9

Knowledge Management in the Public Sector

The ability to draw on critical knowledge efficiently and reliably is what managing knowledge is all about. It is getting the right information, at the right time, in the right context, to support an identified need, strategy or action.
(DCMA 2004)

Although there are still government agencies in which it is not found in full-blown operation, the management function known as *knowledge management* has been widely embraced by a wide variety of organizations in the federal government. In those agencies where KM is found, it is often considered an important if not absolutely necessary management tool; implementing KM will enable the agencies to meet their service and performance requirements in spite of the many challenges government faces in this new century. Moreover, proponents of KM believe that by enhancing the collection, codification, storage, transmission, and sharing of knowledge, government agencies are able to succeed in their missions despite declining budgets, demands for more and improved services, and a skilled, knowledgeable workforce that is disappearing into retirement.

KM is far less visible in either state or local government, however. At the local level, many of the tasks of KM are managed under the auspices of a chief information officer, or similar IT-oriented managers. Because of the still-sparse adoptions of KM in state and local governments, the bulk of the discussion in this chapter must refer to KM as it is found in federal agencies, departments, and functions, with the few state and/or local applications added as they are found.

One of the reasons why government agencies at all levels may have been slow at adopting KM for their operations has been because they have had to fight entrenched agency cultures in which the norm was to keep information

to yourself, not share it (Harris 2001). Proponents of KM believe that they have the power to change this culture. They point out that when knowledge resides in the group instead of an individual, the entire organization is made stronger. They point to the successes of organizational learning as examples of the power of shared knowledge. The culture of the organization must move from hoarding information to sharing information. In this way, organizations benefit from a new openness and continued support of upper-level management. Eric Lesser, a KM consultant at IBM, warned that the problems of opposing cultures are not the only barriers to successful KM programs in government. The most difficult task may be finding the time to give people the opportunity to talk with one another and share information. To deal with this problem, organizations often have to require their employees to participate in KM programs. When they fail to do so, the KM program also fails.

Chapter Objectives

The content of this chapter is designed to serve as an introduction to the series of public-sector KM case studies that follow in part 4. The objectives for this chapter include the following:

- To help readers gain a deeper understanding of the roles knowledge management is coming to hold in a wide variety of government agencies.
- To reinforce readers' recognition that, although it plays a big part as one of the fundamental legs of KM, information technology is only one of the primary drivers in a successful KM application.
- To help readers understand both the similarities and the differences in the roles of the chief information officer and the chief knowledge officer.
- To help readers, by reading about several case histories of agency experiences with and without KM programs, to understand where KM practices and procedures contributed to the ability of agency managers to achieve their missions.
- To help readers, again by reading case histories of successful KM applications, to see where and how KM can—or should—be applied in their own organizations.

KM in the Federal Government

Government adoption of KM began late in the decade of the 1990s, some ten years after a small number of businesses and industries first introduced the concept into their operations. The General Services Administration (GSA) was one of the first federal agencies to see how KM could improve their

ability to carry out their operations. The FAA and the Goddard Space Center of the National Aeronautics and Space Administration (NASA) were not far behind (Ross and Schulte 2005). By the end of the decade and the beginning of a new century, enough federal agencies had expressed an interest in learning more about KM for the Office of Management and Budget (OMB) to take notice.

Initially, KM was more or less synonymous with Information Technology (IT). Private-sector IT vendors were engaged then—and now—in intense competition to sell their hardware and software to any and every agency even remotely interested. The OMB reacted quickly to bring a measure of rationality and planning into IT purchases. Another problem that concerned the OMB was that agencies were purchasing systems that could not communicate with one another, a practice resulting in independent systems with data contained in silos of information

A spokesperson for the Defense Contract Management Agency (DCMA) described how greater application of KM systems would contribute to the solution to these information hoarding difficulties:

> The Federal government is a vast storehouse of knowledge, and its employees are experts in thousands of subjects, from AIDS research to weather prediction. The real challenge is building an environment for a freer exchange of this collective intelligence among federal agencies; an exchange among Federal, state and local governments; and a more accessible exchange between the knowledge stores of the Federal government and citizens. The ability to leverage these extensive knowledge stores and increase the intellectual capacity of agencies to quickly find solutions improve decision-making and effectively respond to other government organizations and citizen is crucial to achieving a major improvement in the Federal government's performance and value to the citizen. (DCMA 2004)

Information technology is universally recognized as one of the four or five key components of a system for managing and leveraging an organization's knowledge. Before 1996, however, IT purchases and applications were considered to be the concern of each individual agency, with each unit's purchases controlled only through the budget and appropriations processes. Congress and the executive branch realized that something needed to be done to bring some measure of control to the ever-growing amounts being spent on IT. To do so, the position of chief information officer (CIO) was established in 1996 by executive order. Agencies appointed their own CIOs, who then began to monitor and manage their agencies' IT planning, purchases, applications, and architectures. The Office of Management and Bud-

get then set up the Federal Chief Information Officers Council (CIO Council). The council is a network where CIOs can share problems, successes, and experiences. With the establishment of the CIO Council all federal CIOs also became members of a *community of interest* devoted to improving the use of IT in government.

