Inter Agency Essay

Col. Arthur D. Simons Center
Fort Leavenworth, Kansas

No. 11-03W July 2011

Role of Information Management in Advancing Homeland Security

by David T. Culkin

More than 50,000 malicious codes, including viruses and software, are developed each day to target the United States. Russia, China, and Iran are actively developing capabilities to attack the information infrastructure of this country. At the same time, the Department of Homeland Security and intelligence agencies of the U.S. government do not have a comprehensive plan to address these threats.[1] Decision makers at all levels of government lack timely information to formulate workable courses of action. They also have increasingly less time to make choices that might significantly impact future generations. And they cannot work in isolation. To make decisions more effectively and efficiently, American policy makers must embrace information sharing in a collaborative learning context. In this complex realm of persistent threats and constricted decision cycles, information management is king.

For decades, homeland security decision makers have struggled with information management. It is difficult to gather, organize, and share data with the right people—especially when time is limited. Archives, more than just a collection of dusty books, can assist decision makers by carrying out these functions of information management. For this article, information management is the process to collect, store, and disseminate significant information across all levels of government. Decisions based upon outdated or inaccurate data can be deadly. Security of the homeland suffers when government mishandles this information.

Homeland security is vital because it is the concerted effort to protect the future of our nation. It is a subset of national security and describes the preservation of freedoms, constitutional guarantees, and the rule of law for U.S. citizens at home and abroad.[2] These freedoms and guarantees are under constant threat by individuals, organizations, states, and other nefarious actors who increasingly employ asymmetric means to achieve their objectives. While myriad players hope to undermine American leadership in the world arena, the U.S. government retains responsibility to protect its interests. Rather than utilize traditional military, economic, financial, or bureaucratic tools to address these threats, the real challenge for policy makers is to harness the power of information to their advantage.

The key to advancing homeland security lies in managing information so efficiently and effectively that U.S. policy leaders acquire the understanding they need to make decisions. Many articles have addressed the tangled web of homeland security issues in terms of authorities, budgets, or intelligence resources. The fundamental problem lies deeper: How can stakeholders at all levels of government control, store, and access data so that it can lead to synthesized information

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Role of Information Management in Advancing Homeland Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Command and General Staff College,Col. Arthur D. Simons Center,655 Biddle Blvd., PO Box 3429,Fort Leavenworth,KS,66027**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

and common understanding?

Today's environment has become more complex and interconnected. Redundant networks have replaced concrete bunkers, decision cycles are reduced, and economies are globalized. Archival best practices such as control, storage, and access can hone contemporary information management methodology, thereby improving homeland security decision making. Decision makers can make timely decisions through information management processes which link them to a greater understanding of complex issues. This article examines how applied archival principles can improve current information management processes, thereby optimizing homeland security decisions at all levels.

Current Process & Challenges

The nature of information is messy and ever changing. Information, unlike physical entities, is never complete. Users morph data through analysis and share information to create knowledge. They have learned to tailor information systems to meet their needs.[3] As a consequence, efforts to manage homeland security information over time must be flexible enough to handle constant change while being robust enough to apply order to perceived chaos. Technology and a collaborative attitude among users can facilitate this process.

There are numerous initiatives to share information holistically across the federal enterprise with emerging information technology. Max GOV, ExpertNet, and Wiki are virtual networks. Government civil servants use such social networking and "cloud" tools to collaborate on interagency projects, research interdisciplinary issues, and summon the expertise of experts. Other federally sponsored, multi-user interfaces include Intellipedia, DoD's Techipedia, and Defense Connect Online. Some agencies restrict these resources to disseminate news to their members; others have no distribution policies. The integrated use of social media will continue as the nature of homeland security challenges become increasingly complex.[4] Presidential vision also provides a long-term azimuth for a national approach to information management.

