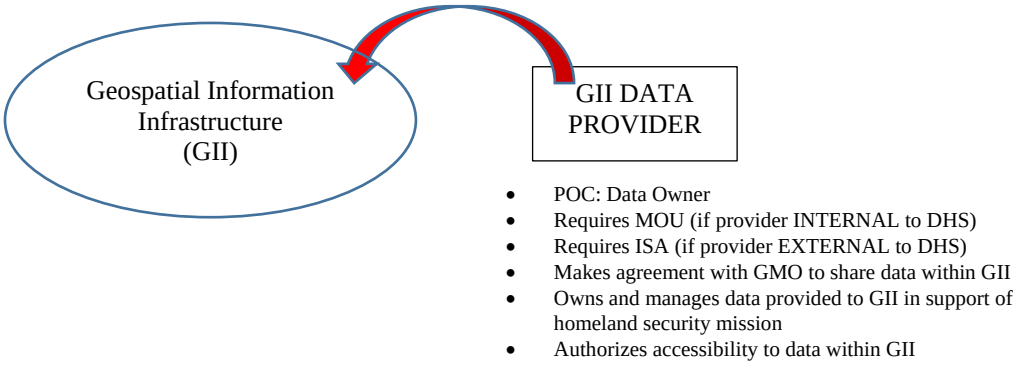
Everyone — Sharing with everyone makes an item public to the entire GII users directory; anyone who has access to the GII can find and use it, and group owners can include it in their group content;

Groups — Members assigned to a group, can share items with that group. Sharing with specific groups restricts access to a smaller, more focused set of users; or

Groups and everyone — An item can be shared with a larger audience (i.e., all GII users) and, also, with a specific group. This allows for shared data to be categorized with items that may be especially relevant to a group while still making it available to others in the organization.

GII Data Provider

A GII Data Provider (or Data Owner) can be both from within DHS and external to DHS.[4] Data owners do not require HSIN authentication. This relationship pertains to applications or systems external to the GII that wish to provide data to the GII without logging in as an individual user, usually due to technical limitations. Through an information sharing agreement (i.e., MOU/A, ISA), the GII Data Provider agrees with GMO to govern the sharing of the Data Provider's data, including designated managerial and technical staff, in the absence of a common management authority. Both parties agree to allow system interoperability using hypertext transfer protocol secure (HTTPS) via the public internet. In the event a direct connection is required, an ISA must be executed between the GII Data Provider and the GMO. GII Data Providers that want to belong to a GII group or that request a group be created must provide a representative that obtains HSIN account credentials with which to access GII as an individual GII user.

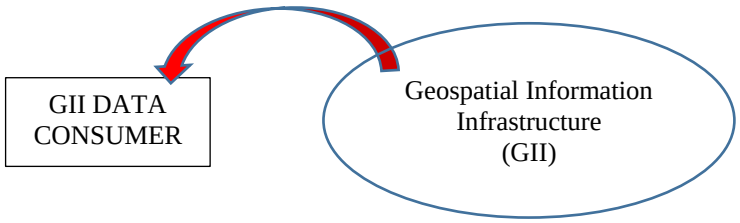


GII Data Consumer

A GII Data Consumer can be both from within DHS and external to DHS and represents an application or system that supports the homeland security mission. Though the Data Consumer does not require HSIN authentication, through a data use agreement (i.e., MOU/A, ISA) with GMO, the Data Consumer can request to receive data from GII into an application or service that the Data Consumer owns, regardless of whether that application or service is within or outside of DHS. The requested data is owned and managed by the Data Owner. If the Data Owner authorizes sharing with the Data Consumer, GMO will make the requested data available to the Data Consumer's application or system. This process ensures that Data Providers still maintain control over with whom their data is shared.

[4] Individual GII users are technically Data Providers as well if they have data to share. Those users just share and interact within the GII.

GII Data Consumers that want to belong to a GII group or that request a group be created must provide a representative that obtains HSIN account credentials with which to access GII as an Individual GII User.