The chair of the CIO Council is the deputy director for management in the OMB; members of the working group elect the vice chair from among the group membership. In 2005, the council had three working committees, with ad hoc groups formed as needed. The three committees are all responsible for some aspect of knowledge management. They are: (1) the *Best Practices Committee,* which focuses on identifying and encouraging the use of best practices to improve the development and delivery of IT solutions across federal agencies; (2) the *Federal Architecture & Infrastructure Committee,* charged with establishing a government-wide foundation for greater adoption of e-government by supporting the development of a common enterprise architecture and infrastructure platform, and by providing models and standards for federal systems; and (3) the *Workforce and Human Capital for Information Technology Committee,* which focuses on two programs: improving the federal government's ability to attract and retain a top-notch IT workforce, and expanding IT education and training opportunities for all federal workers.

By December of 2000, sufficient interest had been generated in KM across federal agencies for a few far-sighted leaders and CIOs in civilian and military organizations to form a special interest group on KM topics. The CIO Council officially formed the Knowledge Management Working Group (KMWG) on January 5, 2000, to be the interagency body that would bring together the best of what federal agencies were doing with KM. Although the working group is particularly concerned with KM in the federal government, it has begun discussions on collaboration and knowledge sharing with state and local governments.

The KMWG includes federal professionals, ICT consultants, vendors, and representatives from academia. The working group includes representatives from more than thirty federal agencies. The primary mission of the federal KM group is to ensure that all government agencies collect and share what the government workers *know.* Governance for the KMWG falls under the leadership of the Best Practices Committee of the CIO Council, which has formally charged the KMWG with responsibility for:

- Identifying best KM practices that can be found in government, business, and industry;
- Encouraging the dissemination of information related to KM; and

- Ensuring the development of competency profiles for public-sector chief knowledge officers.

The KMWG accomplishes these assigned tasks through a variety of special interest groups (SIGs). The number of SIGs operating at any one time varies with assigned tasks, needs, and available resources. Shortly after its formation, the working group identified four far-reaching benefits they believed would result from the growing emphasis on KM in government (Remez and Desenberg 2000). First, *information, knowledge, and expertise will be readily available by subject and interest area.* KM has the ability to break down barriers to learning caused by the practice of "stovepiping" people, their knowledge, and their skills into artificial groups and bureaucracies. It does this by bringing technology—i.e., the Internet, intranets, listservs, and other electronic communications tools—and people together to eliminate physical and organizational boundaries. This enables communities of practice to form and flourish. Communities of practice are informal groups of people located in geographically dispersed areas and groups, but who have a common interest in a work domain, project or product, and/or practice.

Second, *government services will be integrated and accessible.* Knowledge management brings together expertise and action, letting citizens transact business with all levels of government. For example, today it is possible for citizens to access such government services as renewing their pet or driver's license or their passports, and they can pay their utility bills online. Other agencies are working on making it possible for citizens to vote online. The old Web sites that used to be simply data repositories are rapidly becoming knowledge portals that provide real solutions.

Third, *one-stop shopping will come to government.* Knowledge management has the power to bring together different agencies and levels of government, not based on organizational structure, but according to purpose and function. In one Washington State example, an independent knowledge specialist has developed a Web service that makes it possible for citizens carrying out an activity that crosses a number of rural jurisdictions to complete the permitting process online. Applicants go to a single Web site to apply and pay for one permit that is valid in all jurisdictions, and receive the permit in just a few days—the goal is to eventually bring the response time down to just hours. The site brings together the combined knowledge housed in people working in six continuous small communities. Before, the citizens would have had to visit each site to apply for a permit valid in only that one community, meet different requirements in each community, and wait different periods of time for the community official to respond. Overall, the process might have taken weeks if not months.

