2007-03

Requirements and information metadata system

Beckman, Erin M.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

REQUIREMENTS AND INFORMATION METADATA SYSTEM

by

Erin M. Beckman

March 2007

Thesis Advisor:	Robert L. Simeral
Second Reader:	Anthony Kendall

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2007	Master's Thesis

4. TITLE AND SUBTITLE Requirements and Information Metadata System	5. FUNDING NUMBERS
6. AUTHOR Erin M. Beckman	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	A

13. ABSTRACT

This thesis proposes an adoption of a data schema called RIMS (Requirements and Information Metadata System) developed as a pilot project in the Pittsburgh Field Office of the FBI and sets out to determine if RIMS could be an effective and efficient method to capture, catalogue and retrieve intelligence information within the Federal Bureau of Investigation (FBI). RIMS would enhance the search platform used by FBI analysts and investigators who gather or data mine existing information in furtherance of the FBI's priorities.

The use of this coding system can be adapted for use by other U.S. intelligence and law enforcement communities for commonality and uniformity in retrieval, cataloguing, and collecting of intelligence information. The use of this system can be manipulated into a non-classified code for use by state, local, and tribal law enforcement and intelligence entities. Finally, the use of the coding system within the intelligence community will consolidate and integrate information and intelligence and reduce delays in detecting and retrieving pertinent intelligence obtained and shared within the intelligence community.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Sharing, Intelligence Community, Metadata, Integrate Information, Intelligence, Information Tagging	87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

REQUIREMENTS AND INFORMATION METADATA SYSTEM

Erin M. Beckman
Supervisory Special Agent
Federal Bureau of Investigation
BA – Business/International University of Pittsburgh, Pittsburgh, Pennsylvania

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2007

Author: Erin M. Beckman

Approved by: Robert L. Simeral
Thesis Advisor

Anthony Kendall
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis proposes an adoption of a data schema called RIMS (Requirements and Information Metadata System) developed as a pilot project in the Pittsburgh Field Office of the FBI and sets out to determine if RIMS could be an effective and efficient method to capture, catalogue and retrieve intelligence information within the Federal Bureau of Investigation (FBI). RIMS would enhance the search platform used by FBI analysts and investigators who gather or data mine existing information in furtherance of the FBI's priorities.

The use of this coding system can be adapted for use by other U.S. intelligence and law enforcement communities for commonality and uniformity in retrieval, cataloguing, and collecting of intelligence information. The use of this system can be manipulated into a non-classified code for use by state, local, and tribal law enforcement and intelligence entities. Finally, the use of the coding system within the intelligence community will consolidate and integrate information and intelligence and reduce delays in detecting and retrieving pertinent intelligence obtained and shared within the intelligence community.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my gratitude to all Homeland Security professionals who continue to protect America on a daily basis. Their diligence, focus, and professionalism are not always publicly recognized but their daily activities and attention to the numerous complex homeland security issues keep all of us safe.

I would also like to thank the Naval Postgraduate School and the Center for Homeland Defense and Security (CHDS) for the opportunity to study this important topic which affects so many. Special thanks to the CHDS faculty and the many instructors who guided our class in broadening our perception of homeland security and defense.

Thesis advisors, Robert Simeral and Walter Kendall, have provided guidance during the CHDS experience. Thank you gentlemen for your patience and guidance. Special acknowledgement goes to Lauren Wollman who guided all of us through the thesis process. Editor Janis Higginbotham's time and work was greatly appreciated and I thank you. I also thank Nancy Sharrock and Pam Silva in Thesis Processing.

I would like to thank all my classmates at CHDS for the camaraderie and new viewpoints that were expressed which all of us benefited from during the last 18 months.

I would also like to express my appreciation to the Federal Bureau of Investigation for allowing me the time to attend this program. Special thanks goes to M. Chris Briese and Owen Harris for allowing me to "think outside the box" and support my work. Additionally, I thank all the analysts and special agents that I have worked with since late 2005 to develop and validate the RIMS coding system. Their imput was valuable in order to develop this system.

Finally, without the support of my family and friends, I would not have been able to accomplish this program. Thank you for allowing me to bounce a lot of ideas off all of you and for your patience in missed time with you over the past 18 months.

.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Our job is to effectively integrate foreign, military and domestic intelligence in defense of the homeland and of United States interests abroad.