- POC: Applications/System Owner
- Requires MOU (if application INTERNAL to DHS)
- Requires ISA (if application EXTERNAL to DHS)
- Data within GII is limited and managed by Data Provider
- Data availability in the application/system is managed by the data provider (i.e., data owner)
- User access to the application/system is managed by the data consumer (i.e., application/system owner)

Through these information-sharing agreements and administrative support, the GMO provides GII as the infrastructure and environment to securely share data with authorized applications, pursuant to the terms agreed to by the data owners, data consumers, and the GMO. The GII System Owner, Program Manager, and Information System Security Officer (in collaboration with GII technical support staff) evaluate the specifics of the agreements to determine approval for handling data potentially shared within the GII.

While the GII does not restrict what data the GII user can upload, the GII Disclaimer provides governance that "Sensitive Information (e.g., PII, law enforcement sensitive (LES) information) may be provided to this system from external sources not originating from this computer system, and are subject to federal privacy laws (e.g., Privacy Act of 1974), federal records retention schedules, and information security and privacy policy local to the source of the sensitive information. As a user of the GII, you are responsible for the protection, accuracy, and trustworthiness of information shared within this computer system." All GII users must agree to the GII Disclaimer each time they access the GII.

The GMO provides a secured web-application environment of its GII services in collaboration with each data owner's data sharing mission, while maintaining the integrity of each tenant's data management and use. Moreover, the GII provides secure web services of hosted geospatial data and supports several applications. A full list of applications supported by the GII can be found in Appendix A.

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?

- The Homeland Security Act of 2002 as codified at 6 U.S.C. § 121(d)(1); 6 U.S.C. § 121(d)(4); 6 U.S.C. § 121(d)(11); 6 U.S.C. § 121(d)(12)(A); 6 U.S.C. § 121(d)(15); and 6 U.S.C. § 121(d)(17) provide DHS and the National Operations Center (NOC) with authority to establish HSIN and to collect the information in HSIN.
- 6 U.S.C. § 343, provides for the establishment of the office of Geospatial Management within the Office of the Chief Information Officer.
- Pub. L 108-458, "The Intelligence Reform and Terrorism Prevention Act of 2004," Title VIII, "Other Matters, Section 8201, "Homeland Security Geospatial Information."
- 44 U.S.C. Ch. 35, "Coordination of Federal Information Policy."
- Executive Order 12906, "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure," April 11, 1994, as amended by Executive Order 13286, February 28, 2003.
- Office of Management and Budget (OMB) Circular A-16, "Coordination of Geographic Information and Related Spatial Data Activities."
- OMB M-11-03, "Issuance of OMB Circular A-16 Supplemental Guidance."
- DHS Management Directive, Information Technology Integration & Management, Directive Number: 142-02, Revision 00, February 6, 2014.
- DHS Enterprise Architecture Management Policy, Directive Number: 103-02, Revision 00, June 19, 2014.
- DHS Directive Enterprise Data Management Policy, Directive 103-01 Revision 1, August 25, 2014 [Supersedes DHS Policy for Internal Information Exchange and Sharing, February 1, 2007].
- DHS Management Directive No. 034-01, Geospatial Management, Revision 00, January 28, 2015.
- DHS Directive Instruction No. 034-01-001, Revision 00, Instruction for Identifying and Acquiring Unclassified Geospatial Information, March 23, 2016.

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

The GII itself does not collect any mission data; rather it acts as a service that provides a platform for mission partners to share their data. The data remains under the ownership of the data owner or GII user that manages it. For federal mission partners, System of Records Notices (SORN) that apply to the records controlled by each participating data owner will differ based on the source of that data.

The GII does collect data about GII users to provide administrative functions such as creating groups and managing agreements between Data Providers and Data Consumers. This and the information collected by HSIN to provision user accounts is covered by the following SORNs:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792; and
- DHS/ALL-037 E-Authentication System of Records, August 11, 2014, 79 FR 46857.

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

Yes. The GII has a System Security Plan as the system is operational and has been granted an Authority to Operate (ATO).

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

No. As the mission of GII is to allow homeland security mission users to share geospatial and geospatial-related information, including data for critical infrastructure, natural hazards, law enforcement, and aerial imagery, that support the homeland security enterprise mission, GII does not retain ownership or management of the mission data. Data owners are responsible for the retention of records according to their own approved retention schedules.

