Knowledge Management in a Classified Context

Jo Lee Loveland Link

Abstract:
Classified environments focused on national security have profound needs for knowledge- and information-sharing, accompanied by often-contradictory goals and unique challenges that must be solved. To successfully achieve high-performance enterprise knowledge management requires a complex set of transformations in process realignment, cultural adaptation, and selection of technology fitted to achieve enterprise mission goals. Inter-agency knowledge management elevates risk for these transformations to an even higher level, with even more complex inter-relationships and inter-dependencies. This article decodes these dynamics and explores strategies to facilitate the essential transformation to strong knowledge-based enterprises.

"*The only obstacle to communication is the belief that that it has been accomplished."*
--- George Bernard Shaw

Implementing a knowledge management initiative in any organization is a challenging and complex process. To be successful, knowledge management is an enterprise endeavor that involves business process realignment, technology to enhance the new processes, and, usually, revamped governance and leadership decision structures that support the strategic aims of knowledge management for the organization.

Compounding these changes – which hold true for any organization launching or strengthening their knowledge management program – classified environments lead to entirely unique sets of challenges in knowledge management that can at first blush seem daunting.

What Kinds of Knowledge Are Generated through Knowledge Management?

As anyone who has managed or worked in a complex, data-rich organization knows, not all knowledge is alike. In fact, the very complexity of available knowledge is the first obstacle to knowledge-sharing. Transforming the myriad types and amount of information into usable and useful form, and then to ensure that knowledge is applied appropriately – this is the central challenge for intelligence organizations today.

Under pressure of critical mission concerns, knowledge for effective leadership must be obtained and leveraged – the right knowledge at the right time. The Knowledge Hierarchy outlined below describes an approach that has been found useful in defining sources and uses of knowledge. The Knowledge Hierarchy shows how data is transformed into useful information, and information to knowledge that can be applied to address problems, generate solutions, or innovate new approaches and support leadership decisions.

The Knowledge Hierarchy

1. *Data* is comprised of metrics, statistics, raw facts, and other content that can be quantified, counted, and stored. It is transformed into information through the addition of relevance and purpose.

2. *Information* is produced through analysis, reflection, and synthesis of data, and results in definition of ideas, issues, problems, options, etc.

3. *Knowledge* that makes sense of data and information is generated by organizing, conceptualizing, and systematizing -- to scan for meaningful patterns and trade-offs, to chart decisions and actions, to provide input into plans, to build fail-safe solution scenarios, to refocus strategic direction, etc.

Through mature enterprise knowledge, winning courses of action can be configured, creative solutions found, and relevant actions taken. Knowledge is well-managed when an enterprise is able to forge intellectual assets, creative thinking, combined expertise, and the enterprise repository of lessons learned and past solutions that could apply in other contexts. The payoff from amassing knowledge from across the enterprise can lead to unprecendented surprises and solutions – from new understanding of root causes of present events, to analysis of patterns that shed light on potential new enterprise strategies, to identification of essential new opportunities, to providing senior leaders with strengthened decision information. In an intelligence organization, such amplified knowledge can in fact enhance vital mission-critical national security.

As can be seen, this developmental Knowledge Hierarchy can point to how to sort through and organize enterprise knowledge assets. Technological repositories can be organized to yield improved knowledge outputs. To obtain the real advantages of knowledge management, however, requires comprehensive analysis of business processes across the enterprise.

What Are the Key Ingredients for Successful Enterprise Knowledge Management Initiatives?

To achieve the promise of enterprise knowledge management, an initiative must successfully combine engaged leadership with the smart processes, an adaptive organizational culture, and the right technology that together support sharing of critical knowledge across the enterprise. Complicating establishment of successful initiatives is the fact that those interested in knowledge management often split into three camps: (1) those who believe that knowledge management is primarily information tool-based, and that knowledge management challenges can be solved by choosing the right tools and technologies; versus (2) those who give credence to disciplined process-oriented approaches to problem-solving, and believe that the right processes are almost more important than the right people; and (3) those who believe that knowledge management is primarily situated in people and

leadership, enterprise communications, and organizational functioning, and that the right processes and culture are sufficient.