—John D. Negroponte
Director of National Intelligence

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

Let me tell you about three areas where I plan to focus our efforts to achieve that goal. First, we need to operate under a ***common picture of threats*** *we are facing. Second, we need to* ***respond actively*** *to these threats with the* ***appropriate policies****. Third, we need to* ***execute*** *our various* ***component operations in a unified manner*** *so that when we access the intelligence and we have decided upon the proper policies, we can carry out our mission in a way that is coordinated across the board .*

— Secretary Chertoff, *Statement for the Record Before the United States Senate Subcommittee on Homeland Security,* 20 April 2005.

A. PURPOSE

The purpose of this thesis is to describe an intelligence and information tracking system that can support Federal Bureau of Investigation (FBI) activities and allow for the FBI's integration and support to the United States Intelligence Community (USIC). This system will allow a transition from the FBI's existing information sharing and collaboration environment to an environment that will better support the FBI in meeting its goals and mission objectives.

This thesis is intended not only to describe opportunities for better information sharing and collaboration within the FBI enterprise in order to make informed choices,

but also to support subsequent work to realize the benefits. In short, this thesis should be used as a long-range guide to drive results in the FBI's mission to successfully integrate and support the USIC.

B. BACKGROUND

The attacks of September 11, 2001, moved forward the longstanding call for major intelligence reform and the creation of a Director of National Intelligence (DNI). [1] Post-9/11 investigations included a joint Congressional inquiry and the National Commission on Terrorist Attacks Upon the United States (better known as the 9/11 Commission). The report of the 9/11 Commission[2] in July 2004 proposed sweeping change in the Intelligence Community. President George W. Bush signed four Executive Orders in August 2004 addressing structural and institutional changes. In Congress, both the House and Senate passed bills with major amendments to the National Security Act of 1947. Intense negotiations to reconcile the bills ultimately led to the Intelligence Reform and Terrorism Prevention Act of 2004, which President Bush signed into law on December 17, 2004. [3]

Since the attacks of September 11, the overriding priority of the FBI has been protecting America by preventing future attacks. The FBI has refocused its priorities to better accomplish its mission and is making comprehensive changes in its overall structure, organization, and business practices. Even as it evolves, the FBI continues to

[1] The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC). The DNI also acts as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; The DNI also oversees and directs the implementation of the National Intelligence Program. The President appoints the DNI with the advice and consent of the Senate. The Director is assisted by a Senate-confirmed Principal Deputy Director of National Intelligence (PDDNI), appointed by the President with the advice and consent of the Senate. Material and information pertaining to the Director of National Intelligence can be found at http://www.dni.gov/ (Accessed January 28, 2007).

[2] The National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission), an independent, bipartisan commission created by congressional legislation and the signature of President George W. Bush in late 2002, is chartered to prepare a full and complete account of the circumstances surrounding the September 11, 2001, terrorist attacks, including preparedness for, and the immediate response to, the attacks. The Commission is also mandated to provide recommendations designed to guard against future attacks. Full background on the 9/11 Commission can be found at http://www.9-11commission.gov/ (Accessed November 1, 2006).

[3] Full background on the IRTPA can be found at the Library of Congress site: http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.02845 (Accessed January 28, 2007).

meet its traditional responsibilities to uphold and enforce federal criminal laws of the United States and to provide leadership and criminal justice services to federal, state, municipal, tribal, and international agencies and partners. The FBI remains committed to performing these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution and the laws of the United States.[4]

The FBI's top three priorities are: 1) protecting the United States from terrorist attack; 2) protecting the United States against foreign intelligence operations and espionage; and 3) protecting the United States against cyber-based attacks and high-technology crimes. In addition to these missions, the FBI continues to combat public corruption at all levels, protect civil rights, and combat major white-collar crime and significant violent crime.[5]

On June 28, 2005, the president directed the FBI to create a "National Security Service" within the FBI. The attorney general was to implement the White House Memorandum entitled "Strengthening the Ability of the Department of Justice to Meet Challenges to the Security of the Nation," "subject to the availability of appropriations and in a manner consistent with applicable law, including the Constitution and laws protecting the freedom and information privacy of Americans."[6] This directive was implemented through the creation of a new organization — the *National Security Branch* (NSB) — that integrates the FBI's primary national security programs under the leadership of a single FBI official, and through policies and initiatives designed to enhance the capability of the entire FBI to support the nation's national security mission.