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 provisions of the Paperwork Reduction Act are not applicable to the GII as no information is collected directly from members of the public. However, some information from mission partners may be subject to the Paperwork Reduction Act and would be addressed in the privacy documentation for those records.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

The GII provides a secure environment for the publishing and sharing of homeland security mission information across the homeland security enterprise. Within its applications and services, GII users can select from various geospatial datasets that reside on the GII to identify an area of interest to add relevant business, operational, or mission information data layers. Examples of those geospatial datasets include:

- Imagery and remotely-sensed data[5] to include satellite imagery base maps and Earth observation datasets provided by organizations such as the National Aeronautics and Space Administration (NASA), U.S. Geological Survey (USGS), Department of Energy (DOE), National Oceanic and Atmospheric Administration (NOAA)
- Feeds from the Department of Defense's (DoD) U.S. Northern Command (NORTHCOM) Situational Awareness Geospatial Enterprise (SAGE) information sharing platform
- USGS hazards including earthquakes and other types of natural hazards
- Weather, Oceans, and Riverine data, including NOAA weather watches/warnings/advisories and near real-time observations; Federal Emergency Management Agency (FEMA) 100- and 500-year floodplain boundaries; and USGS stream gauges
- More than 600 federal critical infrastructure layers (i.e., Homeland Infrastructure Foundation-Level Data (HIFLD))

Depending on authorization provided by the data owner, the GII user or data consumer can view shared content (e.g., PII or LES information) within GII data layers. The data owner must provide GMO with details regarding the dissemination of data elements and their data's accessibility to GII users. If no authorization is provided by the GII data owner, the data consumer or GII user cannot access data that belongs to the data owner.

Data owners provide data that is consistent with the homeland security enterprise mission in support of the GSSA. The requirement of the use of PII is determined by the data owner. For example, a local law enforcement data owner may have a requirement to share information with a federal law enforcement data consumer or group member. The GII provides the platform with which to share this data in a geospatial structure. This pattern applies across all use cases whereby the data provider determines the use and the degree of use of PII within geospatial data sets in the

[5] Data acquired from a distance such as Light Detection and Ranging (LiDAR).

GII. Any PII will be minimized to the greatest extent possible.

This information may include mission-related PII and LES data maintained within the management of the data owner for accessibility. Specific Sensitive PII (SPII)[6] elements (e.g., Social Security number (SSN), Alien number (A-number), passport information, special protected classes data[7]) are maintained by the data owner outside of the GII. Requests for sharing of SPII are coordinated outside of the GII and through the point-of-contact available on the data Content Details page associated with the information. Data layers created and managed by the data owner and applied for sharing in the GII may include the following about individuals who are subjects of the homeland security mission space:

- Name;
- Date of birth;
- U.S. citizen (yes/no);
- Contact information, including phone numbers and email addresses;
- Address;
- Physical description, including height, weight, eye, and hair color;
- Distinguishing marks, including scars, marks, and tattoos;
- Case number or reference number; and
- Public source data including commercial databases, media, social media, newspapers, and broadcast transcripts (e.g., information collected during an incident response for situational awareness).

Additionally, limited contact and business information about the provider or contributor of the published content is used for follow-up inquiries or requests for additional information.

Moreover, GII users can also upload content or access their GII content via applications and can create features and add features from text files, GPS files, and other files. The GII supports the storage of a number of data files (e.g., .pdf, .csv, .jpg) and mapping files (e.g., .shp, .kml) that users can upload.

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

Individual data owners and GII users are the sources of the data used in the GII, although the GII itself does maintain and provide various geospatial datasets as described above. The

[6] SPII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. *See* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.
[7] Special protected classes of individuals include nonimmigrant status for victims of human trafficking, nonimmigrant status for victims of crimes, and relief for domestic violence victims.

mission of the GII is to provide a secured infrastructure where each mission partner desiring to share or receive GII geospatial data, or the like, can access GII's secured, controlled environment for that purpose. The GII mission partners that provide homeland security data for sharing maintain full management control of their data and its data elements.

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 GII is constructed with commercial-off-the-shelf software that enables the management, visualization, and analysis of information, including that of commercial and publicly available sources. Examples of these sources include geospatial web services from FEMA, NOAA, and USGS. Additionally, GII users can upload data (i.e., a spreadsheet file, image, web service link) to their individual GII account content. The GII user's content can contain any information or data (e.g., PII, LES information, commercial data, social media information) or be uploaded from any source as long as the file type is accepted by the GII. Social media information generally includes content from official sources (e.g., National Weather Service, USGS, Washington, D.C. Emergency Services).