Executive branch policy attempts to enhance information access while ensuring improved efficacy in the use of information. Access does not equate to effective information use; however, access makes knowledge sharing possible. Consider how Mr. X's discrete memorandum emerged to become the national policy known as "containment" during the Cold War. Key information disseminated in an effective manner can propagate powerful decisions. The current model of information management widely in use by homeland security decision makers describes how policy drives the transformation of raw data into shared knowledge.[5]

There are four elements to this model, as depicted in Figure 1. First, stakeholders (individuals and/or groups) apply established or ad hoc processes to collect data to answer their immediate information requirements. Next, they analyze this data to create information which helps them to understand problems systemically. Third, they use information technology to help share synthesized information with other stakeholders. This constitutes the birth of knowledge and facilitates common understanding at the organizational level. Finally, feedback to the stakeholders completes/reinitiates the cycle.

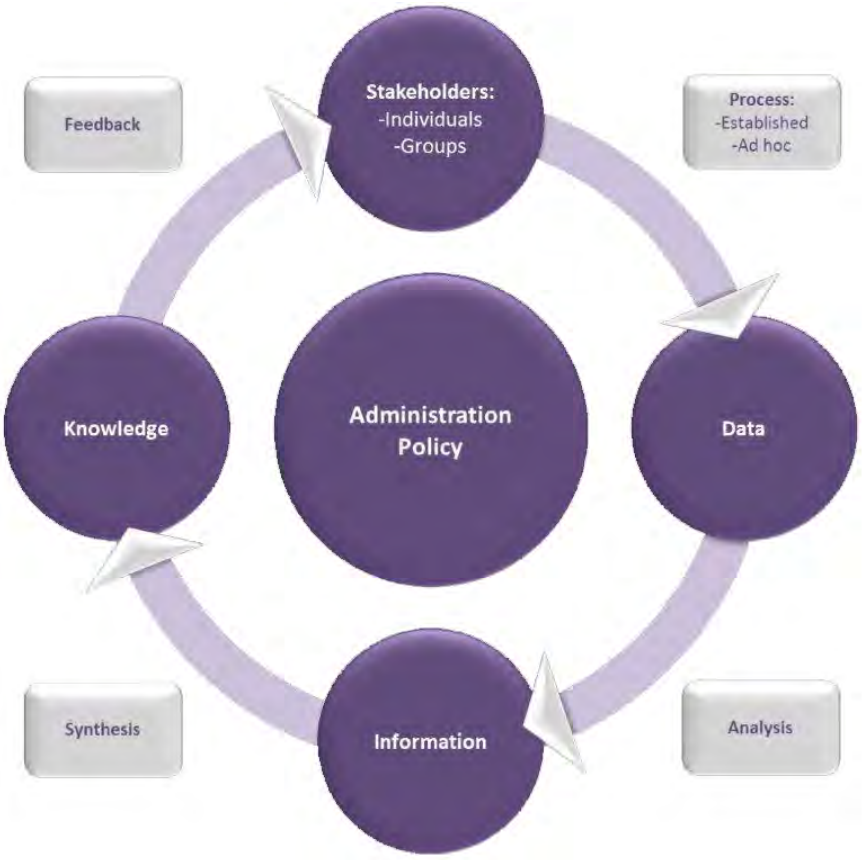

Figure 1: Current Model of Information Management in Homeland Security

This model describes the relationship between homeland security stakeholders and the types of information. What it fails to explain is how these players can use shared knowledge via critical and creative thinking to enhance decision making. Better decisions can lead to better security. Put differently: How can homeland security officials make better decisions with better information?

Decision makers must first assess how the information fits into the context of U.S. homeland security. They analyze data to formulate information that describes the preservation of freedoms, constitutional provisions, and the rule of law for U.S. citizens at home and abroad. They ask how the U.S. can systemically store, share, and manage homeland security information across the government over time. Within this context, there emerge four problems with the current model:

- Problem 1: The legal parameters of privacy are blurred. Some legal theorists believe that it is possible for "cops, spies, and soldiers" to share information in a transparent manner that promotes liberal values of privacy, civilian control of the military, and open channels amongst stake holders.[6] The issue remains controversial largely in part to the direct impact on personal liberties with the Patriot Act.

