Geospatial Information Infrastructure Technical Support

GII Developer Guide

Version 1.0
Submission Date: 6/13/2016

Submitted By:

Ardent Management Consulting, Inc.
1840 Michael Faraday Drive, Suite 120
Reston, VA 20190

Submitted To:
Geospatial Management Office
Office of the Chief Information Officer
U.S. Department of Homeland Security

TABLE OF CONTENTS

1 Overview 3

1.1 Introduction 3

1.2 Program Background 3

1.3 GMO Contact Information 3

1.4 Privacy and Security 4

1.5 References 4

1.6 Acronyms 4

2 Geospatial Applications 5

2.1 GII Portal 5

2.2 Common Operating Picture 5

2.3 ArcGIS API for JavaScript 6

3 Geospatial Services 6

3.1 Accessible GII Web Services 6

3.2 Spatially Enabling Data & Publishing Service 6

3.3 Securing Geospatial Web Services via Token 7

3.4 Geospatial Service Formats 7

3.4.1 GeoJSON 8

3.4.2 GeoRSS/RSS Feed 8

3.4.3 KML 8

3.4.4 WMS 8

3.4.5 WFS 8

4 Summary 8

Table of Tables

Table 1 – References 4

Table 2 – Acronyms 5

Table 3 - Accessible Services 6

Revision History

Version Number	Version Date	Revisions Made by	Description of Revisions
Version 0.1	10/30/2015	Jean Brandenburg	Develop Draft
Version 0.2	4/26/2016	Michael Karikari	Add additional content based on feedback from PM
Version 0.3	5/6/2016	Michael Karikari	Make edits based on the Peer Review
Version 1.0	5/11/2016	Jean Brandenburg	Added Privacy & Security, Summary and Appendix sections
Version ##	Date	<<Enter Name>>	<<Enter Text>>

1 OVERVIEW

1.1 Introduction

The GMO has requested the preparation of the GII Developer Guide. This guide describes the development and implementation guidelines required for Components to build and deploy geospatial applications and services into the Geospatial Information Infrastructure (GII).

This guide is broken up into the following sections:

- ***Overview:*** This section provides program background, GMO Contact Information, References, and Acronyms. It also provides information on ***Privacy and Security***, which the development teams are responsible for.
- ***Geospatial Applications:*** This section provides information on geospatial applications that a development team may use or customize to support their mission needs. Information about the GII Portal, the Common Operating Picture application, and the Esri ArcGIS API for JavaScript are listed in this section.
- ***Geospatial Services:*** This section provides information for development teams on the geospatial services that the GII prefers to consume.
- ***Summary:*** This section sums up the guidance that the GMO is capable of providing to another development team.
- ***Appendix – GII Implementation:*** This section lists the configuration settings for the GII. It is recommended that this section only be available to the GMO GIS Administrator.

1.2 Program Background

The Department of Homeland Security (DHS) Geospatial Management Office (GMO) ensures interoperability across the DHS geospatial systems and facilitates integration of the DHS geospatial information and technology required to meet the needs of all DHS operational elements. The GII is designated as the enterprise geospatial solution for the DHS and the technical architecture uses enterprise solution software to support this platform. One of the custom interfaces provides a "Common Operating Picture" (COP) view of the geospatial and mission data to end users using the Homeland Security Information Network (HSIN).

The Geospatial Common Operating Data (COD) also known as Homeland Infrastructure Foundation-Level Data (HILFD) is comprised of 3 product lines; HIFLD Open, HIFLD Secure, and HIFLD Secure & Licensed. These three distinct product lines are part of a new approach to meet changing needs of stakeholders and consumers. This new approach has led to the products being incorporated in GII data architecture and accessible external applications provided appropriate registration has occurred.

It is the objective of DHS through the GII to provide robust geospatial services, including capabilities supporting Common Operating Pictures and User Defined Operating Pictures (UDOP), supporting centralized archive and storage of COD and federated access to mission and real time data, and supporting services that will include geocoding, imagery map and feature services, and support real time streaming video from both land based and airborne sensors.

1.3 GMO Contact Information

Contact the GMO at DHS_GCOE@hq.dhs.gov for any additional questions or information.

1.4 Privacy and Security

All development teams using the GII must adhere to all privacy and security policies for the DHS. The GII is a non-privacy sensitive system. ***Any privacy sensitive data stored on the GII must be vetted through the System Owner, ISSO and PMO. If a PTA is required, it will have to be drafted and routed to the Privacy Office for approval.*** If a development team wants to store privacy sensitive data on the GII, the onus is on this team to get permission from their Component or organization Privacy Office via a Privacy Threshold Analysis (PTA) and work with the GII ISSO to route the PTA through the appropriate channels. It is recommended that the development team justify gathering this information based on their mission needs.