The NSB consists of the Counterterrorism Division, the Counterintelligence Division, the Weapons of Mass Destruction Directorate, and the Directorate of Intelligence. The NSB promotes the development of a national security workforce with

---

[4] FBI Public Website. http://www.fbi.gov/libref/historic/history/text.htm (Accessed November 3, 2006).

[5] FBI Public Website. http://www.fbi.gov/quickfacts.htm (Accessed November 3, 2006).

[6] The Memorandum for the Vice President, Secretary of State, Secretary of Defense, Attorney General, Secretary of Homeland Security, Director of OMB, Director of National Intelligence, Assistant to the President for National Security Affairs, and Assistant to the President for Homeland Security and Counterterrorism can be found at http://www.whitehouse.gov/news/release/2005/06/print/20050629-1.html (Accessed November 12, 2006).

the skills, training, and experience necessary to carry out our national security investigative and intelligence programs. It also coordinates our national security efforts with the rest of the Intelligence Community under the leadership of the DNI.[7]

Following the events of September 11, 2001, the FBI underwent a significant expansion of its mission responsibilities and a reordering of its priorities to emphasize its counterterrorist mission, though it still retains its important criminal investigation mission. The FBI recognized it would become ever more dependent on information technology in the future to manage the large quantities of information associated with these missions. It is challenging, for any organization engaged in a complex set of activities, to introduce new technologies and to reengineer its key processes to exploit them effectively. It is doubly challenging, as it is for the FBI, to do so when under intense operational pressures—the FBI's traditional work must continue while new technology is introduced and while a culture more adapted to the use of IT evolves. And it is triply so for the FBI in the face of the added strain of its new focus—preventive counterterrorism—in which mission success demands a different mind-set, different operational skills, and the exploitation of an expanded set of information sources.

With the recognition of the dependence upon information technology in the future, the FBI challenged itself to create an interoperable information-sharing environment within the FBI, which would enable the interchange of information among and between FBI entities. This challenge enabled visionary leaders within the FBI to create an information-sharing environment that could be integrated among and between appropriate law enforcement and intelligence partners. This innovative thinking led to the initial development of a ten to thirteen metadata code called Requirements and Information Metadata System (previously called "RICS" by one FBI field division). The use of this coding system was a method to identify, catalogue, and retrieve intelligence information within the FBI.

[7] FBI Public Website. http://www.fbi.gov/hq/nsb/nsb.htm (Accessed March 8, 2007).

C. PROBLEM

A disquieting trait of twentieth and twenty-first-century terrorist or surprise attacks is that the victims later discover they already possessed a substantial amount of information that might have prevented or mitigated the attack. There have been intelligence successes and failures involving attacks by terrorists involving the United States (U.S.). U.S. intelligence agencies already had information in their possession which, if properly assessed and disseminated, might have disrupted, deterred, or perhaps even prevented the attacks on September 11, 2001 (9/11) or the 1993 World Trade Center bombing.

1. Connecting Clues and Intelligence

In the summer of 2001, the Central Intelligence Agency (CIA) received information that al-Qaeda was plotting to use aircraft as flying bombs against symbolic American targets.[8] The CIA passed the information to the FBI. That same summer, the FBI office in Phoenix alerted FBI Headquarters that an "inordinate number of persons of investigative interest" were enrolled at flight schools in Arizona.[9] The Minneapolis FBI office actually arrested one of these persons, Zacarias Moussaoui, and asked for permission to search Moussaoui's laptop computer. Permission was denied. The Minneapolis Special Agent in Charge of the case persisted: He was trying, he said, to make sure that Moussaoui "did not take control of a plane and fly it into the World Trade Center." He got back this answer from the New York field office: "That's not going to happen. We don't know he's a terrorist. You have a guy interested in this type of aircraft – and that's it."[10]

Clues that connected one terrorist to another were frequently missed. At that time, no information technology system was in place to connect the clues and intelligence coming into the various field divisions or FBI Headquarters. "Furthermore, New York

[8] U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks on September 11, 2001, S. Rept No. 107-351, H. Rept. No. 107-792 (December 2002), 212.

[9] Ibid., 325.