- Problem 2: It is not easy to translate information into useful knowledge across the U.S. government. Some agencies have taken the initiative to work across bureaucratic and funding boundaries with limited success. For example, the Office of the Coordinator for Reconstruction and Stabilization (S/CRS) at the U.S. State Department regularly implements a multi-part Whole of Government Planning and Execution Process and has developed

products in conjunction with other departments, including the military.[7] The process enables interagency planners to holistically consider various perspectives of problem statements while informing the decisions of diplomats, intelligence officials, and policy makers. While there are initiatives such as these, there remains no one standard to collect, store, and disseminate significant information across the federal enterprise. Furthermore, the current model does not adequately address the information gap between public and private sector interests. The 2010 Deepwater Horizon oil spill disaster highlights the extenuating information-sharing challenges when federal and multiple state authorities intercede in privately managed affairs which directly impact public safety. Despite significant strides since 9/11, decision makers at all levels still do not get the information they need when they need it.

- Problem 3: We must protect records from natural and man-made disasters. Consider the impact that disasters have had on records. Hurricane Katrina, for example, damaged portions of the archives of several inadequately protected institutions. Information professionals have repeatedly echoed their concern about the dilapidated status of the national information infrastructure.[8] A tsunami in 2009 inundated several archival holdings in American Samoa. Collaborative efforts among the Federal Emergency Management Agency, StarKist, and territorial archivists led to wide-ranging lessons learned as well as a validation of archives' value in "response and recovery, and…in rebuilding damaged communities."[9] We must also safeguard classified digital records. WikiLeaks' recent disclosures demonstrate that the need for protection extends beyond the physical realm. Cybersecurity involves not only national security but also how archives can describe accurately the provenance of records handled illegally by third parties.[10] Disasters, natural and man-made, are inevitable. A comprehensive national strategy should address the measures and resources needed to protect all records of historical and social value.

- Problem 4: There are technological implications of ensuring access over time. Information scientists and archives continue to wrestle with the notion that the technological modes of storage increasingly change over time. Consider how modes such as 8-track tapes and microfilm, once deemed cutting edge technology, are now obsolete. How can future generations preserve and access their information? The National Archives and Records Administration has had some success in developing digital protocols which would allow electronic data and metadata to migrate from obsolete to current modes of storage while mitigating loss.[11] Nevertheless, full implementation of such programs remains a distant objective.

Government should not only gather and analyze information but also synthesize knowledge effectively to understand and respond to critical issues. This information fusion would help ensure policy makers attain a deeper understanding of critical issues. Record keepers play a key role in this arena.

Modern archival practice has helped refine the functions of record keeping. One way to describe these functions is the acronym CADSS: control, accessibility, disposal, storage, and sustain.[12] Control is the acquisition and physical security of primary materials entrusted to private or public record keepers. Policies help standardize how records are stored and ultimately located. Only by establishing a stable level of control can an archive guarantee a reliable degree of access to researchers. Accessibility implies risk to primary materials. The more physical records are manipulated, the more fragile they become. Digital technology has enabled custodians to preserve records and concurrently make them accessible to the public. Disposal concerns the quality of

policies which govern the handling and disposition of records. For example, permanent accession policies directly affect how all records are stored and maintained. Storage and sustain functions relate to the risks and opportunities associated with records keeping. An archive has fulfilled its role when records are stored so that they and their component information are accessible over extended periods of time. Archival best practices help ensure a legitimate level of accountability and transparency.

With increased engagement comes the demand for greater transparency in homeland security issues. Accountability is the way record keepers achieve a condition of mutual awareness between citizens and their governments. Australian researchers have determined that there are discernible elements to accountable record keeping. The key ingredients include an independent recordkeeping authority, established best practices, compliant information systems, and cooperative relationships with other stakeholders.[13] These components constitute success criteria for any process of information management. A model which promotes responsible governance through transparency at all levels will improve information management in homeland security decision making.

