



Cross Domain Information Sharing (CDIS)

Overview

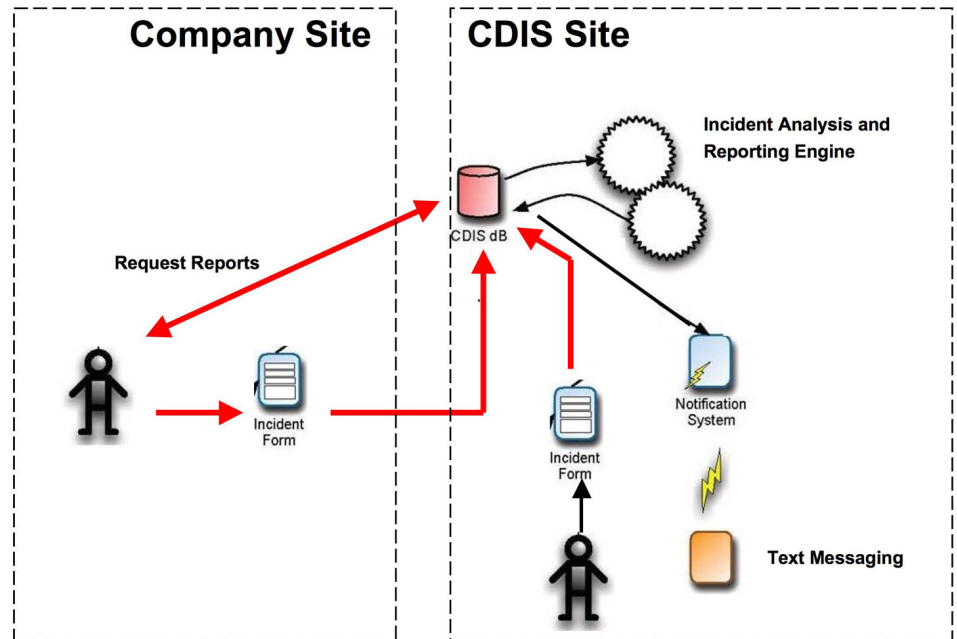
Cross Domain Information Sharing (CDIS) is a proof of concept capability for reporting and analyzing Process Control System (PCS) incident data. CDIS addresses a critical need within the PCS community – enabling centralized reporting and analysis of incident data to facilitate early warning and coordinated response to cyber attacks on the nation’s critical infrastructure. The CDIS architecture is flexible enough to accommodate different Asset Owner reporting models and a range of incident analyses, enabling Asset Owners to measure PCS security return on investment.

CDIS Philosophy

- Administration of a central repository of incident information is best handled by a trusted third party
- A flexible reporting architecture is necessary to
 - Accommodate Asset Owners’ existing reporting systems and processes
 - Enable varying degrees of Asset Owner participation
- Asset Owners retain local control over information release decisions

Key Concepts

- **Anonymous Authenticated Communication**
 - Among authorized Asset Owners
 - Reporting without attribution
 - Privacy over the wire
- **Incident Reporting**
 - Electronic reporting to a central database
 - Asset Owners maintain local control over information release
- **Incident Analysis and Reporting**
 - Statistical analyses
 - Incident trending
- **Notification and Early Warning**
 - SMS-based messaging service
 - Alerting for critical infrastructure events



Denotes use of anonymous authenticated communication

Researcher Contact Information



Chris Eliopoulos
celiopou@mitre.org
 (781) 271-3625

About MITRE

In partnership with government clients, MITRE is a not-for-profit corporation working in the public interest. It addresses issues of critical national importance, combining systems engineering and information technology to develop innovative solutions that make a difference. It operates federally funded research and development centers for the DOD, the FAA, and the IRS, with principal locations in Bedford, Massachusetts, and Northern Virginia.