[10] Ibid., 323-24.

prosecutors who investigated the 1990 killing of the extremist rabbi Meir Kahane insisted against the evidence that his murderer acted alone. In 1993, they discovered that Kahane's killer belonged to the same cell that tried to blow up the World Trade Center – but awareness of that earlier mistake did not prod investigators to follow the next round of clues linking the World Trade Center bombers to international terrorist organizations and foreign governments."[11] No one in the U.S. government had a tracking or tagging mechanism in place to catch anomalies, similarities, or to quickly share such analyzed information to prevent future attacks such as the events on September 11.

2. Legal Issues: Tracking Threats Against America

The CIA tracks foreign threats. Should the terrorist enter the U.S., the CIA hands responsibility to the FBI, which is charged with defending Americans against domestic dangers. The FBI was essentially a federal police force that goes to great lengths to respect the constitutional rights of the suspects it investigates. That was why the FBI refused to authorize the search of Moussaoui's computer. He was not an American citizen under the protection of the American Constitution nor was he a criminal suspect. "He was believed to have been a combatant of a hostile army, an army whose sole purpose was to commit atrocities against American citizens."[12]

The strict rules imposed on the FBI in 1995 were intended to safeguard the division between criminal investigations and counterterrorism. Counterterrorism agents believed they were forbidden to talk to people on the criminal side who might have knowledge about their case. As Richard Clarke, the former chief of counterterrorism at the National Security Council told a joint congressional committee in 2002, the FBI "didn't have the mission. It was not their job to be a domestic [intelligence] collection service. Their job was to do law enforcement. And they didn't have the rules that permitted them to do domestic intelligence collection."[13]

---

[11] David Frum and Richard Perle, *An End To Evil – How To Win the War on Terror* (New York: Ballantine Books, 2003) 7: 165-167.

[12] Ibid., 168.

[13] Frum and Perle, *An End To Evil – How To Win the War on Terror,* 37.

3. FBI Lacked Central Search Platform

The FBI also did not have the interoperable terrorism information-sharing environment needed to fully exploit the information collected across the U.S. Stove-piped investigative applications were prevalent and no central search platform existed to gather information or data mine the myriad of information gained daily from active FBI investigations and sources.

The FBI needed to replace the established information technology (IT) enterprise framework, which stove-piped investigative applications with an improved approach to collect and manage FBI case and investigative information. Additionally, the system must support the operational mission of the FBI by enhancing its information management capabilities. The collection, dissemination, and availability of data and investigative tasking across the entire organization will enable the assembly and management of case information for intelligence and investigative activities and will support rapid and effective information sharing among FBI personnel and with authorized external agencies.

4. Current Information-Sharing Environment

Currently, there is no central search platform to gather information or data mine within a genre of information. Training on data mining and searching the various databases is minimal. Some FBI field offices have taken formative steps to establish structured, relational databases to facilitate robust case management and intelligence support to operations. These offices have elected to use a commercially available, off-the-shelf software analytical application called iBase, which is produced by an IT industry software applications company called i2 INC. In addition, several operational units at FBI Headquarters adopted similar approaches using structured, relational database packages. Ultimately, the FBI must establish an enterprise-wide standardized approach for classifying investigative information into a structured, relational database environment to benefit fully from this technology.

The well-publicized FBI Trilogy Information Technology Modernization Program (Trilogy) did not provide an effective return on the FBI's IT investment (measured in

operational terms—more and better results, increased responsiveness and agility, and improved efficiency of operations).[14] In February 2005, the FBI told the Senate Appropriations Subcommittee on Commerce, Justice, State and the Judiciary that the Trilogy project failed and the FBI wasted $104 million. During the hearing, FBI Director Robert S. Mueller III took some of the responsibility for the Trilogy catastrophe. He assigned the rest of the blame to vendor Science Applications International Corporation. The Department of Justice's Inspector General's Office produced a report that cited several reasons for the failure of the Trilogy project, including: (1) Virtual Case File design modifications made as a result of the FBI's shift from criminal investigations to preventing terrorism, following the Sept. 11, 2001, attacks; (2) poor management decisions early in the project; (3) inadequate project oversight, and (4) a lack of sound IT investment practices.[15]

Trilogy limited the FBI's ability to partner with other U.S. intelligence entities and fully share homeland security information. A new system, SENTINEL, under development by the FBI, plans to transform the way the FBI does business, allowing the FBI to move from a paper-based reporting system to an electronic system of records, as well as eliminating the redundancy in maintaining multiple systems and bottlenecks. SENTINEL will provide a versatile capability to locate different types of information contained within SENTINEL. It will support the preparation and execution of a multitude of different search queries. This capability will be both flexible and powerful to accommodate the substantial volume and wide variety of information available for retrieval in SENTINEL.[16]

---

[14] National Research Council, *A Review of the FBI's Trilogy Information Technologies Modernization Program*, Computer Science and Telecommunications Board, National Academies Press, Washington, D.C., 2004.