A revision of the information management model previously described could better apply the core functions of archival record keeping (CADSS) in a homeland security context. It would stipulate a systemic way of controlling, accessing, disposing, storing, and sustaining interdisciplinary records that is currently unrealized. Furthermore, it calls for more accountable interagency records keeping policies by requiring transparency, with reasonable national security caveats. Updating the process of information management through archival best practices is feasible and necessary.

An Updated Model

Stakeholders possess the means and motivation to update the current model of information management. The stakes are high, but the solution is attainable. Rather than top-down policy driving the reformation, bottom-up action would help key stakeholders commit to a cooperative, long-term solution based upon accepted archival practices. The key is a grassroots effort to inculcate a fresh perspective, seek migratory capability, and employ ever-evolving information technology. To update the current model, stakeholders must replace top-down policy with these components so that they drive collaborative decision making (see Figure 2).

Decision makers must willingly collaborate with information managers and take a long-term perspective. All decision makers must be willing to accept abbreviated decision cycles supplied by timely but incomplete data in complex environments. They must take a holistic and systemic view of their environment to determine sensible ways ahead. Information managers and record keepers must focus their efforts on ensuring continued access to and control of increasingly fleeting information. All stakeholders must acknowledge that a cooperative understanding of the contemporary homeland security domain is no longer "an advantage" but a downright necessity. A collaborative approach among decision makers and information managers would address legal parameters (Problem 1) because it would place the issue in public debate from the outset. This lengthened perspective from the practitioner level would replace "Administration Policy" as the primary driver of the revised information management model.

To realize a broader perspective across entrenched institutional boundaries, stakeholders can seek migratory capability. This capability assumes that information can have value regardless of space and time. The concept extends beyond the recent mobility of phones and computers, and can have significant implications for decision makers in homeland security. For instance, after the 2009 tsunami, archival officials in American Samoa implemented a policy whereby all backup re-

