

Cross-domain office aims for secure data sharing

Links pave the way for fuller and deeper intelligence insight

- By John Edwards
- Jul 28, 2011

In this era of growing security awareness and increasing security risk, government agencies need a reliable way of enhancing and streamlining information sharing while maintaining security barriers among various intelligence user groups and classifications.

Making sure that crucial information can flow unimpeded across security domains while vital secrets are preserved is the job of the Unified Cross Domain Management Office, located in Adelphi, Md.

UCDMO serves the Defense Department and intelligence community, a cooperative of 16 separate investigative and information analysis agencies, including the CIA, FBI, National Security Agency and Defense Intelligence Agency.

UCDMO helps DOD and intelligence community agencies find and acquire cross-domain solutions — controlled software or hardware interfaces that provide the capability to access or transfer information across different security domains, such as unclassified to secret, secret to top secret, and so on.

Bryan Topscher, eXMeritus program manager at Boeing Defense Space and Security, said cross-domain solutions tools, such as Boeing's eXMeritus HardwareWall, are designed to punch through inter-domain roadblocks that can prevent authorized individuals from viewing the critical intelligence they need to reach. "Information is produced at all levels of classification but often is produced above the classification where it is needed and in niches so specialized only a few persons can have access [to] it, regardless of clearance and need to know," he said. UCDMO aims to help DOD and intelligence community organizations deliver disparate chunks of intelligence to the individuals who can squeeze the maximum value of out them.

The need for an organization such as UCDMO became apparent in the days shortly after the 2001 terrorist attacks. As investigations were launched, DOD, intelligence, law enforcement and other officials quickly realized that individual governmental organizations held vital bits of information prior to the attacks, such as FBI reports of suspicious students at local flight schools. Had all the disparate pieces been put together, the combined intelligence might have alerted authorities to the terrorists' plan.

To ensure that such oversights would never happen again, Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 mandated the creation of an "environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties," laying the groundwork for UCDMO's creation. UCDMO was formally established in July 2006.

"You can argue that the UCDMO is the U.S government's formal organizational response to the tragedy of 9/11," said Ed Hammersla, chief operating officer of Raytheon Trusted Computer Solutions, based in Herndon, Va. The Raytheon unit supplies UCDMO with several different types of cross-domain solutions.

Setting the baseline

The core of UCDMO's mission is the UCDMO Baseline, a validated list of cross-domain tools that are available to DOD and intelligence organizations. "UCDMO has preselected and preapproved a set of information-sharing mechanisms that can be used and deployed and which will give instant benefit to the agencies that use them," Hammersla said. "The tools allow agencies to share information across networks so that they can know better how to analyze a threat and can put the pieces of a puzzle together more quickly to assess that threat." Despite the sensitivity of the information supported by cross-domain tools, the UCDMO Baseline is unclassified and can be viewed by anyone.

Most UCDMO Baseline technologies fall into one of two buckets, Hammersla said. "The first bucket is access solutions — something that allows you to access multiple networks but you're not permitted to move something from one network to another."

The other bucket consists of transfer solutions, also known as guards. “These are the mechanisms that allow you to move information from one network to another,” Hammersla said. “The high-speed guard, specifically, allows large quantities of data to be moved automatically from one network to another based on a preset list of conditions or rules.”

Although many people think of sensitive data only as text documents, UCDMO-listed tools actually support a wide range of media. Topscher noted that Boeing’s cross-domain solutions offering is designed to support a variety of file types. “HWW can transfer standard data files, such as Microsoft Office files, imagery and video,” he said. “There are many uses for the HardwareWall, including military applications in airborne and ground tactical units, as well as enterprise solutions.”

Although cross-domain solutions tools are designed to support information sharing, UCDMO considers itself a resource provider, not an adviser. “They tend to stay away from trying to recommend one solution over another because they would rather have the government agency make that decision on their own,” Hammersla said. “They tend to stay a bit agnostic to one solution over another, which is probably appropriate given their role.” UCDMO, which is currently awaiting a new director, was invited to participate in the research for this article, but declined.

Topscher noted that cross-domain solutions were already widely used long before UCDMO set up shop. “The individual agencies and departments each had their own lists of previously approved cross-domain solutions,” he said. “The goal of the UCDMO was to unify this redundancy and produce efficiencies in choosing a guard that had already had a proven track record.” In addition to Boeing and Raytheon, other UCDMO vendor partners include defense industry heavyweights such as BAE Systems, General Dynamics, and Northrop Grumman and smaller firms such as Owl Computing Technologies and Wind River Systems.

Since its inception, UCDMO has managed to reduce the number of approved cross-domain entities from more than 800 to a far more manageable baseline list of about a dozen key solutions and a handful of supporting technologies. “UCDMO has provided a real service to the DOD and the Intelligence Community,” Hammersla said.

Working relationships

UCDMO has close working relationships with virtually every government organization that has DOD or intelligence community ties, in addition to cross-domain vendors. “The UCDMO will provide a government point of contact to interested customers [and] the GPOC will then refer the interested customer to Boeing,” Hammersla said.

Annual conferences are another way UCDMO maintains close ties with vendors and DOD and intelligence community organizations. “It’s a three- or four-day affair where they bring in all the suppliers and they do presentations, briefs, demonstrations and that sort of thing,” Hammersla said. The next conference is scheduled to take place Aug. 1-4 in Chicago.

Hammersla said he believes that by helping DOD and intelligence community organizations study crucial intelligence faster and more completely without compromising security, UCDMO has played a major role in the war against terrorism. “They do a lot to assist the agencies in terms of solving this problem and being able to share information across security domains,” he said.

About the Author

John Edwards is a contributing writer for Defense Systems.



© 1996-2011 1105 Media, Inc. All Rights Reserved.