Fourth, *tacit knowledge will become more accessible*. Many people still experience some unease when they find themselves trying to communicate with nonhuman automatic response systems, or a customer service individual who might be located several continents away. Instead, they prefer to either travel to a government office or wait on hold to speak with a live person in order to reap the benefits they receive from the knowledge of experienced professionals. Certainly, mountains of raw data have long been available for anyone who knows how to maneuver their way through the maze of the World Wide Web. However, the tacit knowledge and experience that a skilled person brings to a citizen's problem has, until just the last few years, been available only in a face-to-face meeting. Knowledge management applications have the power to harness this tacit knowledge and put it to use on a much wider scale. One way this is happening is by the wedding of Internet communications and television. Agencies are using televised vignettes—in stories used as examples of solutions to problems—to capture the tacit knowledge held by professionals on their staffs. Citizens can access these televised stories directly on their home computers. In some instances it is also possible to request and receive a connection to a live representative for real-time communication.

Presidential Support for KM

Federal agency interest in knowledge management was given a large boost early in the administration of G.W. Bush, who included KM in his President's Management Agenda (PMA), along with management improvements, enterprise architecture policies for IT, strategic planning, and e-government initiatives. The president's KM mandate was clarified in a 2002 OMB report:

> The Administration will adopt information technology systems to capture some of the knowledge and skills of retiring employees. KM systems are just one part of an effective strategy that will generate, capture, and disseminate knowledge and information that is relevant to the organization's mission. (OMB 2002, 13)

Today, most agencies in the federal government have appointed chief information officers to oversee their IT operations. In some agencies, the CIO is also responsible for managing the knowledge management system. However, today the KM director is more likely to be a separate, senior-level manager functioning with the title of chief knowledge officer (CKO) or something similar. The government agency CKO has broader responsibilities than the organization's IT. The CKO must plan, implant, and manage a comprehensive program that fosters knowledge collection, sharing, and usage. Under a

KM operating philosophy, IT is one of several equally important tools that help make a knowledge management system possible.

Early Federal Adopters of KM

The General Services Administration was one of the first federal agencies to take on KM as a major strategic thrust. The GSA is responsible for acquiring the buildings, products, services, technology, and other workplace essentials for federal agencies. The agency's knowledge management unit is housed in the Office of Applied Science–Knowledge Management Division. The division describes its responsibilities as follows:

> The Knowledge Management Division is responsible for leveraging the sharing of knowledge, information, and data across the [GSA] organization. It is responsible for identifying, capturing, and disseminating information. The Division will also evaluate he effectiveness of information and determine its relevance and validity to support [the organization's] business. (GSA 2006, 1)

The Federal Aviation Administration (FAA) is responsible for maintaining the safety of the nation's aviation system, including managing the air traffic control network and monitoring aircraft safety. The FAA has a long history of applying knowledge management concepts to its operations. The Knowledge Sharing (KS) office was an early group set up to promote knowledge management across the organization. A follow-on organization was the Office of Knowledge Management. Among the long list of KM programs in the FAA were the Environmental Occupational Safety and Health Event Management System, an FAA Logistics Center, the National Aerospace Information Architecture Committee, the Aviation Safety Knowledge Management Environment, the Technology Transfer Program, and the Traffic Flow and Enterprise Management Collaborative Communications System, among others. FAA'S Traffic Flow and Enterprise Management (TFEM) organization was one of the founding members of the agency's Knowledge Services Network (KSN), a group established to foster collaboration and research and develop the FAA's knowledge management effort (FAA 2003). The TFEM developed and implemented the Collaborative Communications System as a knowledge management tool.

NASA's Strategic Plan for KM

The KM professionals at NASA produced an early version of a strategic plan for knowledge management in April 2002. In the foreword to that plan the authors outlined a chief reason why getting a handle on the scientific and technical knowledge as NASA was so critical.

For most of its history, the majority of NASA's physical and human resources were directed at developing and managing a few long-duration programs such as the Apollo, Viking, and Space Shuttle programs. During those years, NASA had the luxury of its people willingly sharing knowledge throughout their tenure on the programs. Engineers and scientists spent years, sometimes decades, working on a project. During those years junior employees learned from senior members of the project team. Eventually, the juniors became seniors and they, too, mentored new junior team members.