[15] The Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, Audit Report Number 05-7, February 2005.

[16] "Information Technology Issues at FBI, Office of the Chief Information Officer" http://www.fedsources.com/events/download/ZalmaiAzmi.pdf (Accessed February 20, 2007).

5. The FBI Vision of an Interoperable Terror Information-Sharing Environment

The Requirements and Information Metadata System (RIMS) can be integrated into SENTINEL with minimal impact. RIMS uses the current FBI information technology structure. SENTINEL will employ a service-oriented architecture that is compatible with the FBI's Enterprise Architecture, which incorporates all of the FBI business functions. SENTINEL will allow FBI personnel to employ intranet technologies to enter, organize, search, and retrieve information and to import, export, and share case-related information. SENTINEL will replace the legacy system, Automated Case Support (ACS), and assimilate their functionality. SENTINEL will be capable of exchanging information with multiple systems internal to the FBI and will support information sharing with External Agencies.

The FBI is involved in information acquisition and the workflow of information management—how information is acquired, who must act on it, how information of all types flows within the FBI, how it must be processed and analyzed, and what types of inferences must be drawn. For information-intensive missions such as criminal investigation and counterterrorism, modern IT and its proper design and exploitation are critical contributors to truly effective processes. Data must be organized and managed in a way to promote the effectiveness of FBI agents and intelligence analysts. Access capabilities required for intelligence analysis in order to determine possible events in the future are crucial to the FBI as it continues to build a viable domestic intelligence agency and supports the U.S. Intelligence Community (USIC).

Three events depict how the FBI continues to strive for a versatile system which will provide powerful retrieval, information-capture, and cataloguing of huge quantities of information and data.

1. The FBI created a new National Security Branch (NSB) within the FBI and under a single Executive Assistant Director. This service would include the FBI's Counterterrorism and Counterintelligence Divisions, along with the newly formed Weapons of Mass Destruction Directorate, and its

Directorate of Intelligence. The NSB would be subject to the coordination and budget authorities of the Director of National Intelligence (DNI).

Impact: In regards to the FBI's NSB, the DNI has more power over the FBI's intelligence activities – in theory. On December 17, 2004, President George Bush signed the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004.[17] The IRTPA empowered the DNI to lead the Intelligence Community, which it defines as including the FBI's intelligence elements mentioned above. The FBI's national security and intelligence missions are now unified under the authority of the Executive Assistant Director (EAD), Willie Hulon, who reports to the Deputy Director of the FBI. The EAD-NSB has full operational and management authority over all FBI Headquarters and field national security programs, including the authority to initiate, terminate, or reallocate any of the investigations or other activities within the NSB. The EAD-NSB has direct authority over the NSB budget, including the National Intelligence Program (NIP) resources. The EAD-NSB is also responsible for the continued development of a specialized national security workforce and is the lead FBI official responsible for coordination and liaison with the Director of National Intelligence (DNI) and the Intelligence Community (IC). (The DNI is the head of the U.S. Intelligence Community and the principal advisor to the President, National Security Council, and Homeland Security Council on intelligence matters

2. Trilogy Information Technology Modernization Program attempted to further the FBI's ability to integrate its information.

Impact: The Trilogy Information Technology Modernization Program did not further the FBI's ability to integrate its information thus continuing to limit the FBI's ability to partner with other U.S. law enforcement and intelligence entities and fully share homeland security information. Funding to optimize the FBI's ability to contribute fully to U.S. intelligence efforts was not actualized prior to 9/11 and subsequent attempts at technological progress within the FBI was stymied

[17] Full background on the IRTPA can be found at the Library of Congress site: http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.02845 (Accessed January 28, 2007).…

by bureaucratic, cultural, or monetary constraints. A new system, SENTINEL, is in development which will leverage technology to improve the FBI's ability to use the information in its possession.