2.4 Discuss how accuracy of the data is ensured.

Mission partners participating in the GII maintain, through a data use agreement (i.e., MOU/A, ISA) with the GMO, full management control of their data and provide data elements chosen in support of their mission. GII developers may assist in technical configuration or formatting to support the data-sharing effort of the data owner. Because the data remains under ownership of the owner, it is ultimately the data owner's responsibility to ensure accuracy of the data provided to other homeland security mission partners.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that, because ensuring the accuracy of the data on the GII falls upon the mission partner, inaccurate information may be shared to homeland security mission partners.

Mitigation: This risk is not fully mitigated. The GII does not independently maintain mechanisms that validate the accuracy of the data provided by mission partners. However, GII developers may assist in technical configuration or formatting to support data owners inputting data onto the GII.

The mission partner (as data owner) maintains management rights to the data shared on the GII and, therefore, its accuracy. Only GII users that have been authorized by the data owner to

view data available within the GII can access that data. Should there be a question of the accuracy of data provided by a data owner, the GII user can coordinate with the data owner (through contact information provided within the data or send an inquiry through the GMO to the data owner who is responsible for data accuracy) to validate accuracy. Moreover, the GII Disclaimer states, "As a user of the GII, you are responsible for the protection, accuracy, and trustworthiness of information shared." All GII users must agree to the GII Disclaimer each time they access the GII.

Additionally, the data use agreement (i.e., MOU/A, ISA) outlines that data owners are responsible for the accuracy of the data as it is not owned by the GII. The GMO team will also conduct an annual outreach to all data owners to confirm their data is still accurate and active.

Privacy Risk: There is a risk that a data owner will display PII when it is not necessary for the mission need.

Mitigation: This risk is not fully mitigated. However, the GMO team has taken several steps to limit the amount and sensitivity of PII on the GII and to whom PII is authorized for sharing. Certain PII (e.g., SPII data like SSN, A-numbers, passport information) not listed above in Section 2.1 is not permitted for sharing on the GII. If, through the collaborative effort to share PII data, additional PII or SPII is required, the group member may make a request to the data owner. These additional PII and SPII requests are coordinated outside of the GII and through the point-of-contact available on the Data Content Details page for that initial information. The actual sharing of these sensitive data elements is outside of the GII information system and through the point-of-contact available on the Data Content Details page associated with any information that might necessitate more detailed sharing among homeland security mission partners. Additionally, during the Group creation process, the GMO asks the data owner if any PII is planned to be shared in the group and, if yes, to list the PII data types. This gives the GMO team more oversight of the data (to share PII, if required and to omit sharing SPII when required) at a group level. GMO works with the data owner to ensure the data shared follows the restrictions and requirements GMO has established. The GMO also submits a PTA for each user group to the DHS Privacy Office for review and approval. Finally, each time a user accesses the GII, he or she must agree to the GII Disclaimer, which states that users are responsible for the protection of the information they share within the GII.

However, because the data remains under ownership of the data owner, it is ultimately the data owner's responsibility to ensure that the PII uploaded to the GII is limited.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

The GII provides a secure, web-based platform and integration framework to supply

standards-based geospatial content, services, applications, and training resources. GII users who desire to benefit from the mapping and geospatial data sharing services of GII, and who may collect homeland security mission-related data external to GII, use the platform to access these resources and to collaborate with mission partners.

Data owners, however, have complete management capability of data provided through their GII account. In order to collaborate with mission partners or individuals, data owners can make their data and related applications designed within their account available to these partners. This independent data management allows for GII to be securely accessible to homeland security enterprise users, DHS Components, other federal agencies through partnerships with state, local, tribal, territorial, and private organizations and to securely share geospatial-enabled information on critical infrastructure, natural hazards data, aerial imagery, and other user-defined geo-enabled data; as well as perform spatial analysis such as querying, geocoding, and routing functions.

