

# Cross Domain Spatial Data Infrastructure

## Solutions Paper

# Cross Domain Spatial Data Infrastructure

## Business Problem

For years, the same spatial data has been repeatedly replicated and hosted on multiple security domains so that users with different clearances could access it. This has led to complicated and costly schemes for upward and downward synchronization of data. Moreover, it has required the acquisition of multiple hardware and software instances, for which each require individual operations and maintenance (O&M) budget.

## Interoperable Solution

The emergence of label secure database technology, sophisticated high assurance security appliances as well as changes in security policy now make it possible to avoid such costly implementations, which drastically reduce mission latency. Ultimately, this brings more timely data to operators, targeteers, analysts and support personnel.

ERDAS' Enterprise line of Open Geospatial Consortium (OGC) compliant web services has been specially designed to support Oracle Label Security, and thereby Oracle's Cross Domain Security Solution (CDSS). The CDSS is in process for a DCID 6/3 PL4 by the Joint Cross Domain Management Office. This label secure environment enables data of different classifications to reside in the same database, enabling users with different roles and clearance levels to access the same database, and only the data needed, according to their security clearances.

## User Scenarios

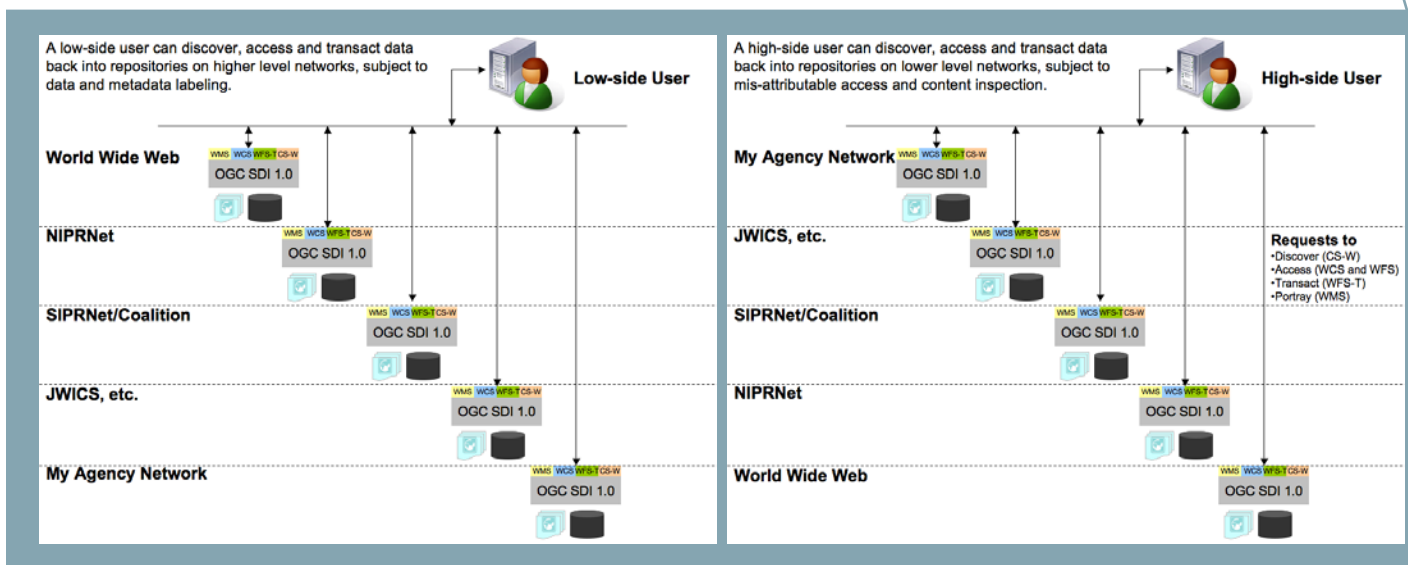
ERDAS' Cross Domain Spatial Data Infrastructure solution allows four distinct user scenarios:

- **Reach Down** A client application or user on a high-side network transparently requests data from a low-side web service.
- **Transact Down** A client application or user on a high-side network transacts data from the high-side via a low-side web service into a low-side database.
- **Reach Up** A client application or user on a low-side network requests data from a low-side web service fronting a high-side, label-aware database.
- **Transact Up** A client application or user on a low-side network transacts data via a low-side web service into a high-side, label-aware database.

ERDAS' web services support for label secure database solutions, such as CDSS, make user cases Reach Up and Transact Up possible. However, additional technologies are necessary to accomplish user cases Reach Down and Transact Down. ERDAS' Cross Domain Spatial Data Infrastructure leverages its OGC compliant web services and support for Oracle Label Security, within the larger context of Safe Harbor Systems' Common Cross Domain Framework (CCDF) [available upon request]. A constellation of high assurance technologies enables users to transparently consume geospatial data from any network, subject to the classification of the data and the target network.

CCDF utilizes a controlled interface acting as a proxy between two networks, allowing auditable, transparent access by paired, known identities on either network. Furthermore, CCDF can process data from a cross-domain enabled database. In this instance, CCDF makes use of Oracle's CDSS to store and protect data. The CCDF databases will label content with the appropriate classification label.

As connections to the database are being established, environmental factors will be taken into consideration to determine access and release of the stored content. For example, in the Reach Up and Transact Up cases, only data for the same classification as the network being accessed from will be retrieved from the database; regardless of the user's clearance. That is, if a user with Secret clearance is accessing data on a TS system, then only Secret data will be returned from the database.



In a High-to-Low scenario, a 'reverse proxy' technique is utilized. Proxy and reverse proxy are mirror images for what they are intended to protect. For a proxy environment, a controlled interface acts on behalf of a network client. A low side identity or address is mapped to a high side identity or address. This technique is important for the Low-to-High user case. In contrast, the reverse proxy acts on behalf of the server. The reverse proxy will not map a high side IP address or user identity; rather it will send an attributable low side IP address acting in surrogate. The result is identity obfuscation of the originator, be it application or human user. Auditing is still accomplished on both sides and can be correlated for forensic purposes.

### Contact Us

If you are interested in architecting and deploying a cross-domain spatial data infrastructure, contact ERDAS Defense Solutions today: [defense@erdas.com](mailto:defense@erdas.com), +1 703 354 7415.