For more than forty years, NASA'S knowledge base and abilities have continued to grow. Today, however, NASA has been forced to adopt a new operating philosophy, one in which it must apply the principles of faster-better-cheaper as appropriate. NASA can no longer sustain the earlier era of apprenticeship and the nurturing of the flow of experiential and tacit knowledge from senior to junior employees. Today, engineers and scientists may work from one to three years on a project and then move on to something new. Individually they gain a lot of knowledge, but what they learn stays with them; the knowledge is not captured or passed on across the organization for future missions. Knowledge management principles offer a solution for moving ahead, accepting today's constraints, and adapting to a world where technology and innovative processes must partially replace the mentoring and measured approaches formerly common throughout NASA. According to Jeanne Holm, chair of NASA's knowledge management team in 2002, "NASA's knowledge, its intellectual capital, is the Agency's primary, sustainable source of competitive advantage. Physical assets age, today's workforce is mobile, and technology is quickly bypassed. Our knowledge as an agency, however, can endure. This knowledge is a fluid mix of experience and know-how that allows NASA employees to strive for and achieve the improbable day after day" (NASA 2002, 1).

The strategic plan highlighted three key areas in which the agency needed to manage its knowledge and that the agency needed to address more effectively. The first was capturing more of the critical knowledge needed to safely conduct missions. The second was making it possible for virtual teams to collaborate more effectively in their work. And the third was managing more effectively the information already captured in the agency. The principles in this strategic plan have guided the agency's KM operations to where it is now one of the most proficient and effective at using KM in accomplishing its overall mission.

KM in the Navy

The Department of the Navy (DON) was one of the first branches of the military to successfully adopt the KM philosophy. Jim Knox, chief informa-

tion officer for the DON, defined the navy's take on KM in a paper presented at a 2005 government KM conference:

> Knowledge Management systematically brings together people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance. (Knox 2005).

The navy's version of KM—the DON KM Framework—is formed from five key interconnecting spokes: content, processes, culture, learning, and technology. Each spoke is further shaped by a number of key factors developed from several knowledge management tools, techniques, or practices. The culture spoke, for example, includes commitment, sharing, building relationships, and communicating. The learning spoke is framed around building content, storytelling, creating, growing, experimenting, and establishing feedback loops. The content spoke includes value, relevancy, currency, credibility, and expertise, while the process spoke incorporates making knowledge explicit by capturing, categorizing, mapping, analyzing, and disseminating. The technology spoke is built on enabling, facilitating, empowering, and promoting innovation.

The navy employs KM in a range of applications, beginning with the DON Virtual Knowledge Repository. This tool is used as a clearinghouse for best practices data. Other DON operational applications include the Naval Network Warfare Command, the Tactical Training Group–Pacific, and the DON Business Innovation Team, among others. Recognized as a leader in KM government applications, the DON has distributed more than 20,000 copies of its Knowledge-Centric Organization (KCO) toolkit to different federal government agencies and units. The toolkit, recorded on a CD, provides information on how to create a KCO that connects people to the right information at the right time for decision making and action.

Varying Degrees of KM Adoption

Knowledge management and knowledge management systems applications have far to go before they become an integral management function everyplace they can contribute to agency performance. The principles and practices of KM have been embraced by such federal offices as all branches of the military, NASA, the Department of Transportation, and many similar offices where the collection and sharing of workers' knowledge is a critical component of operations. Surprisingly, however, in other organizations management's embracing of KM has been far less warm or demonstrative. The examples that follow illustrate situations where an installation of a comprehensive knowl-

edge management system could improve agency performance. The first illustration is the office of the Architect of the Capitol; the second is the Department of the Treasury; and the third is the Department of Homeland Security and several mission-related operations.

The Case of the Capitol Architect

The office of the Architect of the Capitol (AOC) is responsible for the maintenance, renovation, and new construction of all buildings and grounds within the Capitol Hill complex. The U.S. General Accounting Office (GAO) is required by the Legislative Branch Appropriations Act to conduct a thorough review of all legislative branch operations, including the AOC. The purpose of these reviews is to identify where the organizations can improve their strategic planning, organizational alignment (structure), strategic human capital, and information technology—and knowledge—resources so that they might better achieve their mission.

The GAO's 2003 report on the results of their study of the AOC included the conclusion that *managing knowledge* is one of the key steps the agency must take in its legislatively mandated management transformation. The GAO report recommended that the architect's office implement three major management changes (emphasis added):

- Strengthen and consistently implement its human capital polices and procedures, including addressing ways in which management could better gather and analyze data on employee relations issues.
- Continue to improve its approach to financial management by developing strategies to institutionalize financial management practices that support budgeting, financial, and program management.
- *Adopt an agency-wide approach to information technology management by establishing appropriate leadership and developing the policies, procedures, and tools needed to effectively and efficiently manage information technology resources across the agency.*

The last recommendation is emphasized in order to point out that these are key steps in designing and implanting a knowledge management system. Specifically addressing the information technology management issue, the GAO added that they believed the AOC could benefit greatly from knowledge sharing, and by encouraging and rewarding employees who share and implement best practices across the various jurisdictions, teams, and projects. For example, employees included in the study's focus groups overwhelmingly reported that communications from supervisors to employees was insufficient.