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. The GII does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

Yes. GII users may include all DHS Components, as well as other federal, state, local, tribal, territorial, private sector, international, and other non-governmental homeland security mission partners. However, only authorized DHS GMO personnel are assigned administrative roles and responsibilities within the GII.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information within GII may be used in a manner that is inconsistent with a GII user's specific mission area and authorities.

Mitigation: The GII mitigates this risk in several ways. First, access to the GII and the data shared upon the platform is only granted to authorized HSIN account holders who have gone through identity management authentication. Second, data owners within the GII control authorization and access to their data and are enabled to share it how they determine appropriate. Third, the GMO leverages HSIN for the provision of baseline user training regarding privacy-related topics to all HSIN users as a function of becoming a user.

Moreover, access to geospatial data collected and disseminated within the GII accreditation

boundary is managed by approval through the GMO. For non-public geospatial data (e.g., state and local LES information), access is approved from the data owner who, through authorization, gives direction to the GMO to avail data to defined audiences. Publicly available geospatial data, in support of the GSSA mission, and all data within the GII accreditation boundary, is protected through the implementation of security controls to protect the confidentiality, integrity, and availability of that data.

Finally, every GII user agrees to the terms of the GII Disclaimer, as well as all terms related to obtaining a HSIN account. GII mission partners that wish to consume GII content outside of the GII (i.e., in an external application) must adhere to the information sharing agreements (e.g., MOU/A, ISA) that are established between the data owner and data consumer.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

The GII does not provide notice to individuals prior to the collection of their information shared on the GII by mission partners. However, data owners are responsible for determining and delivering appropriate notice to individuals from whom information is collected and incorporated into the GII in accordance with their own legal requirements and policies, generally at the time of initial collection.

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

Depending on the mission partner supplying the data to the GII, individuals may have the opportunity to decline to initially provide the information. The notice provided to the individual by the mission partner at the point of collection will specify for the individual what options exist related to consent, opt-in, or opt-out. However, the GII does not afford individuals the opportunity to consent to use, decline to provide information, or opt-out of their information being shared on the GII.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not provided adequate notice that their information will be shared within the GII.

Mitigation: This risk cannot be fully mitigated. Information posted in data layers to the

GII or provided by users and data owners may contain PII on individuals who know that their information was collected initially by a mission partner, but do not then know that their information has been shared to homeland security mission partners on the GII.

Other than through this PIA, this risk cannot be mitigated by the GII.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

The GII relies on the data provision of its mission partners and does not own or change any of the data provided for sharing within the GII. The retention of data, in accordance with the National Archives and Records Administration's (NARA) General Records Schedules for federal partners, is left as a responsibility of the data owner.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk of retaining information on the GII for longer than permitted by the data's retention schedule.

Mitigation: This risk cannot be fully mitigated. Because the GII leaves the data provision responsibility to the data owner, GMO does not delete or remove a user's data. GMO provides in the GII Disclaimer and all data use agreements (e.g., MOU/A, ISA) that GII users and data owners are "responsible for the accuracy and trustworthiness**,** federal retention schedules, and information security and privacy policy local to the source of information shared."

GII does not have an automatic mechanism in place to monitor data its mission partners share. However, all data owners in the GII can dictate the usage of their data. Data retention requirements, visibility of data elements, and other terms of use can be added by GII administrators, on behalf of data owners, through descriptive metadata fields on the data Content Details page. The data Content Details page is available to any GII user that has authorization to access to that data.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government, and private sector entities.

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

Yes. Federal, state, local, tribal, territorial, private sector, international, and other non-governmental personnel who support the homeland security mission may be granted access to the GII and the data shared within. The specific use and sharing of the GII data will vary depending the homeland security mission of the GII user, data owner, data consumer, and data.

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

The data shared externally from the GII across federal, state, local, tribal, territorial, private sector, international, and other non-governmental partnerships who support the homeland security mission is not owned or managed by the GII. Data is shared to external mission partners according to data owners' and GII users' own legal and policy requirements. Because the data remains under the management of the data owner, external sharing of data is subject to the SORN compatibility analysis on a case-by-case basis. In the case of federal mission partners' data, this sharing would be done in accordance with the SORN and applicable routine uses that applies to the data being shared.

Additionally, the data owner and GII user agree to manage the security and privacy of their data, as provided in the GII Disclaimer.