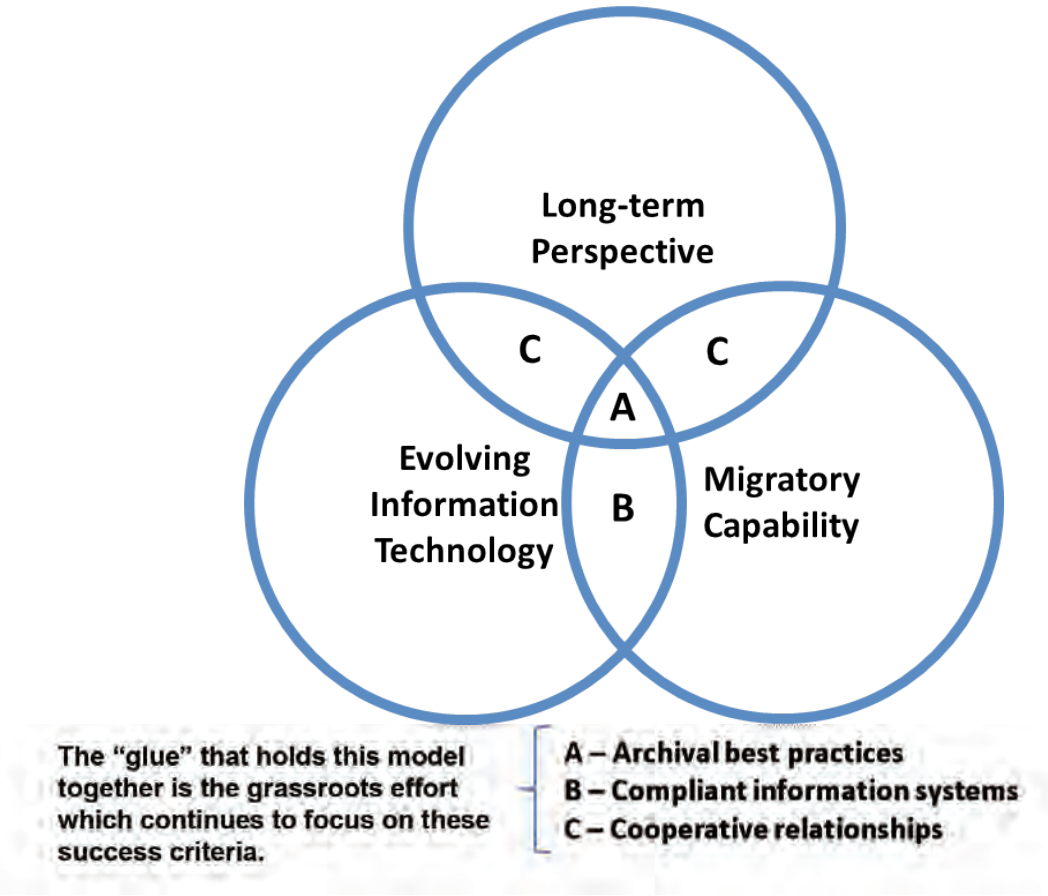

Figure 2: Improving Information Management

cords are now separately housed off island.[14] The ramifications for the protection of records from disasters are obvious (Problem 3). Securing data through repetitive and distributed networks can also make information more readily accessible to more users (Problem 2). This focus on capability rather than "technology of the now" will foster long-term approaches to systemic issues.

Constantly evolving information technology is another critical facet of the revised model because it directly affects the efficiency and thus the effectiveness of archival practices. Technological advances such as the Electronic Records Archives will soon migrate data continuously and reliably from obsolete to maintainable storage systems (Problem 4).[15] While the technology continues to change over time, stakeholders' participation will remain constant. The new model emerges when these interlocked spheres replace policy as the primary driver of information management in homeland security.

The revised model suggests that the grassroots efforts by practitioners are the glue which holds the components together (see Figure 3). The intersections among these facets are the specific success criteria previously mentioned. When stakeholders incorporate a long-term perspective, current information technology, and migratory capability, they necessarily optimize information management for homeland security decision makers. The efficiency and resultant effectiveness of this revived information management process can then be measured in terms of archival principles, information systems compliance, and the growth of cooperative relationships. This linkage ultimately translates into improved homeland security. The grassroots movement is on the march.