In actuality, all these positions are right -- and both, therefore, are wrong!

Actually, successful knowledge management requires sophisticated integration of all three capabilities: technology, processes, and culture. Properly established with these integrated enterprise capabilities, knowledge management can yield powerful leverage and intellectual assets through providing vital insight for decision and action across and within the enterprise.

Obstacles to Knowledge Management in Every Organization

Most enterprises have multiple blockades to knowledge-sharing: e.g. often, units are disincentivized to share knowledge by funding that mistakenly rewards hoarding of information; middle managers are pressured to deliver results fast, vs. take the time to install knowledge-sharing mechanisms or hold open knowledge forums; cross-enterprise channels of knowledge-sharing are nonexistent or malfunctioning; enterprises are concerned about taking time away from already-stretched enterprise operations to set up smoothly-operating processes to support knowledge management; etc.

The Unique Characteristics of Knowledge in Classified Contexts

One subtle advantage classified environments enjoy in installing knowledge management is that these organizations are consciously already knowledge-based. In a global environment dealing with terrorism abroad and at home, the need for improved knowledge-sharing among and across secure organizations has become incontestably clear.

However, awareness of the criticality of knowledge sharing and management is not sufficient to realize the promise. Cultural dynamics pervasive in classified organizations obviously and intrinsically discourage open sharing of knowledge. Reward structures for secure environments often provide disincentives to release of information readily. And reluctance to sharing knowledge by secure knowledge workers is understandable: the stakes are very high, mistakes can have unusually severe consequences, and results of sharing the wrong knowledge at the wrong time can be unforgiving in their consequences

The need for compartmentalization has been justified to protect methods and sources of information.

The Association for Communications, Electronics, Intelligence, and Information System Professionals (AFCEA) 2004 Conference on Horizontal Integration held 21-22 April identified several key issues of priority concern on knowledge sharing within the intelligence community, including:

- Recognition of individuals who may be security threats

- Making connections among complex associations in communications
- Associating ideas and people in communications with locations
- Intelligent Geospatial Information Systems
- Knowledge-Based support for information posting accessible to the Warfighters and intelligence analysts.

The following table provides some indicators of differentiation between priority concerns of non-secure public and private organizations, vs. secure environments.

KNOWLEDGE MANAGEMENT DIFFERENTIATORS PUBLIC VS. SECURE ENVIRONMENTS		
Area of Concern	**Definition and Impact**	
	Public/Private Non-Secure Organizations	**Secure Organizations**
Compartmentalization	In industry, a factor of function, competitiveness, and culture; in non-secure government organizations, primarily a factor of culture.	Traditional approaches to compartmentalization are major issues in resolving cross-domain information sharing, and different issues prevail at different tiers of classification structures
Information Loading, Scarcity, and Overloading	Information overload is an ongoing problem, though increasingly being addressed by knowledge and portfolio management systems and tools; getting the right information to the right people at the right time remains a challenge.	Due to legacy security policies and procedures, many members of the intelligence community have been described as "information-starved." There is variance among intelligence users – analysts often experience even more information overload than non-secure organizations; by contrast, Warfighters "on the edge" often lack the critical, timely information they need. As Net-Centricity and other Transformational practices expand information-sharing, Bandwidth constraints become more evident. Delivery of critical information from commander and field require innovative solutions such as meta-tagging, role-based access controls, etc.
Incentives for knowledge sharing	Traditional structures tend to stove-piping and disincentiving knowledge sharing	Compounding typical organizational dynamics are very real transformations required to address compartmented procedures, products, etc.
Roles of contractors	End-to-end knowledge sharing among contractor communities is evolving. Pressure from customers is requiring greater transparency among technical contractors.	Secure environment contractors (often multiple) are intrinsic and vital to mission success. DoD contractors are still in mid-point of solving necessary permissions and incentives to share across enterprise initiatives. Such

