Sharing Information Today: Maritime Domain Awareness

Michael Todd
Defense Information Systems Agency

In a world where unforeseen human or natural disasters (i.e., U.S.S. Cole, September 11, Hurricane Katrina, the 2004 Indian Ocean tsunami, and the possibility of an avian flu pandemic) may occur, interagency information sharing and collaboration is essential to mitigating effects of these types of catastrophic events. The Maritime Domain Awareness Data Sharing Community of Interest (MDA DS COI) pilot demonstrated a net-centric data sharing capability as a first step towards addressing the common challenge of global identification and tracking of maritime vessels, cargo, and crew usage of existing information sources to better secure our coasts, ports, and waterways. This Department of Defense (DoD), Department of Homeland Security (DHS), and Department of Transportation (DOT) partnership developed capabilities to expose maritime data as a consumable Web-enabled service to authorized, unanticipated users employing community-based agreements defining a common vocabulary and data sharing services. This COI pilot also leveraged enterprise services resulting in a repeatable process, an extensible vocabulary, and reusable services available for developing responsive, agile solutions for any number of data sharing challenges.

The MDA DS COI pilot demonstrated the capability for three federal departments (DoD, DHS, and DoT) to share maritime vessel tracking data so that analysts and policing officials in all three departments will have the ability to exploit information they did not previously have. This mission is in direct response to objectives framed by the National Security Presidential Directive 41 and Homeland Security Presidential Directive 13 to improve maritime domain awareness of global threats to national and maritime security.

The MDA DS COI pilot also addressed information sharing objectives identified in the 2006 Quadrennial Defense Review (QDR), institutionalizing the ongoing transformation of the DoD. Specifically, it identified the approach taken to meet the National Defense Strategy requirement to enable net-centric operations. Section three of the document discussed the reorientation of capabilities and forces and identified actions to be taken to achieve net-centricity. That is, access to information, information sharing, and collaboration among those who need it. The QDR specifically requires the DoD to strengthen its data strategy.

The DoD Net-Centric Data Strategy establishes the policy approach to ensure information can be shared across the enterprise in a trusted and timely manner. Implementation is well under way. Today, it delivers capability as part of pilot initiatives developed by communities with specific information sharing needs. A net-centric COI develops capabilities to expose data as a consumable, Web-enabled service to *authorized unanticipated users employing community-based agreements defining a data sharing vocabulary and services*. The community-based agreements and their descriptions are published to discoverable registries where known and unanticipated authorized users may adopt or extend the agreements to meet additional mission-related data sharing requirements.

The MDA DS COI pilot addressed the cultural and technical challenges for multiple federal departments to come to agreements on how to improve awareness of potential security or defense related threats from maritime vessels, cargo, or crews. The cultural challenge focused on the need for data producers to share data with users with a right to use the data. This replaces the previous need-to-know paradigm that mitigated data being discovered and used by authorized unanticipated users. The cultural shift places a priority on trust and collaboration in a risk-managed data sharing environment. This is promoted by Executive Order 13388, directing improvements for sharing intelligence data and data sharing recommendations after the September 11th attack. Additionally, this effort faced the need for different federal departments to collaborate in defining their shared challenges, agree on a governance process to manage the effort, share resources needed (in the middle of a budget year without prior planning for this effort), come to agreement on a common vocabulary, and share lessons learned as the engineering teams developed the applications across four different data producer sites with different architectures. The key here is the COI was truly a community effort. The DoD Chief Information Officer (CIO) team met with each of the primary stakeholders to discuss the lack of visibility into data collected by other organizations and proposed the community-base approach to develop the vocabulary agreements and share in the engineering efforts. Each agreed this was a high priority problem and that the proposed COI-based process offered an opportunity to solve the problem relatively quickly. The DoD CIO team made recommendations based on an existing problem each COI participant already understood but had not come together to address before. Once the executive leadership determined this to be a priority effort and the staff understood the strategy, the effort was enthusiastically supported. DoD CIO team offered guidance as needed but did not lead the effort. The COI belonged to the community of organizations who would benefit from the effort. This commitment on the part of the COI members helped to ensure they understood the process and the benefits.

The technical challenge focused on moving from producer-to-user point-to-point interfaces, to producers posting data, services, and their descriptions to shared spaces that are discoverable and accessible by known and unanticipated authorized users. The value of networks and therefore collaboration increases as the number of participants increases. However, in the point-to-point design this becomes costly to manage and difficult to evolve. The use of shared spaces to host standard-based data assets and services scales in a more cost effective manner, meeting planned and unexpected mission needs. In addition to using shared spaces to offer data assets, a set of core enterprise services were made available as well. Offering the use of the DoD's Net-Centric Enterprise Services (NCES) Early Capability Baseline (ECB) release of enterprise services helped seal the agreements. Leveraging the NCES ECBs for security, messaging, and content discovery services meant the different

organizations did not have to reinvent these capabilities duplicating the cost, time, and risk. It also meant that all were interoperable and could use common interface standards. The key here is the pilot development and demonstration proved in real terms that reuse of enterprise services can work across technical and organizational domains.