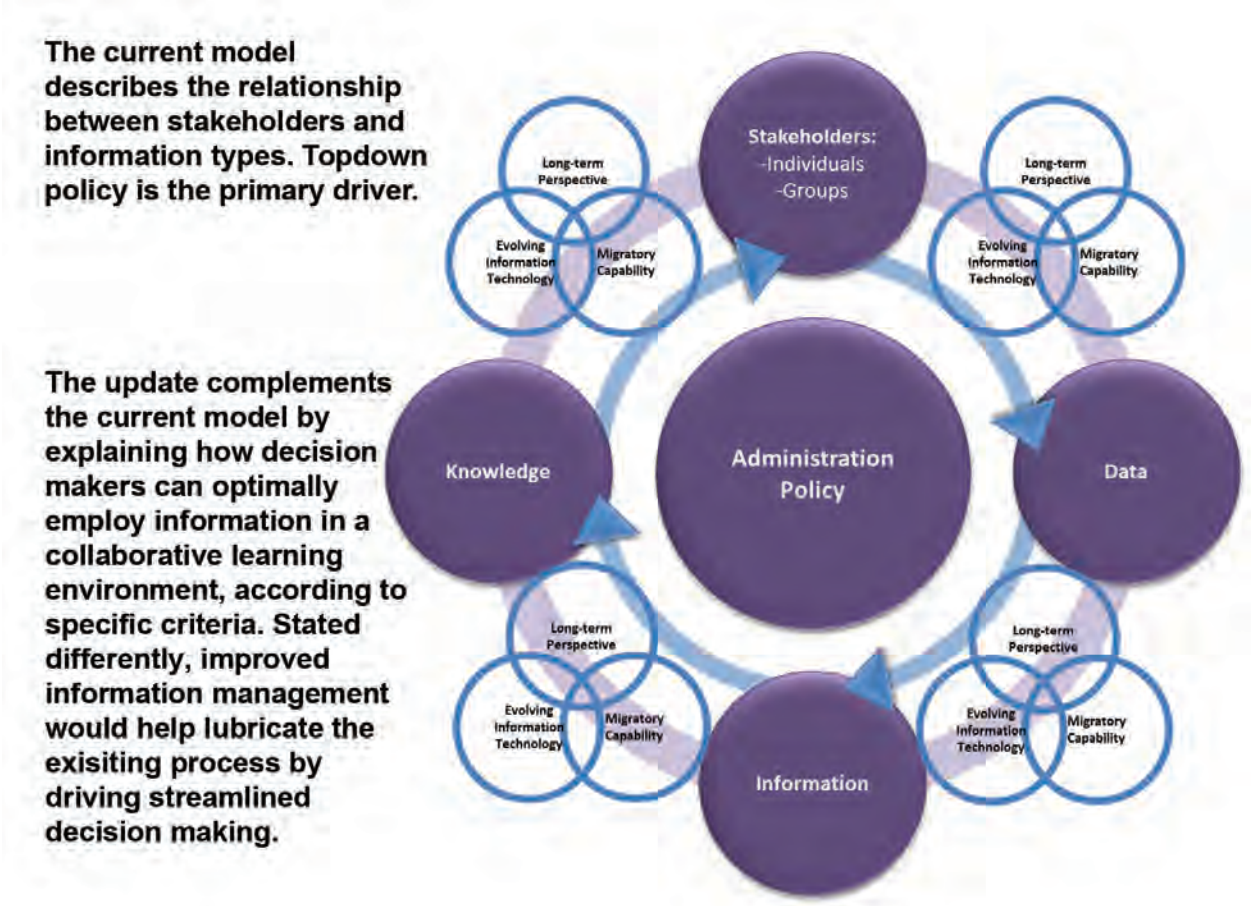

Figure 3: A More Complete Model

The updated model optimizes the information management process for homeland security decision makers. It fulfills President Obama's vision of strengthening partnerships related to data preservation, privacy, and network defense (Problem 3).[16] Furthermore, recent counterterrorism policy emphasizes proactive measures to share information across the government and to strengthen analytical capabilities to protect the homeland.[17] Increased awareness of information management has thus enabled streamlined decision making in homeland security.

Archives will continue to play a key role in promoting security policy. They help manage the public and private resources critical to homeland security. The British Archives recently published a strategy which acknowledges the direct role of archives in policy development: "Archives can, and indeed in many cases do, make a clear contribution to the delivery of local policy initiatives, often through partnerships with other cultural, learning and information organisations."[18] A key element of this is the ability to foster and maintain relationships with sponsors, other agencies, and the public. This is the primary means by which an archive can influence policy makers within the updated model. Archival communities have a direct role in collaboratively advancing information management for the benefit of homeland security.

Homeland security officials are adopting policies and processes which aim to improve information management at all levels. The White House has proposed that new cybersecurity legislation encourage private interests—which own up to ninety percent of the nation's infrastructure—to

develop plans to defend their networks and report security breaches.[19] Defense Secretary Gates issued a memorandum at the beginning of 2011 to establish a principal staff advisor to be the primary liaison for the Defense Department with other agencies.[20] This internal policy will help overcome the salient barriers to interagency communication and resource sharing.

