Geospatial XD System (GXDS)

Features and Benefits

- **Request data between different network classifications**

- **Obtain data in seconds rather than days**

- **Significantly reduce the costs of copying and storing data**

- **Compliant to Open Geospatial Consortium standards**

The Geospatial Cross Domain System (GXDS) enables users on higher classified networks to request data from lower classified repositories up to their respective network levels in near real-time. The feature can be applied to a variety of Intelligence, Surveillance, and Reconnaissance (ISR) data types, including commercial satellite imagery. ISR datasets, including map points, streets, and biometrics can be overlayed on each other and combined with other data sources from multiple networks.

GXDS has been developed to meet Intelligence Community requirements for LIDAR and other unclassified ISR data retrievable by SIPRNet and JWICS users from a single device on the higher classified network. SIPRNet and JWICS users can look at catalogs of unclassified LIDAR, ISR, and commercial data pulling up only the data they require to their respective classified networks for analysis, targeting, and overlaying with classified data sets.

Designed to operate using Open Geospatial Consortium (OGC) standard service calls, the data can be viewed and processed by clients and Geographic Information Systems (GIS), including Google Earth, ArcGIS, and QGIS, PlanetGIS Explorer and many others. GXDS can also provide cross-domain connectivity to several other products, including servers from ESRI, DigitalGlobe, Pixia, Planet, Terra Bella, Terra Pixel, Vricon and others.

Copying PetaBytes or YataBytes of data to multiple networks takes a considerable amount of time, dedicated hardware, and personnel. GXDS automates this process by enabling analysts on higher classified networks to request the massive amounts of commercial and unclassified data from lower classified repositories up to their respective network levels. The requested data can then be cached and made available to analysts for the duration it is required or that days hotspot.

Users can work from one classified network to obtain the required data they need in seconds rather than days, and administrators can significantly reduce the costs of copying and storing all of the data to multiple networks.

GXDS has adapted cross-domain technology to demonstrate this ability through a secure bidirectional set of cross-domain guards between unclassified networks and both Secret and TS/SCI networks. GXDS utilizes an Open Geospatial Consortium standard of web service requests to inspect the metadata, visually browse it, and retrieve the desired data. Setting up the architecture in this way restricts all traffic across the GXDS to strictly OGC web service calls and data.

The implementation of OGC standard service calls, used by GeoNetwork applications on the classified side, makes use of its harvesting capabilities to issue periodic requests to the GeoServer repository on the unclassified side. The GeoServer software allows the secure sharing and editing of geospatial data, and GeoNetwork applications to provide a defined set of search and discovery tools. GeoNetwork applications issue requests to the GeoServer repository and stores the retrieved metadata in its catalogs. When a high side user discovers a dataset in the catalogs of interest, the OGC client they are using will issue requests via the GXDS to the GeoServer repository, which sends back the requested data.

Data flow between the security domains, via the GXDS, occurs in the following way:

- Secret or TS/SCI users will log on to their terminal and connect to the GeoNetwork application.
- An operation request for a catalog of the data, with an OGC call, is sent to the GXDS. The OGC request is validated before being moved across a one-way data diode utilizing Cubic's XD Guard technology. The OGC request is redundantly validated before it is sent to an approved GeoServer repository for processing.
- The GeoServer repository processes the request and sends the requested results back to the GXDS.
- The data sent to the GXDS is validated before being moved across a different one-way data diode utilizing Cubic's XD Guard technology. The requested data is redundantly validated before it is sent back to the requesting user on the classified network.

The GXDS feature supports the following OGC compliant calls:

- Web Map (Tile) Service (WMS/WMTS)
- Web Feature Service (WFS)
- Web Coverage Service (WCS)

Cubic Mission Solutions
cubic.com/ruggedIoT

21580 Beaumeade Circle #230
Ashburn, VA 20147

Tel: +1 (571) 258-5020

CMS-GXDS-18JUNE2020