

DIGITAL dialogue

Facilitating the National Security Challenge of Cross-Domain Information Sharing

Speaker



Marianne Bailey,
Director of the Unified
Cross Domain
Management Office

Moderator

Rutrell Yasin,
GCN Senior
Technology Editor,
1105 Government
Information Group

"This Digital Dialogue does not imply endorsement or support by eSeminar participants of any product, service, or offering."

The following are highlights from the April 14, 2010 eSeminar entitled "The National Security Challenge: Cross-Domain Information Sharing."

The Unified Cross Domain Management Office opens up channels and promotes information flow to help achieve missions

One of the most pressing issues facing the intelligence community today is cross-domain information sharing. Due to current world events, mandates, and conflicts, there is an unprecedented need to share information among agencies and with other governments; yet connecting IT systems to facilitate this sharing exposes vulnerabilities that raise concerns and stymie progress. Organizations are left to grapple with how to allow other agencies and governments into their networks to access the data they need to complete their mission, while protecting the rest of the data on their networks from unauthorized access. This has become increasingly difficult in today's world where adversaries grow more sophisticated each day, and the technology environment that must be protected grows more and more complex.

In 2005, the U.S. Department of Defense (DoD) and the Intelligence Community (IC) commissioned a study to determine how their organizations were dealing with the issue of cross-domain information sharing. The study determined that there was a lack of leadership; commands and services were left on their own to figure out how to manage the issues of developing, testing, funding, sustaining, supporting, and avoiding duplication regarding information sharing.

As a result, the Unified Cross Domain Management Office (UCDMO) was established in July 2006 to deal with the complexity and sensitivity around cross-domain information sharing, as well as manage the logistical, technological, political, and cultural aspects of

linking networks and exchanging data.

"Today we have this incredible need to share information," says Marianne Bailey, director of UCDMO. "A lot of times when you hear that things aren't working as they should in the government, people will cite information sharing as one of the major downfalls."

UCDMO was established to manage cross-domain efforts across the DoD and IC, with Bailey, its director, reporting to the CIOs of both organizations. An oversight panel also was created, comprised of DoD service-level CIOs and technology executives from the IC, to offer advice and guidance to the office. In addition to establishing secure cross-domain access to, and sharing of, timely and trusted information, the UCDMO also was chartered with creating a seamless enterprise infrastructure that would enable and protect data sharing.

Since its inception in 2006, the UCDMO has been working to achieve four goals: To deliver the capabilities required to support a secure and integrated information enterprise; to mitigate risk by enabling global awareness of cross-domain operational connections; to maximize return on cross-domain investments, while reducing duplicated efforts and increasing the efficiency of cross-domain activities. It also aims to provide leadership across the interagency spectrum to ensure coordinated cross-domain governance, oversight, and community reciprocity.

Deliver Capabilities

The UCDMO facilitates the development of extensible cross-domain technology capabilities

that create an enterprise foundation for information sharing. The more information-sharing capabilities that can be tied into this enterprise architecture the better, since a unified foundation is more likely to allow for reuse of technology and testing, as well as standardized implementations of capabilities. The office looks at enterprise services as a whole – be it e-mail or Web browsing – and examines how to enable them for cross-domain information sharing. Such services could access different networks and pull information from them without the user having to know where the data was stored or which network it was on.

The UCDMO has a senior technology architect on staff to look at the enterprise capabilities from the DoD and the IC and combine and leverage them where appropriate. The enterprise working group looks at the challenges organizations are facing today, near term, and in the more-distant future.

Realizing that not all cross-domain functions will be able to take advantage of this enterprise architecture – such as operations at the edge of networks with limited bandwidth or tactical solutions that are built on the fly – the UCDMO also works to provide point solutions for cross-domain information sharing as well.

“Some of our customers have niche, or one-off, requirements based on their mission, so we will always have point solutions in bandwidth-constrained or niche areas,” says Bailey. “But we expect the enterprise to provide a significant amount” of capability. The UCDMO maintains close partnerships with commercial technology vendors and gets involved in user forums to highlight new and emerging technologies that could be integrated into the enterprise architecture.