As the Principal Deputy Under Secretary for Intelligence and Analysis for the Department of Homeland Security attests, the department has established seventy-two fusion centers which attempt to link gaps in the national information architecture. These centers collect data from various sources, conduct analysis, and disseminate information to law enforcement and first-response agencies at all levels.[21] The department's open participation in government-wide planning and operational activities indicates it is sensitive to the public's security needs as well as demands for accountability. Collaboration must occur among three entities: 1) government agencies which create policy; 2) private industry which manages critical infrastructure; and 3) public consumers (Problem 2). Regardless of the policies pursued, a systemic approach would connect resources to information demands across bureaucratic chasms and set the conditions for a holistic understanding of complex security issues.

The updated model of information management is simple enough to articulate and implement over time. Systemic thinking can help record keepers from diverse organizational cultures understand fundamental problems first and collaborate more effectively to achieve common goals for future generations.

Conclusion

Archival principles can improve current homeland security information management processes and, ultimately, decision making. The key to promoting homeland security lies in managing information so efficiently and effectively that U.S. policy leaders have the understanding they need to make significant and timely decisions. Decision makers must first agree to recognize the heightened role of information management. They then can apply archival best practices such as control, storage, and access to streamline the information management methodology. The disciplined operation of the updated model will foster timely and accurate decision making in the homeland security realm.

Imagine a day when there is a standard means to collect, store, and disseminate significant information across the government. It will significantly strengthen the security of the homeland, and it may be closer than you think. Indeed, nothing is impossible for the king that is information management.

Endnotes

1. Alex Wagner, "US Vulnerable to Terrorism, Especially Cyber Attacks, Intelligence Chiefs Say," retrieved on 13 April 2011 at http://tinyurl.com/3wvdwl2.

2. U.S. Department of Defense, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, accessed at https://jdeis.js.mil/jdeis/index.jsp on 7 February 2011. Homeland defense is a more specific term which pertains mainly to activities of the Department of Defense. See also JP 3-28.

3. Dennis N. Hart and Shirley D. Gregor, Editors, Information Systems Foundations: The Role of Design Science, The Australian National University E Press, Canberra, 2008, pp. ix and 4. Available at http://epress.anu.edu.au/is_foundations_citation.html.

4. Kate Theimer, "Thing 3: what is Web 2.0?" accessed on 7 July 2011 at http://23thingsforarchivists.wordpress.com/beginning-things-1-23/thing-3/. "23 Things" is a great resource for anyone to learn more about interactive technology.

5. Michael Gurstein, "Open Data: Empowering the Empowered or Effective Data Use for Everyone?" 7 February 2011, First Monday, Vol. 16, No. 2, p. 2, accessed on 7 February 2011 at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3316/2764. Michael Gurstein's effective use model can inform a reasonable approach which maps the processes whereby raw data produced by a single office can become shared knowledge across the federal enterprise.

6. Nathan A. Sales, "Mending Walls: Information Sharing After the USA PATRIOT Act," Texas Law Review, Vol. 88, p. 1854.

7. Merrie Archer, "The Whole of Government Planning Process," U.S. Department of State, Washington, D.C., 18 February 2011. Ms. Archer is a senior planner with S/CRS and presented these remarks at Ft. Leavenworth.

8. Blake Ives and Iris Junglas, "Information Systems at Northrop Grumman Ship Systems Sector: The Hurricane Katrina Recovery," Communications of the Association for Information Systems, Vol. 18, 2006, p. 558.

9. Tom Clareson, "Big Ideas to Battle Monster Disasters," Archival Outlook, Society of American Archivists, March/April 2011, p. 8.

10. Rachel Miller, "The WikiLeaks Phenomenon," Archival Outlook, Society of American Archivists, March/April 2011, p. 26.

11. See Steven Puglia, Jeffrey Reed, and Erin Rhodes, "Technical Guidelines for Digitizing Archival Materials for Electronic Access: Creation of Production Master Files—Raster Images," National Archives and Records Administration, June 2004, accessed on 25 February 2011 at http://preview.tinyurl.com/4q5aree.

12. Ann Pederson, "What Goes on in the Archives?" John Curtin Prime Ministerial Library, accessed on 22 February 2011 at http://john.curtin.edu.au/society/index.html.