From a security standpoint, the GII has a FIPS 199 rating of High, High, Moderate for confidentiality, integrity, and availability respectively. HSIN is also used to authenticate the user to Portal. HSIN provides secure integration and interoperability of information-sharing resources within the Homeland Security enterprise.

For more information on privacy and security, as it directly relates to development or integration with the GII, refer to the ***GMO Contact Information.***

1.5 References

The following table contains URL reference information that are inputs for this guide.

URL	NOTES
http://server.arcgis.com/en/portal/latest/use/welcome.htm	WebApp Builder for ArcGIS
https://developers.arcgis.com/javascript/	Detailed resource on ESRI API which could be used to build out custom applications
http://services.arcgisonline.com/arcgis/rest/services	ArcGIS Online (AGOL) Basemaps – Free and Open
http://www.esri.com/software/arcgis/extensions/datainteroperability/supported-formats	ArcGIS Data Interoperability supported formats. All of the Esri supported formats are listed here too.
http://www.opengeospatial.org/standards/gml	Geography Markup Language (GML) GML schemas: The GML needs to be v2.1.2, v3.1.1 or v3.2.1.
http://www.opengeospatial.org/standards/kml	Describes the KML schema specification, working group details, and related news
http://www.opengeospatial.org/standards/wfs	Describes the WFS implementation specification
http://www.opengeospatial.org/standards/wms	Describes the WMS implementation specification and best practices
http://geojson.org/geojson-spec.html	Describes the GeoJSON schema specification provides example of syntax structure

Table 1 – References

1.6 Acronyms

The following table contains a list of acronyms used in this document.

Acronym	Description
ArdentMC	Ardent Management Consulting
COD	Common Operating Data
COP	Common Operating Picture
DHS	Department of Homeland Security
GII	Geospatial Information Infrastructure
GIS	Geographic Information System
GML	Geospatial Markup Language
GMO	Geospatial Management Office

Acronym	Description
HIFLD	Homeland Infrastructure Foundation Level Data
KML	Keyhole Markup Language
NOC	DHS National Operations Center
OGC	Open Geospatial Consortium
POC	Point of Contact
UDOP	User Defined Operating Picture
WFS	Web Feature Service
WMS	Web Map Service
XML	EXtensible Markup Language

Table 2 – Acronyms

2 GEOSPATIAL APPLICATIONS

The GII as a platform host several geospatial applications that enable and foster the sharing of spatial data throughout DHS for its components and external agencies. Below is the list of the GII's primary applications that utilize geospatial services along with their capabilities.

2.1 GII Portal

The GII Portal is a DHS hosted application deployed by the GMO to leverage geospatial services and related datasets into a user friendly interface that allows user to quickly gather and assess data for a larger audience or a limited group of users. As such, this ability to visualize and manage spatial data is the primary focus of the application. The following items are major capabilities that GII Portal makes available to end users of the application:

- Create, save and share web maps
- Create and host web mapping apps
- Search for GIS content within your organization
- Search for GIS content from external sources
- Create groups for sharing GIS information with other users
- Share links to GIS applications
- Share map and layer packages to use in Desktop application
- Consolidated search across external data sites (GeoPlatform.gov and Data.gov)

2.2 Common Operating Picture

The Common Operating Picture (COP) is used to monitor situational awareness across DHS. It is a web – accessible interface that coupled with data from Homeland Security partners and Homeland Security Information Network (HSIN), provides actionable information, enhanced contextual understanding, and geospatial awareness. As an application it enables government and private sector leaders to make timely and informed decisions, and identify courses of action during an event or threat situation. The COP provides users a broad set of capabilities based on best-in-class technologies that deliver a rich, end user experience through these features:

- Ability to define role based access
- Incident Management - Create, visualize and display incident information in a common operating picture available to all HLS partners.

- Map Visualization - View geo-extracted, auto-ingested information and create user-defined views of incident information.
- Reporting - Create, edit and update multiple reports for the Homeland Security community.
- Alert/Notification - Automatically alert users when information of interest is received or incidents are created.

2.3 ArcGIS API for JavaScript

This product is available through ESRI and allows developers to create custom geospatial applications tailored to meet business and technical requirements of an organization or specific effort. For more information on its capabilities and sample code, refer to ***References.***

3 GEOSPATIAL SERVICES

This section provides guidelines on the geospatial service formats that other components can develop to be consumed by the GII. The GMO prefers to consume geospatial formats that are supported by the ArcGIS Data Interoperability. For more information on supported geospatial formats, refer to ***GMO*** Contact Information

Contact the GMO at DHS_GCOE@hq.dhs.gov for any additional questions or information.