3. In the fall of 2005, the FBI embarked on a Domain Management Initiative (DMI) wherein five field offices were provided authority by FBIHQ to find innovative methods or systems to determine the offices' domain using new technology methods to include "thinking outside the box." This innovative thinking led to the initial development of a ten to thirteen metadata code called Requirements and Information Metadata System (previously called "RICS" by one field office). The use of the RIMS code is a method to identify, catalogue, and retrieve intelligence information within the FBI.

Impact: Use of the RIMS metadata decreased the time FBI personnel needed to retrieve specific intelligence on documents which incorporated the code into the documents contents.[18] The use of the RIMS metadata would improve information assurance by eliminating misspelled words and poor indexing. RIMS would reduce the probability that a user of ACS would not retrieve vital information in a timely manner for analysis and making that link to a possible terrorist threat. This innovative system is cost effective, having minimal impact on the FBI's current information technology structure. There are minimal new equipment costs to the FBI, and the system uses existing alpha and numeric codes familiar within the USIC and the U.S. government. Additionally, since there are no formal cataloguing, metadata, or retrieval methods approved within the FBI this cataloguing and retrieval system was an immediate improvement to current FBI

[18] See Thesis Chapter VII, "Requirements and Information Metadata System," Section E, "RIMS as a Corporate Product?" for the results of focus group discussions involving RIMS users. It was determined that RIMS allowed the users to find and retrieve data, determine relationships between such data and notify processed intelligent information to interested parties faster than typical word searches within ACS. A RIMS search on the existing FBI Enterprise Architecture system allowed users to locate shared data items based on content or the structured attributes of RIMS. RIMS facilitated the identification of associations between content, people, places, and organizations. This collaboration service enabled multiple individuals to interact with each other on areas of mutual interest. These services crossed organizational program (counterterrorism, counterintelligence, cyber, or criminal) boundaries with rich content allowing formerly unknown linkages or anomalies to surface for quick analysis.

methods. To date, five FBI field offices were involved and trained with this concept. Positive interest from FBIHQ NSB entities occurred.

In summary, the FBI continues to strive for a versatile system which will provide powerful information retrieval, capture, and cataloguing capabilities to its users. The problem is this system is still in development within the FBI. The threat of terrorist acts continues and every day large amounts of information and intelligence is collected within the FBI through various investigative methods from the FBI's diverse program responsibilities. No central search platform exists for FBI analysts or investigators to use the information gathered or to data mine existing information in furtherance of the FBI's Priorities. An enterprise-wide standardized approach to classifying investigative information into a structured relational database environment is needed.

D. RESEARCH QUESTION

How can RIMS metadata be developed and implemented in the FBI in order to have a central search platform for use by FBI analysts or investigators to gather or data mine existing information in furtherance of the FBI's Priorities?

E. SIGNIFICANCE OF RESEARCH AND RESEARCH OBJECTIVE

The use of the RIMS code is a method to capture, catalogue, and retrieve intelligence information within the FBI. Currently, there are no formal cataloguing, metadata, or retrieval methods approved within the FBI. Agents and analysts rely on searching paper files or using unstructured text searches within the current Automated Case System (ACS). The use of the RIMS metadata to capture, catalogue, and retrieve intelligence information within the FBI would improve information assurance and accuracy by eliminating misspelled words and poor indexing of information. RIMS would reduce the probability that a user of ACS would not retrieve vital information in a timely manner for analysis and make that link to a possible terrorist threat.

RIMS would provide results from a central search platform and enable the ACS user to data mine within a genre of information. This type of intelligence tagging system will better capture, catalogue, and retrieve information at a high probability of detection and prevention.