In 2003, the AOC still did not have an agency-wide approach to managing its information technology (IT) functions; it had not implemented the requirement to prepare a technology architecture plan (i.e., a blueprint for current and future IT needs); nor had it named a senior-level executive to be responsible and accountable for IT management and spending. Rather, control of IT purchases and operations remained in each AOC organizational component.

GAO auditors concluded that without proper agency-wide management of IT, the Architect of the Capitol will be unable to effectively manage all the critical building and operating systems knowledge that resides in the minds of its personnel. When such problems as the anticipated retirement and departure of large numbers of senior-level professionals occur, the AOC may find itself forced to continue to "reinvent the wheel" for each solution, thereby unnecessarily increasing both the cost and the time to complete a project. Decades of critical knowledge will be irretrievably lost.

The Case of the Treasury Department

An illustration of what happens in a government agency when there is insufficient or unfocused management of data, information, and knowledge was reported in a GAO report on activities in one unit of the U.S. Treasury Department shortly after the September 11, 2001, terrorist attacks. The study was not tied to that catastrophic event, but clearly illustrates the notion of better control and sharing of information and knowledge.

The U.S. Department of the Treasury has many diverse responsibilities, organized in twelve separate bureaus. The department summarizes its many duties and responsibilities into three overarching tasks: promoting the nation's economic well-being, managing the government's finances, and ensuring the integrity of financial information both inside and outside of the federal government. In the August 2004 annual report of its operational results, the department succinctly summarized these responsibilities by identifying itself as the "chief manager of the nation's finances."

The department is also charged with enforcement of the laws and regulations that relate to such responsibilities and functions as the Alcohol and Tobacco Tax and Trade Bureau, the Financial Crimes Enforcement Network, the Inspector General, the Internal Revenue Service, and the U.S. Mint, among others. To carry out these enforcement duties, the individual bureaus typically coordinate and collaborate with other federal, state, and local law enforcement agencies. In March of 2002, the General Accounting Office (GAO) issued a report of its review of the department's Office of Enforcement (now the Office of Terrorism and Financial Intelligence, which combines the

department's intelligence and enforcement functions). The enforcement office was established to provide oversight, policy guidance, and support to the department's enforcement bureaus. The GAO report spelled out why it is so important for government agencies to manage the knowledge that exists within their domain.

The GAO reported that they could not find any single comprehensive source in Treasury that provided guidance to either the enforcement staff or the bureaus in those instances when the bureau must interact with enforcement personnel, nor could they find any established documentation for twelve of the twenty-nine situations where such interaction is required. When documentation did exist, the GAO considered it to be (1) generally too broad in nature for its purpose, and (2) a failure at providing explicit information on half of the bureau/enforcement interactions. About half of the bureau officials interviewed said that they were not aware of any written requirements for their interactions with enforcement, nor did they know when to interact. The knowledge factors that influenced the requirements for interactions included professional responsibility, experience, judgment, and even common sense.

The GAO report emphasized that the agency's internal control needed to be clearly documented and that documentation should be readily available for examination by managers and field workers as needed—clearly a role for a knowledge management system. The GAO went on to add that, without a well-defined and -documented set of policies and procedures covering operational and communications activities, the enforcement office of the Department of the Treasury runs the risk of not being able to perform its functions and meet its goals efficiently. KM can help the department to surmount this threat.

The department has moved to rectify the shortcomings identified in 2002; progress on a number of change initiatives was spelled out in its 2004 President's Management Agenda report (DOT 2004). Those changes clearly reflect knowledge management thinking without the KM label. For example, Treasury's human resource offices, business units, and information technology offices now work together to identify current and planned technology, required skills, and current and anticipated skill gaps. This information is used to frame the department's long-term plans for closing the skill gaps and maintaining appropriate skill levels.

A program to enhance workforce capabilities has resulted in the implementation of a comprehensive, multidimensional, and integrated technology knowledge-sharing strategy. At the same time, greater integration and control over investments in technology and processes are being implemented to ensure that knowledge, skill, and training needs are included in all technology proposals and implementation plans.

Changes at Treasury that specifically address the lack of coordination and procedures with enforcement include an electronic information exchange system to allow law enforcement agencies—federal, state, and local—to quickly attain information from U.S financial institutions about suspects, businesses, and accounts in major money laundering and counterterrorism investigations.