3.1 Privacy and Security

All development teams using the GII must adhere to all privacy and security policies for the DHS. The GII is a non-privacy sensitive system. ***Any privacy sensitive data stored on the GII must be vetted through the System Owner, ISSO and PMO. If a PTA is required, it will have to be drafted and routed to the Privacy Office for approval.*** If a development team wants to store privacy sensitive data on the GII, the onus is on this team to get permission from their Component or organization Privacy Office via a Privacy Threshold Analysis (PTA) and work with the GII ISSO to route the PTA through the appropriate channels. It is recommended that the development team justify gathering this information based on their mission needs.

From a security standpoint, the GII has a FIPS 199 rating of High, High, Moderate for confidentiality, integrity, and availability respectively. HSIN is also used to authenticate the user to Portal. HSIN provides secure integration and interoperability of information-sharing resources within the Homeland Security enterprise.

For more information on privacy and security, as it directly relates to development or integration with the GII, refer to the ***GMO Contact Information.***

References.

3.2 Accessible GII Web Services

The GMO in conjunction with partner DHS components makes its own map and web services available outside of the GII platform. Access to these services are granted and managed by the GMO. Available services are listed below:

ACCESSIBLE SERVICES	NOTES
COP Incident Feeds	Incidents generated from GII applications for DHS components and efforts
HIFLD Data	Open [public], Secure, Secure and Licensed datasets about critical infrastructure within the Homeland for Federal agencies through State, Local, Tribal, and private partnership

Accessible Services	Notes
ESRI Basemaps	Map depicting background reference information such as landforms, roads, landmarks, and political boundaries
KML Utility Service	Used for loading and visualizing KMLs
GeoRSS Utility Service	Used for loading and visualizing GeoRSS Feeds

Table 3 - Accessible Services

3.3 Spatially Enabling Data & Publishing Service

The GII offers infrastructure capabilities that enable it to connect or host external data sources. If an organization/component does not already have spatially-enabled web services available then the following steps can explain how to spatially enable data from a database in order to publish it to GII applications (Portal and/or COP):

1. Prerequisites
    a. ArcGIS for Server Publisher Credentials
        i. Must also provide database credentials to GII for registration purposes
    b. Data being published must have a spatial element associated with it in the form of: (latitude/longitude, address, or a geometry/shape field)
    c. Proper port/firewall configuration must be in place to allow successful communication between systems (Must coordinate with the GII system administrator)
    d. If editing is not required, publish a map service instead of a feature service
    e. If a feature service is required, use a simple query
        i. http://server.arcgis.com/en/server/10.3/publish-services/windows/00075-query-layer-has-a-complex-query.htm
2. Connecting to a database from the query layer interface in ArcMap
    a. http://desktop.arcgis.com/en/arcmap/10.3/map/working-with-layers/connecting-to-a-database.htm
3. Creating a query layer
    a. http://desktop.arcgis.com/en/arcmap/10.3/map/working-with-layers/creating-a-query-layer.htm
4. Publish Service
    a. http://server.arcgis.com/en/server/10.3/publish-services/windows/how-to-publish-a-service.htm

3.4 Securing Geospatial Web Services via Token

To ensure data integrity across the GII applications, the GMO has enabled an authentication system utilizing a token string for all services hosted within the GII. As such, in order for an application to take advantage of any service whether it be a map, routing, or feature service it will require being provisioned a token. The following information is required in order for any 3rd party application to use GII services:

- Point of Contact Name
- Point of Contact Email
- Application Name
- Application URL (Tokens are directly tied to the HTTP Referrer)

Once information is provided to GMO, a token will be issued to the POC with instructions on how to append the token to GII service URLs. Refer to ***GMO Contact Information*** for information on how to contact the GMO.

3.5 Geospatial Service Formats

The GMO prefers to consume a geospatial service using one of the following Esri formats:

- Esri ArcGIS Layer
- Esri ArcInfo Coverage
- Esri ArcInfo Export (E00)
- Esri ArcInfo Generate
- Esri ArcSDE
- Esri Geodatabase (File *.gdb*)
- Esri Geodatabase (Personal *.mdb*)
- Esri Geodatabase (XML)
- Esri PC ArcInfo Coverage
- Esri Shapefile

The following geospatial formats are also acceptable:

- GeoJSON
- GeoRSS/RSS Feed
  - GML
  - Simple
- KML
- WMS
- WFS

3.5.1 GeoJSON

GeoJSON is an open standard format used for encoding a variety of geographic data structures (Point, Line, Polygon, Multipoint, Multiline, Multipolygon) based on JavaScript Object Notation. Refer to ***GMO*** Contact Information
Contact the GMO at DHS_GCOE@hq.dhs.gov for any additional questions or information.

