

Shaping Industry Interaction Through Secure Information Sharing

Part II: Collaborating to Improve Collaboration

Richard Skedd ■ Paul Grant

This is the second of a three-part series, "Shaping Industry Interaction Through Secure Information Sharing." Part I, published in the previous issue of Defense AT&L, examined the need for information sharing and collaboration among key aerospace and defense organizations and governments, including the Department of Defense; and the role of the Transglobal Secure Collaboration Program (TSCP) in meeting the need.

Part II examines the collaboration efforts of those involved to set industry-wide specifications for secure collaboration.

The benefits of secure collaboration have been dramatic for the Department of Defense, which is now looking at how to extend this value through global reach. However, extending global reach is a challenge with which DoD and other participants of the TSCP have been wrestling for nearly half a decade.

Striving to deliver fundamental changes to the way in which organizations collaborate in the aerospace and defense sectors through the translation of goals into capabilities, the TSCP faces the unique challenge of collaborating to improve collaboration. Its international team of part-time volunteers across nine time zones is just one of the challenges that make the TSCP's collaboration efforts particularly tricky—but not impossible.

In support of the TSCP's search to improve industry-wide collaboration, members of the TSCP have worked together to find a better way to collaborate. Their efforts, which build upon years of continuously refined methods, yield several interesting reference points applicable to managers tasked with delivering complex collaborative projects.

Diverse Team, Shared Goals

As a not-for-profit consortium, the TSCP is chartered with figuring out how to best implement a complex set of relationships in a digital setting. Current members include DoD, the U.K. Ministry of Defence, the Netherlands Ministry of Defence, BAE Systems, The Boeing Company, EADS/

Airbus, Lockheed Martin, Northrop Grumman, Raytheon, and Rolls-Royce.

To effectively manage such a diverse team, the TSCP found it necessary to define a solution that met the needs and objectives of all partners for a particular collaborative capability. The consultation and exchange of views during this initial step of activity management ensures alignment between the participants and a shared understanding of the high-level goals as well as constraints on the ability of a solution to meet these goals.

Achieving this alignment and shared understanding is helped by carrying out the planning of the next phase of work alongside the definition of the high-level goals.

The TSCP has found that different interpretations of shared goals are uncovered by the discussion during the planning activity, which is not surprising, given the wider range of cultural backgrounds of the participants and the broad cross-discipline issues being addressed by the affiliation.

In order to proceed, consensus and agreement among participants is typically assured through a gate review, which is generally regarded as a best practice in project management. Gate reviews are used within the TSCP to manage the progressive maturing of a capability from concept to production and are conducted in a manner that meets the needs of all participants.

From Concept to Solution

At a high level, the maturing of a capability takes place in two stages, the development stage and the transition-to-production stage, each of which includes a number of gate reviews. Initial work in the development stage is concentrated within a single lab environment to facilitate rapid prototyping and learning before being replicated by participant organizations in their own lab facilities to assist knowledge transfer and detailed review.

Once the development stage has been completed, capabilities enter the transition-to-production stage. The process of moving activity to the participant organizations is continued throughout this stage. Once collabora-

Skedd is the IT strategy manager in the corporate IT office of BAE Systems. Grant is the deputy information sharing executive for the Department of Defense.

The benefits of secure collaboration have been dramatic for the Department of Defense, which is now looking at how to extend this value through global reach.



tive developments of design definition, documentation, and participation in risk-reduction test activities reach participants, the capabilities move to the next step of the production stage: testing.

Build-out of initial scale production systems are used by pilot user communities to confirm that the solution capability delivers the benefits in real-project activity. This is the last checkpoint beyond which participants proceed to full-scale production at the pace required to meet their business needs. As the transition-to-production stage continues, a central team acts as design authority, providing reference implementation to support test activity among participants.

Bitesize Management

The gate review approach enables the TSCP to take “one bite at a time” of the secure collaboration elephant. It provides short-term objectives needed to maintain the focus of teams that are drawn on a part-time basis from many organizations. It also provides the stability required to plan and manage the work of the team.