		mandates as those being instituted by U.S. JFCOM tend to foster vs. discourage knowledge-sharing among contractors. Solutions are evolving to address corporate proprietary concerns which add to security concerns in inhibiting knowledge sharing.
Mission Clarity	While knowledge management usually emphasizes alignment with enterprise mission and business goals, organizations are various in how well this is performed (and some new initiatives founder as a result)	Mission is often clearer than how to execute alignment to assure knowledge-sharing; leaders are various in emphasizing necessary alignments. Mission goals are often in conflict with security rules and constraints.
Security	Information security a growing concern; on the other hand, non-secure government organizations enjoy missions that encourage open information flow to agency customers, and corporate sector firms are using web-enabled information sharing to attract and retain customers.	Security is a much higher degree of concern, and has broader scope (potential impact is national or global). Security policies are in flux to balance requirements of mission-critical information sharing with necessary protection of vital information.

Taken together, these dynamics fuel the very real need for cybersecurity and information assurance. These factors germane to classified environments leaves many bewildered about how to achieve the right balance of information protection and sharing the information that would help ensure national security.

What Roles Do Leaders Need to Play in Classified Knowledge Environments?

Leadership in such enterprises that seeks to leverage knowledge management is more pivotal than in the civilian, non-secure counterparts (if any organizations or business concerns can be called "non-secure" these days). Messages and mandates of leaders in classified organizations are even more important. Certainly, emerging new security policies and technological innovations are needed to address some very real obstacles to knowledge-sharing in (and especially across) classified organizations. Even before fully realizing the policy and technology breakthroughs that will ultimately support elevated levels of knowledge management performance, leaders in secure organizations have prerogatives that can create foundations for successful knowledge management. The first step is to figure out what kinds of knowledge are the "vital few" processes and information value that will improve effective enterprise knowledge-sharing in the near term.

Knowledge management requires goal-setting in partnership with senior decision-makers to define their goals and desired outcomes for enterprise knowledge-sharing and development

of measurement criteria that will provide visibility into the value – or lack of value – of steps take to install enterprise knowledge management procedures, mechanisms, and processes.

Why and How Do Business Processes Need To Be Aligned with Knowledge Management?

Some enterprise leaders intending to install knowledge management seek first the "right" technology prior to installing the right processes. Winners in the field of knowledge management – including Federal Highway Administration, Federal Aviation Administration, NASA, Transportation Security Administration, U.S. Army Training and Doctrine Command, Air Force Material Command, Naval Personnel Development Command, U.S. Secret Service, U.S. Coast Guard, the World Bank – have found their success stories depend on launching a knowledge-sharing enterprise that capitalizes on redesign and realignment of business processes first. *Only then* does investment in technology tailored to the new processes make sense.

Organizations have accessed a rich array of knowledge management approaches. Successful knowledge management enterprises have utilized communities of interest, knowledge banks, applying agency business cases to include knowledge management, a Lessons Learned system to capture and capitalize on evolving assets, a formalized "drill-down" infrastructure that provides entry points for the entire organization to provide useful information – approaches can be tailored to a wide range of enterprises. Whatever approaches are taken, an enterprise with robust processes may generate information, as data is retrieved, reviewed, and analyzed.

The secret is to invest upfront to help assure success of a knowledge management installation. Enterprises launching knowledge management are wise to invest sufficient resources, expertise, and time to install effective processes, and to seek to "do it right the first time." Experience shows that organizations that fail at knowledge management the first try have much greater resistance on subsequent initiatives.

In fact, the importance of enterprise culture is the "elephant in the living room" that those working to evolve knowledge management eventually discover.

The Impact of Enterprise Culture on Knowledge Management

As noted by Federal Highway Administration's Senior Knowledge Officer, Mike Burk, "companies that have undertaken knowledge management initiatives have found that only 20% of their efforts involve technical issues; the remaining 80 % of their time is taken up with institutional matters to create an environment for sharing and open exchange." Experienced Federal knowledge management leaders converge on corporate culture as the deal-breaker for knowledge management, unless well-managed. Leadership and culture are perhaps the core success factors for enterprise knowledge management.