3.6 Privacy and Security

All development teams using the GII must adhere to all privacy and security policies for the DHS. The GII is a non-privacy sensitive system. ***Any privacy sensitive data stored on the GII must be vetted through the System Owner, ISSO and PMO. If a PTA is required, it will have to be drafted and routed to the Privacy Office for approval.*** If a development team wants to store privacy sensitive data on the GII, the onus is on this team to get permission from their Component or organization Privacy Office via a Privacy Threshold Analysis (PTA) and work with the GII ISSO to route the PTA through the appropriate channels. It is recommended that the development team justify gathering this information based on their mission needs.

From a security standpoint, the GII has a FIPS 199 rating of High, High, Moderate for confidentiality, integrity, and availability respectively. HSIN is also used to authenticate the user to Portal. HSIN provides secure integration and interoperability of information-sharing resources within the Homeland Security enterprise.

For more information on privacy and security, as it directly relates to development or integration with the GII, refer to the ***GMO Contact Information.***

References for more information on working with this geospatial web service.

3.6.1 GeoRSS/RSS Feed

3.6.1.1 GML

GML is an XML format used to express geographical features. GML serves as a modeling language for geographic systems as well as an open interchange format for geographic transactions on the Internet. As with most XML based formats, there are two parts - the data schema that lists the fields and the actual data used. The GML schema describes the fields being used, which contain generic geographic data sets like points, lines and polygons. Note: An application schema may refer to roads, highways, and bridges, instead of points, lines polygons.

The GML schema version should be v2.1.2, v3.1.1 or v3.2.1. For more information on GML, refer to ***GMO*** Contact Information
Contact the GMO at DHS_GCOE@hq.dhs.gov for any additional questions or information.

3.7 Privacy and Security

All development teams using the GII must adhere to all privacy and security policies for the DHS. The GII is a non-privacy sensitive system. ***Any privacy sensitive data stored on the GII must be vetted through the System Owner, ISSO and PMO. If a PTA is required, it will have to be drafted and routed to the Privacy Office for approval.*** If a development team wants to store privacy sensitive data on the GII, the onus is on this team to get permission from their Component or organization Privacy Office via a Privacy Threshold Analysis (PTA) and work with the GII ISSO to route the PTA through the appropriate channels. It is recommended that the development team justify gathering this information based on their mission needs.

From a security standpoint, the GII has a FIPS 199 rating of High, High, Moderate for confidentiality, integrity, and availability respectively. HSIN is also used to authenticate the user to Portal. HSIN provides secure integration and interoperability of information-sharing resources within the Homeland Security enterprise.

For more information on privacy and security, as it directly relates to development or integration with the GII, refer to the ***GMO Contact Information.***

References.

3.7.1.1 Simple

Designed to be concise, in both representation and conception. Each of the four GeoRSS objects require only a single tag. Refer to ***GMO*** Contact Information
Contact the GMO at DHS_GCOE@hq.dhs.gov for any additional questions or information.

3.8 Privacy and Security

All development teams using the GII must adhere to all privacy and security policies for the DHS. The GII is a non-privacy sensitive system. ***Any privacy sensitive data stored on the GII must be vetted through the System Owner, ISSO and PMO. If a PTA is required, it will have to be drafted and routed to the Privacy Office for approval.*** If a development team wants to store privacy sensitive data on the GII, the onus is on this team to get permission from their Component or organization Privacy Office via a Privacy Threshold Analysis (PTA) and work with the GII ISSO to route the PTA through the appropriate channels. It is recommended that the development team justify gathering this information based on their mission needs.

From a security standpoint, the GII has a FIPS 199 rating of High, High, Moderate for confidentiality, integrity, and availability respectively. HSIN is also used to authenticate the user to Portal. HSIN provides secure integration and interoperability of information-sharing resources within the Homeland Security enterprise.

For more information on privacy and security, as it directly relates to development or integration with the GII, refer to the ***GMO Contact Information.***

References for more information on working with this geospatial web service.

3.8.1 KML

An XML language focused on geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the sense of where to go and where to look. KML is complementary to most of the key existing OGC standards including GML, WFS and WMS. Currently, KML 2.2 utilizes certain geometry elements derived from GML 2.1.2. These elements include point, line string, linear ring, and polygon. Refer to ***GMO*** Contact Information
Contact the GMO at DHS_GCOE@hq.dhs.gov for any additional questions or information.