13. Ann Pederson, "What is an Effective Recordkeeping Regime?" John Curtin Prime Ministerial Library, accessed on 22 February 2011 at http://john.curtin.edu.au/society/archives/index.html.

14. Clareson.

15. National Archives and Records Administration, "Electronic Records Archives (ERA)," accessed on 26 April 2011 at http://www.archives.gov/era/about/index.html.

16. Barack Obama, "National Security Strategy," May 2010, p. 28.

17. Barack Obama, "National Strategy for Counterterrorism," June 2011, p. 12.

18. B. Andrews, B. Follett, and M. Wills, Archives for the 21st Century (consultation draft), HM Government, United Kingdom, 2009, p. 1.

19. Tom Gjelten, "U.S. Outlines Cybersecurity Initiative," National Public Radio, 12 May 2011, accessed on 16 May 2011 at http://www.npr.org/2011/05/12/136250408/obama-lays-out-cybersecurity-plan. See also http://tinyurl.com/3vp4rnl.

20. Robert M. Gates, "Strategic Communication and Information Operations in the DoD," Memorandum for Secretaries of the Military Departments, 25 January 2011, p. 1.

21. Bart R. Johnson, "How Fusion Centers Help Keep America Safe," 25 October 2010, US Department of Homeland Security Leadership Journal, accessed on 23 February 2011 at http://tinyurl.com/44xzdgf.

About the Author

Lieutenant Colonel David T. Culkin is an Army strategist currently serving as an instructor in the Department of Joint, Interagency, and Multinational Operations at the U.S. Army Command and General Staff College, at Fort Leavenworth, Kansas. He is a graduate of the Army's School of Advanced Military Studies and has served in various command and planning positions in Hawaii, Korea, and the U.S. Strategic Command. He holds a Masters of Library and Information Science from Florida State University.

InterAgency Essay Series

The ***InterAgency Essay*** (*IAE*) series is published by the Simons Center for the Study of Interagency Cooperation. The series is designed to provide an outlet for original essays on topics that will stimulate professional discussion and further public understanding of the interagency aspects of national security issues encountered at the tactical and operational levels.

This essay represents the opinions of the author(s) and does not reflect the official views of the Department of the Army, the Department of Defense, the United States Government, the Simons Center, or the Command and General Staff College Foundation.

Contributions: The Simons Center encourages the submission of original essays based on research from primary sources or which stem from lessons learned via personal experiences. For additional information see "Simons Center Writers Submission Guidelines" on the Simons Center website at www.TheSimonsCenter.org/publications.

About the Simons Center

The Col. Arthur D. Simons Center for the Study of Interagency Cooperation is a major component of the Command and General Staff College Foundation. The Center's mission is to foster and develop an interagency body of knowledge to enhance education at the U.S. Army CGSC while facilitating broader and more effective cooperation within the U.S. government at the operational and tactical levels through study, research, analysis, publication and outreach.

About the CGSC Foundation

The Command and General Staff College Foundation, Inc., was established on December 28, 2005 as a tax-exempt, non-profit educational foundation that provides resources and support to the U.S. Army Command and General Staff College in the development of tomorrow's military leaders. The CGSC Foundation helps to advance the profession of military art and science by promoting the welfare and enhancing the prestigious educational programs of the CGSC. The CGSC Foundation supports the College's many areas of focus by providing financial and research support for major programs such as the Simons Center, symposia, conferences, and lectures, as well as funding and organizing community outreach activities that help connect the American public to their Army. All Simons Center works are published by the "CGSC Foundation Press."

Col. Arthur D. Simons Center
655 Biddle Blvd., PO Box 3429
Fort Leavenworth, Kansas 66027
ph: 913-682-7244
www.TheSimonsCenter.org

CGSC Foundation, Inc.
100 Stimson Avenue, Suite 1149
Fort Leavenworth, Kansas 66027
ph: 913-651-0624
www.cgscfoundation.org