The Case of Homeland Security

Homeland security is a classic example of an area in which significant efforts at managing critical knowledge are warranted. One of the reasons often cited for the failure of national and local law enforcement and intelligence agencies to identify and deter the terrorist attacks of 9/11 was the long tradition of protecting—hoarding—information of this type. This practice is referred to as collecting and holding agency-gathered knowledge relating to potential threats to the nation in secure "stovepipes" or "silos." In an Op-Ed article in the *Mercury News* of San Jose, California, the dangers of the practice of information and knowledge hoarding were described in a hypothetical case in which a field agent at the Chicago, Illinois, FBI office and a CIA operative in Kabul, Afghanistan, both become aware of separate leads regarding a possible biowarfare attack on Chicago. Under the traditional system, it is unlikely that the two reports would have been put together or that either agent would be made aware of the other agent's information (Baird and Barksdale 2004).

The authors of the "think piece" article were officials of the Markle Foundation, a nontraditional private foundation that sponsors research in counterterrorism, among other fields. The foundation has a long history of working to improve the nation's healthcare and medical education systems, promote interactive communications programs for children, and promote policy initiatives for adoption of IT in government. Its work on issues relating to the nation's security network was a logical outgrowth of its work in promoting IT applications. In this role, Markle brought together leaders and innovators from technology industries, various government agencies, public interest organizations, and business to promote technical and policy changes relating to new and better uses of IT in government.

After September 11, 2001, the foundation formed a study task force comprising leading national security experts from the Carter, Reagan, G.H. Bush, Clinton, and G.W. Bush administrations, and other experts on technology and civil liberties (Dempsey 2005). Their charge was to identify ways to strengthen the nation's security against the threat of terrorism. The progress reports, produced in alliance with the Brookings Institution and the Center

for Strategic and International Studies, were issued in 2002 and 2003. The foundation described its interest in knowledge management in healthcare and national security thus:

> These are two of the most critical issues of our time, where the benefit to be gained from the ability to put the right information into the right hands at the right time is enormous. In each of these areas, the effective use of [shared knowledge] can literally save lives. These are areas where IT promises great breakthroughs, and where without better use of IT our nation's goals cannot be met. At the same time, healthcare and national security also highlight the major challenge in seeking better ways of using information: the risk such use poses to our established privacy and civil liberties. (Markle Foundation 2003, 2)

In its final report, *Creating a Trusted Information Network for Homeland Security,* issued in December 2003, the Security Task Force stressed the importance of creating a decentralized network of information sharing and analysis around presidential guidelines to address the challenge of homeland security. The report also identified the following seven key characteristics that are needed to enable homeland security units to take full advantage of the nation's strengths in information technology:

1. Handling of information should be decentralized and take place under users, following a network model rather than a mainframe hub-and-spoke model.
2. The network should be guided by policy that simultaneously empowers and constrains government officials by making it clear what is permissible and what is prohibited.
3. The government's security strategy should focus on prevention.
4. To deal with the difficulty of distinguishing between domestic and foreign threats, the government should avoid creating blind spots, or gaps between agencies, that arise from such distinctions. New rules must replace the old "line at the border" rules that distinguished domestic and foreign information-collecting responsibility.
5. The network must recognize that many key participants are not in the federal government, but instead may be in state or local government or the private sector.
6. The network must be able to use information gathered in clandestine intelligence activities, information from normal law enforcement investigations, and also information held by private companies. This should occur only after guidelines for its collection and use are formed.

7. Policies and actions for combating terrorism need to have the support—and trust—of the American people. Privacy and other civil liberties must be protected.

The report then identified a list of steps for implementing the policies, adding that the federal government needed to give greater priority to sharing and analyzing information. The report concluded that it is no longer possible to justify the practice of restricting access to information that characterized the intelligence policies of the Cold War. Rather, the agencies involved need to adopt a program similar to what the study termed the *Systemwide Homeland Analysis and Resource Exchange* (SHARE).

The report also spelled out a set of goals, policies, and practices that are part and parcel of a typical *knowledge management system.* Reaffirming the principles of the first report, the 2003 document included greater detail on how and why government must create networks for information collection, sharing, analysis, and use across federal, state, and local agencies and the private sector. The network as conceived by the task force includes more than just technological architecture; it must also focus on the people, processes, and information that must go hand in hand with the technology, including the rules necessary to govern how all the elements interact.

The task force did note that the federal government has made some progress in developing the envisioned network; both the executive branch and Congress now have an understanding of the need for more information sharing and for networks that break down agency "stovepipes." Steps have been taken at all levels of government to expand the sharing of terrorist-threat data among all agencies, while at the same time improving analysis of terrorism-related information.