Some well-intentioned knowledge management leaders may develop business processes they think will facilitate and accelerate knowledge management in their agencies but that are out

of sync with the larger corporate culture. World Bank knowledge management pioneer Steve Denning initially found resistance to the very idea of "knowledge management." Stepping back from his initial efforts, Denning instead looked to see how the Bank culture itself disseminated knowledge. What he found was that powerful shared stories spread practices, rapidly and with minimal resentment. In particular, one story launched the entire successful World Bank knowledge management initiative:

> *"In June 1995, a health worker in a tiny town in Zambia logged on to the website for the Center for Disease Control in Atlanta Georgia and got the answer to a question on how to treat malaria.*
>
> *"This was June 1995, not June 2001. This was not the capital of Zambia but a tiny place six hundred kilometers away. This was not rich country: this was Zambia, one of the poorest countries in the world. But the most important part of this picture for us in the World Bank is this: the World Bank isn't in the picture. The World Bank doesn't have its know-how accessible to all the millions of people who made decisions about poverty. But just imagine if it had. Think what an organization it could become. In 1996 in the World Bank, this story helped galvanize staff and managers to imagine a different kind of future for the organization and to set about implementing it."*
>
> – Steve Denning, **The Springboard: How Storytelling Ignites Action in Knowledge-Era Organizations** (Butterworth Heinemann, 2000).

The research-based Federal Highway Administration (FHWA), known for hiring the best civil engineers, followed a different model to cultural acceptance. FHWA provides a use case on the effectiveness of rumble strips to help convey the relevance and utility of knowledge management for their agency. Showing how to find information in various categories, FHWA communication describes what can be found under the "Knowledge" area of their internal website. "This area includes a summary from the California Department of Transportation of a 1985 study that indicated a 49% reduction in run-off-road crashes after shoulder rumble strips were installed along sections of Interstates 15 and 40 in San Bernardino County. Also…are descriptions of the types of rumble strips – milled, rolled, formed, and raised – and a Quick Time movie of John Watson of the New York State Department of Transportation explaining the types of rumble strips and how they are installed. Finally, there's an examination of some drawbacks of rumble strips, including the difficulty they pose for bicyclists.

The FHWA "resources section … includes a library that features research papers, state rumble strip policies and specification and video clips…The communication section contains three key elements of community-of-practice interaction: an "ask the expert" page, a mailing list, and a discussion group…The discussion group recently featured 17 subject threads, including portable rumble strips, rumble strips in freezing conditions, rumble strips and bicycles, and raised rumble strips."

These two examples show the importance of accessing both formal and informal knowledge in an agency. Sometimes referred to as "explicit" and "tacit," these two kinds of knowledge challenge how much trust in knowledge-sharing exists in an agency's culture. Without accessing knowledge at both these levels, knowledge management is incomplete and will likely yield faulty outcomes.

The Importance of Selecting the Right Technologies

Having emphasized the importance of leadership/culture and the right processes, scrutiny now needs to be on the right technologies. The technology partner community in the secure environment has become increasingly sophisticated about the real needs for knowledge sharing within and among national security organizations.

Since knowledge management is not just one system -- but must be tailored to each enterprise and its mission, short- and long-term goals, customers, methods of operations, etc. -- a paramount requirement for any knowledge management tool(s) must be adaptability and flexibility.

Setting criteria for selection of the right technology, therefore, means assurance that any technology chosen will specifically fit the enterprise, facilitate enterprise processes, and support communication and cultural adaptations necessary for knowledge sharing.

In a secure environment, added to these must be tools that provide specialized capabilities. Role-based access controls, identity management, thinking through the desirable uses of social media – all become critical in the secure environment. George Washington University adjunct professor of systems engineering and knowledge management, Charles H. Bixler, D.Sc., has identified these additional specialized concerns for knowledge management tools in secure environments:

- **Production (business) requirements:** Identify critical success factors that relate to the security strategy, priorities or actions that directly relate to the agency's security mission and goals. To deploy a KM system in the security environment, it is essential to understand the organizational processes and procedures that support security requirements and goals.