6.3 Does the project place limitations on re-dissemination?

The GII itself does not place limitations on re-dissemination. The GII enables mission partners and data owners to determine their own sharing requirements based on MOU/A and ISA agreement documentation. By default, data is private to a data owner. The data owner must explicitly share the data to other GII users for it to be viewed and accessed. Once shared, the data is still controlled by the data owner and access to other GII users can be removed by the data owner at any time. Any re-dissemination limitations would be put into place by the individual data owner.

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

The disclosure of GII content outside DHS is dictated by the terms of the MOU/A and ISA

agreement documentation with the data consumer (i.e., application or service), data owner, and GII user. GMO maintains a record of all data use agreements for the sharing and disclosure of data on the GII within and outside DHS. The GII does not, however, maintain a record of the specific data exchanges or data disclosures for GII users.

The GII user can discover or assign other GII users within the information system and can select to share data with those users as group members. If one GII user shares data with another, the GII system audit logs maintains a record of those accounts and if they are within a shared group. However, the individual data being shared is not tracked. To monitor accounts created within and external to DHS, GII leverages HSIN to capture a record of accounts accessing GII in support of the GII mission. The GII Information System Security Officer (ISSO) and System Owner perform a periodic review of accounts created within GII.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that authorized users may inappropriately disclose GII information, either intentionally or unintentionally.

Mitigation: The GII partially mitigates this risk in several ways. All GII users are required to complete privacy training (via HSIN) that addresses the appropriate and inappropriate uses and disclosures of information they receive as part of their official duties. Additionally, users are required to undergo full identity access management to be recertified annually. Auditing information collected within the GII is correlated across the system, operational, and enterprise levels. At the system level, the GII relies on HSIN to monitor access, time stamps, user identity authentication, and other security relevant events. Information collected on GII servers is correlated by the DHS Security Operations Center on a continuous basis. The DHS Security Operations Center provides significant events and findings and information is correlated across the enterprise and distilled back to operational centers for situational awareness. Moreover, all use of the system and access to data is monitored and audited. Should a user inappropriately disclose information, the disclosure will be referred to the appropriate internal investigation entity and the individual is subject to loss of access.

Privacy Risk: There is a privacy risk that more information may be shared than is necessary for a recipient's use.

Mitigation: This risk is partially mitigated. The GMO has procedures to limit the PII that can be shared. Section 2.1 outlines the information that is permitted to be shared on the GII. Prior to onboarding a new group to the GII, the GMO team will work with the data owner to ensure that data intended for sharing fits within the restrictions outlined in this PIA. If, through the collaborative effort to share PII data, additional PII or SPII is required, the group member may make a request to the homeland security data owner. Additionally, PII and SPII requests are coordinated outside of the GII and through the point-of-contact for that initial information. Also,

each time a user accesses the GII (i.e., as an Individual User), the user must agree to the GII Disclaimer which states that users are responsible for the protection of the information they share within the GII.

However, because the data remains under ownership of the data owner, it is ultimately the data owner's responsibility to ensure that the PII shared on the GII is done so in an appropriate manner and to those with a need-to-know.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

The GII relies on the data provision of its mission partners and does not own or change any of the data provided for sharing within the GII. Because the GII does not own any of the data, the ability of individuals to access their information lies with the data owner. Each data owner may have different procedures that allow for individuals to access their information depending on the applicable SORN, for federal agencies, and applicable handling requirements for other non-federal agencies, such as local law enforcement.

Individuals seeking access to any record contained within a DHS source system of records, may submit a Privacy Act or Freedom of Information Act (FOIA) request in writing to the Headquarters or Component FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under - contacts. If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA, Privacy Office, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

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

Because the GII does not own any of the data shared, the ability of individuals to correct inaccurate or erroneous information lies with the data owner. Each data owner may have different procedures that allow for individuals to correct their information. Individuals seeking correction of any DHS record contained in a source system of records may submit a request in writing to the Headquarters or Component FOIA Officer as described in Section 7.1

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

Because the GII does not own any of the data shared, it cannot notify individuals directly about the procedures for correcting their information. This PIA serves as notice that individuals must contact the data owner or follow the data owner's process if they seek to correct their information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that individuals will be unable to correct or amend information about them that is shared in the GII.