One example of this greater coordination and cooperation is the Antiterrorism Information Exchange (ATIX) network developed by the Justice Department and the FBI to provide all law enforcement agencies and public safety, infrastructure, and homeland security groups access to some homeland security information. At the federal level, creation of the Terrorist Threat Integration Center (TTIC), a joint operation of the CIA, the FBI, the DHS, the departments of State and Defense, and other members of the intelligence community, was announced in January of 2003. However, the 2003 report also charged the Department of Homeland Security and the TTIC of laxity in developing the needed knowledge management system. Moreover, the DHS was apparently lax in its duties by not taking the necessary steps to build the communications and sharing network required to deal with a terrorist threat. Nor did the agency begin producing regular, actionable intelligence products for other agencies on time, as needed. The DHS had not produced a vision of how it would link federal, state, and local

agencies in a communications and sharing network, or what the agency's role would be with respect to the threat integration center and other federal agencies. The report concluded that the DHS instead appeared to be focused on building a new information technology infrastructure to support and unify its twenty-two components. Finally, the study determined that neither the TTIC nor the DHS had accomplished much in the way of putting in place the necessary staff or framework for analyzing information and sharing it among the relevant federal, state, and local agencies.

By 2005, however, the Department of Homeland Security had made a number of important strides in resolving these critical shortcomings. One such advancement was the formation of a network for sharing information, connecting, and improving homeland security, Lessons Learned Information Sharing (LLIS.gov). LLIS is a national online network of lessons learned and best practices for emergency response providers and homeland security officials. The restricted and secure network serves approximately 12,500 members as the official clearinghouse for all homeland security–related information (Travis 2005).

One of the growing problems associated with the installation of a comprehensive terrorist information network is the large and growing number of government, nonprofit, and private-sector companies involved in one or more aspects of the field. For example, the LLIS program is sponsored by two agencies: the DHS Office of State and Local Government Coordination and Preparedness (SLGCP)—formerly the Office of Domestic Preparedness—and the National Memorial Institute for the Prevention of Terrorism (MIPT). Reflecting the special vertical sharing requirement for antiterrorist information, SLGCP is responsible for assisting states and local jurisdictions to prevent, plan for, and respond to acts of terrorism, while the MIPT sponsors research to discover equipment, training, and procedures that might assist first responders in preventing terrorism and responding to it.

The LLIS knowledge management system has become the official repository of lessons learned and best practices for the Department of Homeland Security. To encourage usage, access is both free and secure (only cleared law enforcement and antiterrorism professionals have access to the network). The network provides users the following KM benefits:

- Analytical Tools: Government analysts are provided with custom query building and recording tools.
- Collaboration: By connecting emergency response personnel across the country—users have access to a searchable member directory, secure e-mail message boards, and user surveys—a culture of collaboration and sharing is being formed.

- Document Library: The library supports the collection and storage of structured and unstructured data and multimedia content and organizes and categorizes content using a custom-designed taxonomy that permits users to find information following more than one path.
- Document Management: Manages a system for approving and posting documents, workflow management, and back-end document management, including archiving information and knowledge so that it is not lost.
- Feedback: The feedback tool encourages users to comment on system content and technical issues, as well as providing users an opportunity to add new content to the system.
- Integration: The system integrates system content and user communities with independent emergency response applications using Web services.
- Search: LLIS uses a third-party search engine to support full-text searching, category matching, and relevancy ranking.
- Security: LLIS assigns security and access rights to groups and individuals.

Law enforcement agency collaboration and information sharing about terrorists and terrorism is not only a problem in the United States. Box 9.1 describes examples of how the intelligence community in Europe is reacting to this need.

The United States is not the only nation affected by the actions of Muslim extremists and terrorist group activities. Bombings in Bali and Madrid, murders, and plots to set off dirty bombs in the UK are only a few of the terrorist activities taking place around the world. One of the problems in identifying and stopping terrorism in Europe is the porous nature of the borders within and without the European Union. Once inside any of the twenty-five nations composing the EU, it is possible for terrorist suspects to move easily to any other country.

Terrorist organizations have moved many of their planning and fundraising activities to Muslim population enclaves that exist from Norway to Spain and beyond. The intelligence and law enforcement communities of these European countries are finding it extremely difficult to maintain current information databases on terrorists because the needed information-sharing infrastructure is only now emerging.