- **Functional requirements:** Identify critical success factors that address how the KM system will support the identified production and business drivers. It is necessary to identify and specify the required KM system functionality. Also, the KM system must be integrated with existing enterprise knowledge and communication systems. As stated in the definition, the critical functional outcome is to succeed in getting the right information to the right people at the right time and place.;

- **Technical requirements**: Recognize critical success factors that identify the architectural specifications, tools and information technology policy that must be adhered to in the KM system design. Additionally, identify and establish baseline metrics to determine if KM functional requirements are meeting security goals and requirements. Technical requirements include KM hardware and network infrastructure, system performance, security requirements and technical support. In the security environment, the key is to develop a KM system that is not only secure, but scalable, accessible and effective to the user.

- **Implementation requirements:** Identify the critical success factors that identify the constraints and conditions that must be adhered to during system deployment.

Implementation requirements address the achievement of system migration (if required) with minimal disruption to normal business activities and user routines. In practice, it is essential to implement a KM system that will be easy to use and have widespread acceptance.

Knowledge management tools, well adapted to the specific enterprise mission and concerns, can actually help stimulate cultural acceptance of knowledge management and accelerate adoption throughout the enterprise.

There is one further set of factors essential to successful knowledge sharing -- knowledge gathering must be collected from the full range of enterprise intellectual assets. This means that both explicit and tacit knowledge are integrated into the knowledge management system.

Why Are Explicit and Tacit Knowledge Important in Knowledge Management?

In the field of Knowledge Management, knowledge has come to be described as containing both:

Explicit knowledge, which is formal, usually openly available, and systematic, and relatively easy to capture, communicate and share. Often, explicit knowledge is contained in documents, manuals, procedures, reports, studies, etc. Many technical solutions limit their focus to communication of explicit knowledge.

Tacit knowledge, which is more subtle and hard to capture. Tacit knowledge is learned only by experience, and communicated only indirectly and through informal conversations on technical "tips," comparing notes on project experiences, retelling organizational stories, communicating "know-how," etc.. Much of an organization's true intellectual capital is unwritten and undocumented, and is filed away in the minds of its people (and therefore, walks out the door every day).

While explicit knowledge is certainly important, the value of tacit knowledge sharing can be seen in the successes of face-to-face and virtual collaborations, task forces, working groups, and such institutionalized collaboration as the U.S. Joint Forces Command (JFCOM), with its mission of "jointness" and forums that encourage sharing of informal knowledge across the Services and even to organizations beyond the Department.

Corporate America has gradually begun to explore how to transform tacit knowledge into explicit knowledge, and therefore make it useful broadly across their enterprises. Knowledge portals – while varying in quality and depth – nevertheless are an expression of the seriousness with which industry is working to leverage this kind of vitally useful but hard-to-refine knowledge.

As corporations mature in their mastery of knowledge management, they put in place building blocks of knowledge sharing (or "harvesting," as it is sometimes called). Beginning with individuals, knowledge sharing expands to greater communities of interactions across units, branches, divisions, and other organizational boundaries, finally expanding to inter-

organizational exchanges. In fact, in U.S. corporations, there are knowledge-exchange initiatives between former competitors that have found each of their ability to grow and prosper is enhanced by these exchanges.

How Can Enterprise Knowledge Management Succeed within Secure Environments?

To engineer the organizational and cultural changes necessary for enterprise knowledge management, a "corporate will" to succeed is a critical to success. Tangible actions and results by senior leadership reinforces that knowledge sharing is a priority. Lessons learned from experienced organizations provide indicators as shown in the table below.
of 12 key success factors in any environment.

12 Key Success Factors for Knowledge Sharing

1. **Obtain senior management sponsorship and involvement.** At least one key senior leader needs to become the organizational spokesperson for knowledge management. The knowledge management initiative coordinators need to have regular access to this leader.

2. **Establish a regular management forum** for reports on progress of the knowledge management initiative, and dialogue on proposals and recommendations for further development, as well as management insight and tracking of results.

3. **Develop a clear set of objectives** for the knowledge management initiative. Sharing of both explicit and tacit knowledge must be focused on objectives.

4. **If you plan to make changes in the Information Technology system, plan the ideal management system first then build and adapt the legacy information systems** to support the knowledge management you need to support your mission. Often the knowledge management processes are driven to support the legacy or proposed technology. A technically driven change processes tends to create a culture and process mismatch, which despite massive efforts, produces little improvement in knowledge sharing.