Plans are developed within this framework by defining a logical sequence of “chunks” of work to tackle and successfully pass through the next gate review. This network of chunks—the associated outputs and the downstream chunks that use these outputs—ensures a common understanding across the team of the work to be done and its sequence. It also clearly shows the impact of issues in one part of the work on other activities. The number of chunks and outputs is driven down as far as possible to ensure that the plan is easily visualized and communi-

cated, yet remains sufficient to ensure that as soon as the inputs required for a chunk are available, the teams can complete the work and produce the outputs.

If required, more detailed planning within the chunk is entirely self-contained. This approach echoes good practices associated with the division of work breakdown into “control accounts” that are the basic units for management and reporting. The nature of the collaborative contribution of resources to the TSCP means that not all of the reporting is appropriate, but the planning approach provides the basis for simple and easy progress reporting.

The use of a shared information management system by the TSCP means that information sharing within individual work efforts and across teams is accomplished simply by the publication of evolving outputs and supporting information into the appropriate location in the shared environment. These shared environments are used not only to manage sharing of documents but also for meeting calendars, definition of work groups, and sharing of contact information for team members.

Setting a Roadmap

While the approach described above enables individual capabilities to be managed through to production in this progressive fashion, it also provides a framework that can be used to articulate the strategic roadmap for the TSCP. Each capability represents progress towards the eventual goal of secure collaboration, and this progress takes place in defined steps. Future capabilities can be planned to reuse some elements of existing solutions or to upgrade those solutions with new technologies and these linkages

across capabilities can easily be integrated into the roadmap.

The approach continues to evolve as the TSCP progresses. Currently, an effort is under way to implement a restructuring of work teams to provide greater focus on the integration of the wide range of skills required to manage the development of a capability through its life cycle. This restructuring is intended to provide a platform for delivery of the 2008 work plan.

The initial definition and development of a capability in the development stage will be the responsibility of the Enterprise Architecture Group. This group, which has been at the core of the TSCP since inception, will be expanded and strengthened. It will also bring together technology and process to define and develop viable capabilities that address the highest priority collaboration challenges.

When the development stage is complete and a prototype has been shown to work across participant organization lab facilities, the EAG will hand over leadership of the capability represented by that work package to the Business Delivery Group, which (like the EAG) is multidisciplinary and is formed specifically to take a single capability through the transition to production stage. This single capability focus ensures close engagement with the initial user community and the specialists involved in delivery of production systems for a quick and successful adoption of the capability leading to the delivery of business benefits.

Looking Ahead

Maintaining the engagement and utilizing the skills of participants in a distributed effort such as the TSCP is a continuing challenge. The management approach developed by the TSCP has proven effective; it continues to be refined to better meet the needs of participant organizations and individual team members.

The TSCP has begun to deliver important initial capabilities and will deliver improved collaborative capabilities for the aerospace and defense sectors throughout 2008 and beyond. Amazingly, the working approaches defined early this decade are still largely used today. Further progress has been made by the members through their commitment to translate goals into capabilities that will be used across the global aerospace and defense communities. To accomplish this, participants prioritized and bound ex-



The move toward mature secure collaboration still has a long journey to make. However, the Transglobal Secure Collaboration Program's collaboration efforts have been critical steps in the right direction.

ecutable segments of work based upon the common need and mission requirement. For each segment of work, international laws and rules impacting information mobility were assembled. These have been primarily in the areas of export controls and personal privacy.

Equally important, participants continuously address the self-regulation mechanism needed between members to establish and maintain trusted relationships for sharing of sensitive information. Only then can members successfully apply technology standards and solutions to enable secure collaboration and sharing.

The recent work of the participants has been to deal with the "devil in the details" of the journey toward these goals. Capabilities thus far include a federated identity management capability and the ability to send signed and encrypted e-mail using organic enterprise public key infrastructure.

The move toward mature secure collaboration still has a long journey to make. However, the TSCP's collaboration efforts have been critical steps in the right direction. Today, the path is rather well-defined and the capabilities are beginning to move into the operational arena.

In the third and final installment, we will examine the implementations of the TSCP's specifications for information-sharing among member organizations for major programs.

The authors welcome comments and questions and can be contacted at richard.skedd@baesystems.com and paul.grant@osd.mil.