KM at the FBI

The use of KM tools and processes is not new in government, although not always with the name for the practice. Agency innovators have long used KM to improve collaborative actions, capture and share best practices—a program that gained a strong following during the 1990s empha-

Box 9.1

Building an Information-Sharing Culture in Europe

Networks of Islamic jihadists are reported to exist all across the European Union. They are descendants of guest workers recruited in the years following World War II. Although those guest workers helped to create the postwar economic miracle in Europe, most remain social outcasts. They are, unable or unwilling to become full-fledged citizens of their adopted countries. Many of their children have joined terrorist groups, joining illegal aliens, asylum seekers, and students who came to Europe seeking refuge. Militant minorities in these groups carried out many of the terrorist activities across Europe. They were implicated in the September 11, 2001, attacks on the New York World Trade Center and the Pentagon, bombings in Spain, murders, and more than thirty other terrorist plots.

Many politicians and intelligence bodies in Europe consider terrorism to be a crime problem, not a war. Terrorism activities are considered isolated attacks and not part of a larger, coordinated plot against the West. Some progress in collaboration and coordination is occurring, however. For example, in France, Germany, the Netherlands, Spain, and the United Kingdom police and intelligence officers regularly meet to share information wiretaps and video or satellite photos. Yet, counterterrorism agencies in Europe are still reluctant to share sensitive information or cooperate on prosecutions. Fragmentation and rivalry among the EU's security organizations continue to hamper counterterrorism efforts.

Source: Leiken 2005.

sis on Total Quality Management (TQM)—and provide e-learning (often as distance learning).

The FBI has employed state-of-the-art knowledge management technology for several years, and is now coordinating its antiterrorism investigation and enforcement activities with Homeland Security. The FBI's systems allow the agency to gather, organize, share, and analyze both structured and unstructured data (Schwartz 2003). FBI agents are able to use KM tools to make connections they might never have been able to make earlier. Agents can now access information from other open FBI cases that might be rel-

evant to their own cases. In addition, the bureau has forged agreements and is working out standards for cooperating with the CIA, the DHS, and other intelligence-gathering agencies—a benefit that expands the possibilities for fighting terrorism.

One of the key concerns of the FBI and other agencies involved in counterterrorism activities is how to change the traditional culture of keeping tight control of all intelligence information. Secrecy has been a hallmark of the intelligence network since it was formed. Often critical pieces of information discovered in an investigation were not reported to other agents because a first analyst determined the data to be immaterial. As a result, later analysts were not able to include the bits of information in their take on the situation, thus missing knowledge that might have raised alerts. The FBI has moved to change that culture. Early in 2003, a bureau directive was circulated mandating that all information be shared unless an agent can justify why it should not be. In the past, all FBI case files were restricted to the agent on the case, making it impossible for other agents to know what they contained. Agents working on similar cases could not share information.

The next step in moving to a knowledge-sharing culture was moving information into the FBI's counterterrorism database, the Secure Collaborative Operational Prototype Environment for Counterterrorism (SCOPE). A variety of search engines and other knowledge management tools are used to access and share information in the database. Agents are now able to have all information relating to a case they are working on tagged and sent directly to them without additional searching.

Despite the accomplishments of the bureau and other agencies involved in the war on terrorism, significant challenges remain to be resolved. The biggest challenge still seems to be determining how to share data effectively so that safe, secure, efficient, and effective knowledge management is ensured. The FBI, the CIA, and the DHS must find ways to share knowledge internally, horizontally, and vertically—internally so that all their personnel have access to the information they need when they need it, horizontally with other intelligence agencies at the federal level and internationally, and vertically with state and local law enforcement groups and private-sector security organizations. That is where the systems, procedures, and tools of knowledge management are already helping the FBI and its sister agencies.

Conclusion

The federal government, with only few exceptions, appears to have adopted the knowledge management philosophy that emphasizes sharing of knowledge, and has implemented many of the processes, procedures, and tools

developed for this still-evolving management initiative. State and local governments are still waiting to see whether KM will really provide enough of the performance improvements promised to warrant making the sometimes-substantial investment required.

The federal government's Chief Information Officer Council formed the first knowledge management working group early in 2000. As of 2004, the KMWG had grown to include membership from more than thirty different government organizations.

Among the federal agencies that have been leaders in adopting KM are the General Services Administration, the FAA, NASA, the Department of the Navy, and many others. The chapter also touched upon some of the difficulties agencies such as the Architect of the Capitol, the FBI, and the Department of Homeland Security have encountered in meeting their KM mandates. Later chapters will include in-depth KM application case histories of the experiences of some federal agencies.