5. **Develop mechanisms to launch knowledge sharing** – both new governance structures and communication structures to publicize pivotal knowledge sharing initiative news. Encourage members of the knowledge leadership to create innovative approaches – such as FHWA's use cases or the World Bank's elicitation of stories with business impact -- to spread adoption of knowledge management. These mechanisms can actually help foster the cultural climate to encourage knowledge sharing through a series of high visibility, interactive events.

6. **Involve rank and file users in the design from the start.** What kinds of information do they need to more effectively do their job? What temporary concessions need to be

made to help assure both productivity and morale? Senior level sponsorship is important, but there are often differences in what each unit perceives needed for optimum performance. All levels can provide useful information to build new capabilities.

7. **Develop incentives for knowledge sharing.** Perhaps even more importantly, disincentives to information sharing must be identified and redesigned to align with initiative goals and desired outcomes.

8. **Set up an integrated process team or working group to lead the process**. This team will need to be comprised of all genuine stakeholders, and will need both senior leadership endorsement, and a master facilitator in order to work effectively together.

9. **Get security involvement from the start**. Security organizations may find it necessary to create their own working group or forum to work on standards and guidelines to help foster knowledge sharing without violating real security concerns.

10. **Make certain that the enterprise knowledge management performance is leveraged by senior management.** Be careful here, however: the right metrics can foster knowledge sharing; the wrong ones can serve as a further disincentive. Good metrics spur accountability but are not punitive. Create a protocol for performance assessment of the enterprise knowledge management initiative for exceptional circumstances.

11. **Create a knowledge taxonomy tailored to enterprise needs** and based on organizational mission and objectives, knowledge schema (critical for an internal meta-tagging process), and security requirements. With solid senior management insight into the knowledge management initiative, it is possible to create many levels of knowledge sharing while preserving security considerations on the methods for obtaining the data or other necessarily confidential information.

12. **Create an organizational culture that both "learns form the mistakes" and checks to see if what they thought they learned was correct**. To ensure genuine value from lessons learned requires a high-level process such as the U.S. Army's "After-Action Review," to develop consensus on just what lessons were really learned and would be useful to leverage.

What Are Best-Practice Approaches to Inter-Agency Knowledge Management for Secure Environments and across Enterprises?

For these most challenging of all knowledge management initiatives, specific measures must be taken for any reasonable chance of success. Quite aside from "turf boundary" issues, there are genuine differences among agencies in their understanding of mission and other strategic factors, and consequently in communicating and leveraging knowledge across organizational boundaries. To realize the gains and opportunities of knowledge

management in a classified environment, the following nine elements have been found to be useful.

Ten Critical Elements for Knowledge Sharing in Classified Environments

1. **Set the agency's strategic and cultural context for all who will be involved.** Emphasize the larger purpose and promise for intelligence and national security organizations; for example, analysts are essential to improve accuracy and speed of intelligence to national leaders; Defense intelligence is needed to shorten decision cycles for field Commanders; cross-agency information sharing will rapidly increase the impact of intelligence in the War of Terrorism. Communicate clearly the enhancements possible for agency's mission, and send out the message repeatedly, through several kinds of communications channels.

2. **From initiative launch forward, involve key stakeholders.** At the outset, interview stakeholders to identify their concerns and goals. In intelligence organizations, key stakeholders may include division leads, Congressional staffers, representatives from both Defense and intelligence officers, etc. Establish vehicles for communication between the senior leadership team and the stakeholder community to provide regular updates on the knowledge management initiative, together with guidance from the leadership on expected outcomes and goals for the knowledge management initiative.

3. **Where appropriate for an inter-agency knowledge-sharing initiative, create an interagency Memorandum of Agreement (MOA)** among senior leaders from all involved organizations, to specify mutual goals and "rules of engagement." MOA's are especially important to address and resolve intelligence standards, policies, and differing mission requirements.

4. **Establish a leadership steering committee** comprised of representative senior leaders and specialists from each of the agencies. This group will need authorization from the most senior executive level to assure open channels for verification of any critical questions that arise, and to endorse and communicate important decisions and actions generated. Authorities to help assure progress form the highest levels can help not only the knowledge-sharing initiative but help create models to spread adoption across national security organizations.