3.9 Privacy and Security

All development teams using the GII must adhere to all privacy and security policies for the DHS. The GII is a non-privacy sensitive system. ***Any privacy sensitive data stored on the GII must be vetted through the System Owner, ISSO and PMO. If a PTA is required, it will have to be drafted and routed to the Privacy Office for approval.*** If a development team wants to store privacy sensitive data on the GII, the onus is on this team to get permission from their Component or organization Privacy Office via a Privacy Threshold Analysis (PTA) and work with the GII ISSO to route the PTA through the appropriate channels. It is recommended that the development team justify gathering this information based on their mission needs.

From a security standpoint, the GII has a FIPS 199 rating of High, High, Moderate for confidentiality, integrity, and availability respectively. HSIN is also used to authenticate the user to Portal. HSIN provides secure integration and interoperability of information-sharing resources within the Homeland Security enterprise.

For more information on privacy and security, as it directly relates to development or integration with the GII, refer to the ***GMO Contact Information.***

References for more information on working with this geospatial web service.

3.9.1 WMS

A standard protocol for serving georeferenced map images over the internet that are generated from a map server using data from a GIS database. It’s important to note that with a WMS, you are essentially getting an image of geospatial data (i.e. JPG, GIF, PNG file). While this has its uses, it is an image only, and therefore does not contain any of the underlying geospatial data that was used to create the image. Refer to ***GMO*** Contact Information

Contact the GMO at DHS_GCOE@hq.dhs.gov for any additional questions or information.

3.10 Privacy and Security

All development teams using the GII must adhere to all privacy and security policies for the DHS. The GII is a non-privacy sensitive system. ***Any privacy sensitive data stored on the GII must be vetted through the System Owner, ISSO and PMO. If a PTA is required, it will have to be drafted and routed to the Privacy Office for approval.*** If a development team wants to store privacy sensitive data on the GII, the onus is on this team to get permission from their Component or organization Privacy Office via a Privacy Threshold Analysis (PTA) and work with the GII ISSO to route the PTA through the appropriate channels. It is recommended that the development team justify gathering this information based on their mission needs.

From a security standpoint, the GII has a FIPS 199 rating of High, High, Moderate for confidentiality, integrity, and availability respectively. HSIN is also used to authenticate the user to Portal. HSIN provides secure integration and interoperability of information-sharing resources within the Homeland Security enterprise.

For more information on privacy and security, as it directly relates to development or integration with the GII, refer to the ***GMO Contact Information.***

References for more information on working with this geospatial web service.

3.10.1 WFS

A standard protocol for serving geographical features across the web using platform-independent calls. A WFS can be thought of as the vector geospatial data behind a map. Using a WFS, you can pull distinct records from each point, line, or polygon associated with a given service. Refer to ***GMO*** Contact Information
Contact the GMO at DHS_GCOE@hq.dhs.gov for any additional questions or information.

3.11 Privacy and Security

All development teams using the GII must adhere to all privacy and security policies for the DHS. The GII is a non-privacy sensitive system. ***Any privacy sensitive data stored on the GII must be vetted through the System Owner, ISSO and PMO. If a PTA is required, it will have to be drafted and routed to the Privacy Office for approval.*** If a development team wants to store privacy sensitive data on the GII, the onus is on this team to get permission from their Component or organization Privacy Office via a Privacy Threshold Analysis (PTA) and work with the GII ISSO to route the PTA through the appropriate channels. It is recommended that the development team justify gathering this information based on their mission needs.

From a security standpoint, the GII has a FIPS 199 rating of High, High, Moderate for confidentiality, integrity, and availability respectively. HSIN is also used to authenticate the user to Portal. HSIN provides secure integration and interoperability of information-sharing resources within the Homeland Security enterprise.

For more information on privacy and security, as it directly relates to development or integration with the GII, refer to the ***GMO Contact Information.***

References for more information on working with this geospatial web service.

4 SUMMARY

This document is intended to provide guidance to development teams in other DHS components or organizations on the GII geospatial applications and services available for use as is or for customization in order to meet a mission need. The GMO GII team is available to provide guidance and recommendations to other development teams or organizations on the best way to implement a mission need. Refer to the ***GMO Contact Information*** in order to get in touch with the GII team.

As a reminder, any component or organization developing or integrating with the GII application or its services is responsible for ensuring privacy and security based on all DHS policies. Refer to ***Privacy and Security*** for more information.