Mitigation: This risk cannot be mitigated by the GII. Individuals may correct information as provided for in the applicable SORN for federal agencies or via the process afforded by state, local, tribal, territorial, private sector, international, and other non-governmental GII users. This PIA provides notice of this risk, but the GII cannot mitigate it itself.

Section 8.0 Auditing and Accountability

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

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

The GII maintains compliance to DHS policy for the implementation of security controls to manage the security of all GII data. The GMO ensures all GII users are authorized to operate within the bounds of their actual authorities, DHS policy, and the agreed-upon terms spelled out within the GII Disclaimer, MOU/A and ISA agreement documentation, and authorization documentation for the access and use of the GII and its information. Additionally, the GII ISSO and System Owner perform a periodic review of accounts created within GII as part of the GII account management best practices for security.

The GII System Owner, Program Manager, and ISSO review security- and privacy- related functions and system requirements for GII on annual basis or whenever a significant change occurs to ensure compliance with DHS policy. The GMO team will also conduct an annual outreach to all data owners to confirm their data is still accurate and active.

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

The GMO is dedicated to promoting the geospatial tradecraft, professional development, and building a stronger community of interest across industry, academia, government, professional

organizations, and individual stakeholders. All users, internal to DHS and external, who handle PII within the GII are required to complete DHS Privacy training provided at https://www.dhs.gov/xlibrary/privacy_training/index.htm to fulfill their agreement (e.g., MOU/A, ISA) to provide or access PII data available within GII. Additionally, relevant to the GII mission, HSIN offers baseline training regarding the privacy-related topics listed below to all HSIN users.

- Privacy and FOIA compliance
- Records Management
- Roles/Limitations
- Classifications and Markings (PII, Sensitive Security Information (SSI), For Official Use Only(FOUO))
- Nomination/Validation Certifications
- Mobile Device Access
- Shared Space Activities

Moreover, all DHS personnel receive annual privacy and security 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?

By default, data is private to a data owner or individual user. Access to the data is determined and provisioned by the data owner or individual user, who have the ability to remove access to data provided or to invite/remove GII users to a group. The GII is designed for all data owners and individual users to determine who should access their data, and that responsibility falls on those individuals. The GII, as a service provider, can facilitate any issues regarding access or revoking access permissions to support users.

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?

The DHS GMO supports homeland security mission partners within the GII. To provide secure data feeds to external mission systems, GII users must request access from the GMO by submitting a data use agreement (e.g., MOU/A, ISA) as a process of sharing geospatial and other homeland security mission-related data delivered by or retrieved from a data owner within their independent GII account.

The GII System Owner, Program Manager, and ISSO (in collaboration with GII technical

support staff) evaluate, based on DHS policy, the data use agreement and make a determination based on the data format, technical details, delivery method, classification level, inclusion of PII, ports, protocols, etc., if the information is appropriate for the GII. The GMO is working with DHS Privacy Office to update its MOU/A template to align with requirements to ensure the secure handling of privacy information with all parties of the MOU/A and ISA documentation.

Responsible Officials

Lewis Summers
Program Manager
Geospatial Information Infrastructure
Geospatial Management Office
Department of Homeland Security