Another important function of the UCDMO is to develop unified processes and methods around cross-domain information sharing so that everything is done the same way across organizations, therefore facilitating reuse that can save resources and money. However, development of common processes requires common standards; one example that UCDMO is currently working with is the National Institute for Standards and Technology’s 800-53 set of security controls that are designed to ensure the security of government cross-domain systems. The community that UCDMO serves has been working with the security controls and developing testing methods against them, and the office hopes to roll

out these controls this summer. Such standards offer users of the technology a common process that is much easier to achieve than attempting to harmonize them once they are already built.

It also has created a list of baseline products – currently numbering 17 – that the office is confident have been properly developed and tested to meet specific needs, and the office also provides test data and lifecycle support for those products. Being able to test cross-domain information sharing technologies just once, instead of multiple times due to multiple implementations by different organizations, will represent a significant cost savings, since it costs on average \$300,000 to \$500,000 to certify such technology.

Also, in the case of old operating systems or other legacy technologies that are still being used, the UCDMO creates a sunset list of technologies that should be phased out, giving the community two years to do so.

“When we sunset something we make sure other capabilities are available, so a customer doesn’t take something off inventory when there isn’t something better to replace it with,” says Bailey. “We’re constantly looking at the lifecycle evaluation process and how can we make that better.”

The office also hosts Developer Days, where a panel of subject-matter experts come together to discuss a new cross-domain information sharing capability, to assess the need for it, and discover if the capability is already under development. Cross-domain technology can take a very long time to develop and test, so the UCDMO aims to work with developers throughout the process and try to get in front of the cycle, identifying where gaps in the enterprise architecture are today and where they might be down the road. Once a capability is flagged as something that is indeed needed, the UCDMO works to get the development funded and speed the acquisition cycle, which typically in the government is fairly slow.

One reason why the UCDMO is chartered with overseeing the logistics of cross-domain information sharing is not because these connections don’t exist today, but because connections typically have not been developed in a standardized manner that takes into account the surrounding environment.

“In reality, we are really vastly connected, even hyper-connected,” Bailey says. “Pick any network and any agency

Information Sharing

that resides on it and look at their mission and who they are interconnected with, and you'll find out there are hundreds of interconnections. The problem is it hasn't been done in any great, strategic way, but mission-by-mission. No one has looked at a better way to do this; instead everyone goes out and gets their own connections using different technologies."

And, one of the biggest problems created by non-standardized connections is that it opens up the possibility for cyber attack.

Mitigate Risk

Another portion of the UCDMO's charter is to provide a layer of defense for network protection. Connections established between different security levels must meet three needs: Information sharing to provide warfighters and intelligence operators with the data they need; information protection to secure sensitive data from unauthorized access, manipulation, and leakage, and network protection to safeguard networks from corruption by malicious code.

"Cross-domain solutions have to enable information sharing, but also have to protect information from unauthorized access. When you're connecting multiple networks you have to make sure only the data you want to transfer is transferred, and that no one can access the other information or even the other networks if you don't want them to," explains Bailey. "It's also protecting networks from corruption and malicious code, and making sure nothing is leaked out. To some it might sound easy, but it's very difficult."

The security of these connections grows more important as adversaries become more sophisticated. For example, in a typical network today, the high volume of bots (malware code that remains largely undetected until a central controller gives them a task such as stealing information from the network or infecting other PCs) illustrates the ability of adversaries to infiltrate networks. Often it's these type of connection points that become the weakest link and the entry point for malware to infect a network. "These cross-domain connections are the nuggets that people would love to get at," says Bailey.

Oversee Resources

The UCDMO also acts as a facilitator to ensure that there is no duplication of efforts in developing new technology for information sharing, and that when money is spent on new

technology, the groups are getting the most for their dollars. This includes gaining an understanding of the tremendous amount of research and development going on today to help facilitate communication, as well as what technology initiatives already have been developed and are moving into the testing phase and those that are ready to be deployed on a network.

In order to help corral all the ongoing initiatives and uncover unmet needs, the UCDMO performs gap analyses and writes policies and procedures that would fill those gaps and fix the problems for the entire community. It also attempts to target new research at those areas in need of solutions.

Provide Leadership

The UCDMO is also the champion of reciprocity in the cross-domain information sharing efforts, encouraging one group to give up an asset that they can control and move it into the enterprise architecture for cross-domain information sharing, allowing another group to take advantage of it. According to Bailey, this responsibility is also the top challenge that the UCDMO faces, due to the cultural issues surrounding it.