The MDA DS COI was formed as a cross-functional and organizationally diverse community that was experiencing a data sharing problem. The COI defined the problem as a single statement and identified a limited number of data sources to expose as a consumable service for the initial pilot. The initial effort was scoped for a nine-to-12-month effort to rapidly develop the needed capability. The community adopted existing data standards in the development of semantic and structural agreements (extensible metadata schemas) to facilitate the understanding of the data by human or machine data users. Application-level services were developed using this community vocabulary to Web-enable legacy capabilities and commercial browsers to make the data visible and accessible in a trusted data sharing environment. Foundation level services adopted existing enterprise services from the DoD's NCES ECB, and the DHS's Homeland Security Information Network (HSIN). These enterprise services are designed for reuse across the respective enterprise, mitigating duplicative investments and reducing individual program risk, while enabling consistent performance similar to a public utility in the commercial sense.

The MDA DS COI documented the pilot effort as a repeatable process that resulted in successful demonstrations of the discovery and access to data from four functionally and geographically separate data producers within eight months. The repeatable process continues to evolve as it is shared with other COIs and in follow-on spirals for the MDA DS COI. The documented process and lessons learned are being consolidated and will be posted for additional use. The strategy is simple:

1. Define a data sharing problem among an operational community.
2. Gain leadership support and staff buy-in for the means of solving the problem as a community.
3. Develop the semantic and structural agreements for a common vocabulary all will agree on as the means of understanding and exchanging the data, (avoid selecting more than a dozen data sources to manage the risk and scope of the effort).
4. Adopt existing services as the technical means of sharing the data are developed.
5. Buy or create the services needed if no partial or complete services already exist.
6. Register the vocabulary and services in enterprise visible and accessible registries for follow-on use.
7. Demonstrate the working capability and market as a risk reduction for programs associated with sharing the same types of data, (this works even better if those programs participate in the pilot deriving direct benefit from the effort).
8. Document all of the lessons in the process for future use by this and other teams.
9. Post assets for general discovery, understanding, and use (vocabulary, services, repeatable process).

The execution of a successful pilot like this requires a strong, cooperative team and committed leadership support. This eight-month effort took between 60 and 90 days to develop the agreements on the problem set, resources needed, vocabulary and schema development, and the services needed. The development of Web-services leveraging the NCES ECBs and the HSIN became progressively easier, taking far less time with each subsequent implementation across the four data producer sites involved. Milestones were measured in days and weeks rather than months and years overall. As was stated before, the MDA DS COI team was enthusiastic in the pursuit of their goals sharing a clear understanding of the importance and benefits of working together as a team. Obstacles such as parochial ownership of needed assets were resolved quickly and the team was able to deliver.

The piloted capability demonstrated is available for limited use at this time. The pilot leveraged an early release of the NCES program that is under development. This in turn proved the value of the NCES effort to deliver a service-based infrastructure for reuse by DoD and other departments. As COIs apply the rapid development cycles and continue producing more user services and the NCES infrastructure adds more robust capabilities, this will be made available to a broader user community. Currently, the NCES program is approved for a limited operational support while developing at a rapid pace. The MDA DS COI and others are signing up to extend the initial success cited here implementing the Net-Centric Data Strategy and leveraging NCES (which increases the value of the NCES investment while reducing the cost to the DoD overall). Engineering lessons learned by the COIs are fed back into the NCES effort, providing further user guidance for the evolution of this enterprise program.

The demonstration allows a user to define their operational picture in near real time using live data feeds. The new MDA DS COI data sharing capability is a first step towards addressing the common challenge of global identification and tracking of maritime vessels, cargo, and crew using existing information sources to better secure our coasts, ports, and waterways. The successful eight-month pilot demonstrated proof of the DoD Net-Centric Data Strategy and implementation of an enterprise service-based architecture. COI members are studying means of applying the extensible data sharing capability in future spiral deliveries of operational programs supporting operational missions. The community is also exploring additional data sharing priorities to further improve global maritime domain awareness supporting the national defense and homeland security missions of the DoD, DHS, and DOT.

In a world where unforeseen human or natural disasters (i.e., U.S.S. Cole attack, September 11, Hurricane Katrina, and the 2004 Indian Ocean tsunami), may occur, this means of improving responsiveness and ability to develop solutions for data sharing needs is a critical solution for any number of data sharing challenges.◆

About the Author

Michael Todd is an advocate for the net-centric revolution across the DoD and its strategic partners. He is currently supporting DISA's NCES Program Office. His most recent accomplishment was to provide DoD CIO policy guidance and stewardship for the successful Maritime Domain Awareness Data Sharing Community of Interest pilot during 2006. Todd is a 1998 graduate of the Advanced Management Program at the National Defense University where he received his CIO and Information Resource Management Certifications.

DISA
ATTN: Mike Todd PEO-GES
PO Box 4502
Arlington, VA 22204-4502
Phone: (703) 882-0420
Fax: (703) 602-0830
E-mail: michael.todd@disa.mil