5. **From the start, involve all the agencies' security officers,** providing them with clear guidance from the leadership team regarding required outcomes and goals for the knowledge management initiative. Their tasks will include evaluation of the initiative's methodologies and mechanisms for security concerns, and development of clear security guidelines to steer the initiative. As cross-domain information-sharing policy evolves, these guidelines will need to be revisited periodically. At least one representative from this group should sit on the leadership steering committee.

6. **Provide clear guidance from the leadership steering committee on knowledge sharing goals, outcomes, and solutions sought for the initiative.** To support their work, create methods for auditable documentation of what is shared. Secure

organizations may need to tailor tracking mechanisms for knowledge sharing activities, and assure that the right permissions are in place for access. Importantly, make sure there is a central knowledge base that is shared across the involved agencies.

7. **Institute an infrastructure network of working groups** to research options, provide recommendations, and implement decisions on behalf of the leadership steering committee, and to provide additional sources of feedback from the agencies. Especially in agencies that are launching knowledge sharing initiatives, the working groups themselves provide models and experiential evidence of the power of sharing information and working with a robust suite of intellectual resources to solve problems.

8. **If Information Systems are to be sharing information, build to the emerging common technical standards** for information systems, taxonomies and meta-data standards.

9. **Periodically, gather mid-managers from each of the component organizations to engage in an input/feedback session.** These can be worth their weight in gold in surfacing dissension prior to serious resistance, and to generating knowledge that can be useful to the inter-agency knowledge management initiative.

10. **When launching the initiative, and periodically thereafter, conduct targeted surveys of the involved organizations** to determine areas where improved knowledge management could make a significant difference in overall operational results. Dynamic intellectual assets yield ongoing pay-offs, especially in classified environments.

The rationale behind traditional sheltering of intelligence and knowledge across secure organizational boundaries is understandable. However, the unintended consequences of severely restricted access to enterprise and inter-agency knowledge sharing has been shown – not solely but certainly reinforced by recent events, and their aftermath – to have seriously negative results. Secure organizations are now under increasing pressure from their own leadership as well as from Congressional and Presidential offices to improve, quickly and significantly, in knowledge management across boundaries.

In fact, over the past several years, real momentum for knowledge-sharing has accelerated across the national security community. Beginning in the last two decades with problem-solving on how best to share mission-critical imagery, knowledge-sharing has evolved across DoD and the intelligence community to the point where real progress is being made through integrated Net-Centric capabilities. Through such initiatives as the DoD/OSD/NII Horizontal Fusion Portfolio, the Net-Centric Enterprise Services initiative from the Defense Information Systems Agency (DISA), and the intelligence community's Transformational efforts in Horizontal Integration, giant steps have been made toward providing the right information at the right time, to much broader communities of interest.

Conclusion

Clearly, intelligence information is too critical a national security issue to continue risking gaps in communications. To create a vibrant and highly effective knowledge management program in classified contexts must be an overarching goal. Still, respecting the special challenges inherent in communications between secure organizations, and between secure and non-secure organizations will require thoughtful planning and execution. Nevertheless, there is growing agreement among national leaders that organizational cultural factors have been major inhibitors of exchange of knowledge across law enforcement and intelligence organizations.

Diagnosis of both successful and less successful knowledge management programs reveals interplay of cultural/ leadership, process/operational factors, and carefully aligned technologies must be orchestrated to leverage organizational intelligence into dynamic knowledge sharing.

The approach recommended here sets a framework for action that draws on successful knowledge management programs, while eliciting valuable insights from across an organization. The resultant approach has been shown to yield knowledge management programs that are durable, that inspire commitment and wide use, and that generate sharing of timely and valid knowledge in the national interest.

Jo Lee Loveland Link is a specialist in enterprise transformation, organizational design, and socio-technical integration. A pioneer in the OSD/NII Horizontal Fusion Portfolio, Ms. Link has worked extensively with military and intelligence Information Technology organizations, including the Department of Defense Office of the Chief Information Officer, Carnegie-Mellon University's Software Engineering Institute, as well as industry and non-governmental associations.