"It's amazing that we still have folks out there who say 'that's not my way' and don't trust the community. That's why we have a lot of duplication," Bailey says. However, she adds that she is also seeing a lot of progress in this area of late, where organizations are using solutions that were developed in another organization. And she finds that organizations first will look at the baseline technologies that UCDMO has approved to fill a need, and if they can't find what they are looking for, they'll consider developing their own solution. The UCDMO is working on a baseline memo that would say if an organization can't make use of one of the 17 technologies for a project, it will have to justify why it can't and explain the reasons to the joint community.

Another responsibility is governance, which is achieved largely through influence and collaboration with the technology executives among different groups to convince their IT staffs that the UCDMO's directives should be followed.

When problems arise, UCDMO moves quickly to solve them. For example, the office has established a number of working groups that are focused on solving specific problems related to cross-domain support services or agencies pushing

technologies down into their organization.

“We’ve had some very engaging and heated conversations, people are passionate about coming to a resolution where everyone agrees,” says Bailey. “We can push out gaps we see in our baseline with capabilities that exist today, and small teams can resolve issues.”

Real-World Example

Bailey offers the example of the current Afghanistan/Pakistan theatre as a case study of how cross-domain information sharing helps to achieve goals. In this theatre, many networks have been established so that each invested party can achieve their goals. Bailey uses the metaphor of young children playing soccer, where everyone runs after the ball at once. These networks have been moved from their host environments – such as NATO and European countries – into this theatre, where resources are severely constrained. Not only is bandwidth limited, but human resources also are strained, as people who typically do one job end up taking on four. Best practices break down, and operators resort to measures such as transferring data on CDs, which isn’t only inefficient and insecure, but also usually means someone is doing a task that they weren’t sent there to do.

A tiered approach has been developed in the Afghanistan/Pakistan theatre, so that large, enterprise global centers are the first tier of operations, followed by a second tier of tactical enterprise operations. The third-tier is being made up of point solutions for bandwidth-constricted environments, which rely on some existing capabilities.

“Everyone is very happy with the progress we’re making in communications,” says Bailey. “It’s a cultural shift, we have to re-look at how we provide support to major operations like this.”

Beyond DOD and IC

The UCDMO is looking beyond the DOD and IC to discover how it can facilitate cross-domain information sharing in other areas, such as when disaster hits a given community. In those

cases, making it easier for the National Guard, state and local governments to share information could help avoid mistakes that were made in the past, such as with Hurricane Katrina. By utilizing technologies and capabilities that allow certain workers into certain areas while cordoning off other parts of networks, information could flow much easier among entities. Best-of-class commercial technology such as virtual private networks combined with high-assurance capabilities could allow for the necessary access and separation of all partners involved, while sharing all the information that needs to be shared.

In support of such goals, UCDMO has asked to expand its mission from managing pure cross-domain, high-assurance devices between networks to a greater information-sharing space.

“Pulling the pieces together is really the job – making sure the linkages happen and the strategy is in place,” says Bailey, “so we’re moving in the right direction to take advantage of all the capabilities and talents that exist...to solve the problem.”

SecureOffice® cross domain products, from Trusted Computer Solutions, are installed and accredited in operational systems around the world. These solutions arm the warfighter with easy-to-use applications enabling secure access to information on multiple classified networks, the transfer of information between networks, and the ability to operate on multiple networks from a single device.

Trusted Thin Client® – provides secure access to multiple classified networks from a single desktop; supporting a thin client device, virtual access within a workstation, and remote access through a secure operating system and virtual machine run from an encrypted thumb drive.

Trusted Gateway System™ – enables secure bi-directional transfer of files and data from multiple networks at different classification levels.

WebShield™ – allows secure browse-down and information retrieval between classification levels.

With over 16 years developing and supporting cross domain solutions, TCS today has the most solutions on the UCDMO Reuse Baseline list.



Visit: www.TrustedCS.com
or call 1.866.230.1307

Content is from an April 14, 2010 eSeminar titled

“The National Security Challenge: Cross-Domain Information Sharing”.

Go to <http://gcn.com/webcasts/2010/04/fcw-cross-domain-info-sharing.aspx> for the complete transcript.