Approval Signature

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

_____

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

Appendix A: Applications Supported by the GII

- **Cyber-Communications Common Operating Picture (COP)** – The Cyber COP is an application focused on incidents related to cyber-crimes including such issues as fiber cuts, fires, infrastructure collapses, attacks on systems, and exercises. Used by National Cybersecurity & Communication Integration Center (NCCIC), Cyber-Communications COP implementation is a joint effort by the NCCIC, DHS National Operations Center (NOC), and federal, state, local, territorial, tribal, and industry partners to integrate objectives, goals, and processes which drive daily operations of the Cyber-Communications COP and integration with the DHS Common Operating Picture through a broad set of capabilities based on best-in class technologies that deliver a rich, end user experience through a web accessible interface.
- **DHS COP –** The DHS COP is an application developed to provide Homeland Security Enterprise professionals with enhanced situational awareness and a common operating picture for the entire Federal Government. The DHS COP architecture coupled with data from federal, state, local, tribal, and territorial (FSLTT) and international customers and partners provides actionable information, enhanced contextual understanding, and geospatial awareness for government and private sector leaders to make timely and informed decisions, and identify courses of action during an event or threat situation prior to, or in the aftermath of a natural disaster, act of terrorism, or man-made disaster.
- **Countering Weapons of Mass Destruction Office (CWMD)–** The Countering Weapons of Mass Destruction Act of 2018 redesignated the Domestic Nuclear Detection (DNDO) Office as CWMD and established the Securing the Cities (STC) program under CWMD. STC provides for the safety of staff and continuation of Mission Essential Functions (MEFs) to mitigate illness while minimizing mission disruption during a biological incident (e.g., a pandemic disease outbreak, an emerging infectious disease outbreak, or an adversarial biological attack). Moreover, it uses the Radiation Alarm Reporting application, designed for those who specifically support the STC program and for those in the field tracking real-time incidents, to assist in tracking radiation reports throughout the country.
- **GII Portal** - The GII Portal is an application hosted on the GII that allows users to upload, manage, and consume geospatial content, as well as leverage web mapping tools and services. Upon logging into the GII, users are presented with the GII Portal homepage. This homepage provides access to training resources, announcements, and user guides and serves as the jumping off point for other GII hosted applications such as the NOC COP, Cyber COP, etc.
- **Homeland Infrastructure Foundation-Level Data (HIFLD) Open** – The HIFLD Open data portal was developed for the collection and sharing of national foundation-level geospatial critical infrastructure data to provide a common foundation for data visualization and analysis useful to support community preparedness, response and recovery, resiliency, research, and

more. Integrated with the Geospatial Platform through Data.gov and other data providers that provide shared and trusted geospatial data, services, and applications for use by the public and by government agencies and partners to meet their mission needs, HIFLD Open contains 320 public datasets—consisting of re-hosted public data and direct pointers to live data services.

- **HIFLD Secure** – The HIFLD Secure data portal was developed, similar to HIFLD Open, to provide web-enabled delivery of For Official Use Only (FOUO) and licensed critical infrastructure data (i.e., Chemical Manufacturing, Educational Services, Air Medical Communication or Dispatch Centers, Fire Stations, Public Safety Answering Point (PSAP) 911 Service Area Boundaries, National Security International Affairs, Justice, Public Order, and Safety Activities, Hospitals) and commercially licensed content. Composed of over 125 data layers, HIFLD Secure provides access to the most current and authoritative data available.
- **Joint Task Force (JTF) COP** – The DHS JTF COP and Common Intelligence Picture (CIP) provides the Department and Joint Task Forces East, West, and Investigations the ability to identify, fuse, and visualize critical information, which contains a location or address, in a single environment. This enhanced situational awareness supports the Department's unity of effort in securing the Southern Border and Approaches region. By pulling together, through the "acquire information once, use multiple times" approach available through the GII, partner feeds from the National Oceanic and Atmospheric Administration, the National Geospatial-Intelligence Agency, and the U.S. Northern Command, among others, the JTF COP ensures that DHS mission owners can acquire and assimilate required information when they need it to operate more effectively and efficiently.
- **National Biosurveillance Information Center (NBIC) COP** – The NBIC COP is an application that integrates, analyzes, and distributes key information about health and disease events to help ensure the nation's responses are well-informed, save lives, and minimize economic impact. Formally as part of the DHS Office of Health Affairs, and now as part of CWMD, NBIC collaborates with and serves as a bridge between federal, state, local, territorial, and tribal partners to integrate information from thousands of sources about biological threats to human, animal, plant, and environmental health, improving early warning and situational awareness.
- **Requests for Information (RFI)** – The RFI tool is an information sharing application designed to support the DHS Office of Operations Coordination (OPS) mission to provide information daily to DHS leadership to enable decision-making; oversee the DHS National Operations Center (NOC); and lead the Department's Continuity of Operations (COOP) and Government Programs that enable the continuation of primary mission essential functions of DHS. RFI integrates intelligence, situational awareness, and COP information received at the

NOC that must be rapidly analyzed, displayed, and reported into intelligence products that are shared with federal, state, and local level partners.

- **The Radio Frequency Interference Tracker (RFIT) –** The RFIT is a collaborative, inter-agency web-based application that allows stakeholder agencies to document and share, in real time, GPS-related outage information. This application is used primarily by the U.S. Coast Guard (USCG).