This work was supported under Award number 2003-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

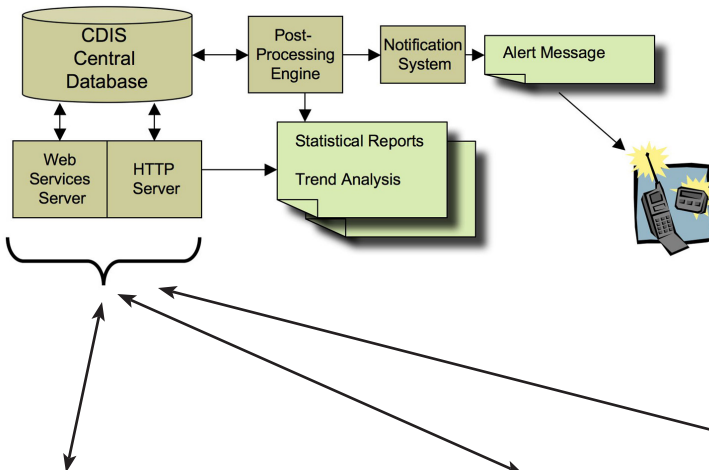
Functional Description

The CDIS site maintains a central repository of PCS incident information. Access to the site will be granted to authorized users to facilitate the electronic sharing of information in an anonymous, yet authenticated way. Preserving anonymity in this environment is critical for protecting Asset Owners' reputations and shielding the bottom line from the potential ill effects of a well-publicized incident. Data is reported to the site anonymously through the use of crypto-based authentication technology developed at Sandia National Labs.

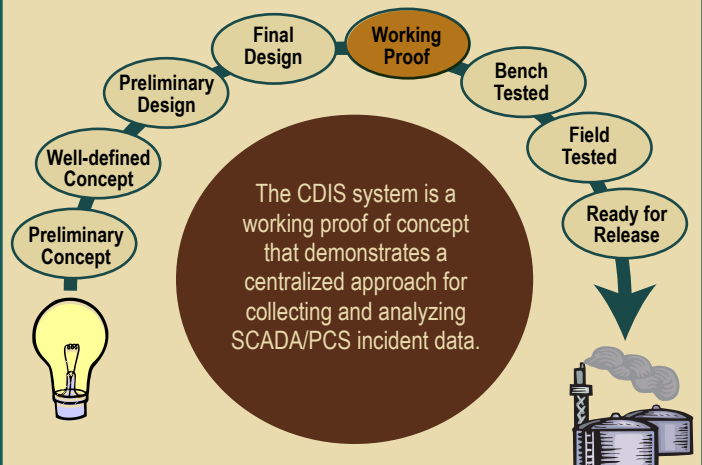
CDIS enables incident reporting via web-based forms on which users can enter information about breaches in physical security, suspected cyber attacks and their effects, as well as system status and outages. Data can also be fed from existing corporate incident databases and filtered according to site security policy before being published to the CDIS central database.

Aggregate data, depicted graphically, will show basic infrastructure status and enable Asset Owners to gather statistical information on recent incident activity. This technology, developed by Dartmouth College, is also capable of identifying trends in incident activity that could be useful in determining return on investment for PCS security or indicating a widespread infrastructure attack.

The CDIS notification service, an SMS-based messaging capability, can be used to alert users to critical infrastructure problems or attacks. Using this service, important information can be broadcast to the community in a timely manner.

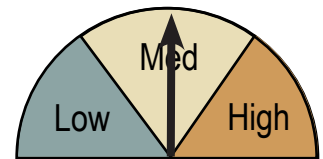


Technology Transfer and Readiness



The CDIS proof-of-concept demonstration contains software components developed by MITRE, Sandia National Labs, and Dartmouth College. Most of the software components can be provided to U.S. Government entities via a no-cost license. Non-governmental organizations can negotiate licenses; contact Chris Eliopoulos (celiopou@mitre.org, 781.271.3625) for more information.

Summary of Costs



	Low	Medium	High
Component	<\$1,000	\$1,000-\$10,000	>\$10,000
Engineering	Drop-in	Moderate modification	Complete System Design Lifecycle
Bandwidth/Network Burden	None-Passive Only	Moderate Traffic, Medium Overhead	Heavy Traffic, Large Overhead
Training	No training required	Moderate training	Intensive training, additional staffing may be required
Maintenance and Operation	< 1 hour per week	< 5 hours per week	> 5 hours per week