Furthermore, within the USIC the RIMS code can be adapted to ensure commonality and uniformity in retrieval, cataloguing, and capturing of intelligence information. The use of the RIMS code can be manipulated into a non-classified code for use by state and local law enforcement and intelligence entities for integration into the USIC's knowledge base. The RIMS code can be adaptable and flexible throughout the intelligence community and with local/state entities working within the homeland security arena.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW — INFORMATION SHARING

Successful surprise attacks in modern warfare are not always a surprise. The recipients already possessed information suggesting that the attack was oncoming. Among such "intelligence failures" by recipients are the 1940 German invasions of Norway and France and the Soviet Union in 1941, the 1941 Japanese navy's attack on the American fleet at Pearl Harbor, the 1944 German attack on Allied forces in Ardenne, 1967 Egyptian preemptive attack on Israel, the 1968 Tet Offensive by the North Vietnamese and Viet Cong, and the 1973 Egyptian attack in the Sinai against Israeli forces. In each example, post attack analysis revealed that essential information had already been collected by the recipient's intelligence agencies but the information was ignored, lost, interpreted in a limited fashion, or completely negated. If assessed or disseminated properly, the recipient should have been able to disrupt or even prevent attacks. So prevalent were these failures that some analysts concluded that the failures are simply to be expected; as Richard K. Betts put it, "Intelligence failures are not only inevitable, they are natural."[19]

Other analysts argue that intelligence failures are not so inevitable and not always successful. For example, Ariel Levite cites the surprise attack in 1942 on Midway Island which intended to lure the U.S. fleet into a decisive open-seas battle and which Japan expected to win. The Japanese attacks was decisively defeated by the U.S. Navy's own surprise counterattack, made possible by deciphering of some of the Japanese navy's communication codes.[20]

Concerning terror attacks on the U.S., the debate continues today. In 1993, terrorists launched an attack on one of the World Trade Center towers in New York City; the attack was only partially successful but did not bring the building down as intended. Other terror events such as the attempt to blow up the Lincoln and Holland tunnels, the George Washington Bridge, the United Nations, and the FBI's New York Field Office in

[19] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," 31, *World Politics* (1978): 61-80.

[20] Ariel Levite, *Intelligence and Strategic Surprises* (New York: Columbia University Press, 1987).

Manhattan were prevented by American intelligence and law enforcement. At the Millennium, terror attacks were stymied. Nonetheless, on September 11, 2001, surprise terror attacks were launched in the U.S., which killed many, severely damaged the Pentagon and destroyed the World Trade Center towers. In sum, there have been surprise terror attacks in the U.S. and information has been discovered that revealed the USIC had in their possession the information but were not properly assessed and dissemination.

A huge amount of literature exists on intelligence organizations and their role in national security decision-making processes. It has generated a huge number of hypotheses about the cause of intelligence failures. Levite lists general explanations such as individual failures in correctly assessing intelligence information, intelligence failures stemming from the interaction of humans in small groups, intelligence failures due to bureaucratic politics, and intelligence failures involving limitations on learning and information processing by individuals and organizations.

There are three broad schools of thought in regards to the ongoing debate over 9/11 and intelligence failures. The most prominent school or viewpoint notes the inherent institutional structure of the intelligence community since Pearl Harbor. At that time, the failure was due to the lack of a unified intelligence command and trained analysts and the lack of a unified military command structure which disseminates to policymakers all collected information and all analytical production. The first post-war institutional reforms included a unified command within the Central Intelligence Agency, the Department of Defense, the Joint Chiefs of Staff, and the National Security Council to aid the president utilize the information and advise on national security issues. As Sherman Kent, a Yale historian and former officer with the Office of Special Services during World War II and author of one of the earliest treatises on intelligence, Strategic Intelligence for American World Policy, observed “the intelligence of grand strategy and national security is not produced spontaneously as a result of the normal procession of

government; it is produced through complicated machinery and intense purposeful effort."[21] What allows this debate to continue is the simple fact that most key structural issues remain unsolved.

A second general school of thought stresses the tradeoff any particular structural choice necessarily involves. For example, in Betts article referenced above, he argues that organizational solutions to intelligence failure are hampered by three basic problems, "the first dealing with procedural reforms addressing specific pathologies accenting other pathologies."[22] In order to fulfill present circumstances, policymakers structure their government to work against particular immediate defects. This is a criticism of Betts. Flexibility in adapting habits, which one day are relevant while the next day are not, requires different types of performance.

A third general school of thought downplays the impact of structure and highlights the importance of motivation and quality of analysts. Policymakers are receptive to information and advice from the intelligence community. For example, Betts states, "Intelligence failure is political and psychological more often than organizational…Intelligence can be improved marginally, but not radically, by altering the analytic system…The use of intelligence depends less on the bureaucracy than on the intellects and inclinations of the authorities about it."[23]

The fact that most descriptions of the nature of the process by which information is gathered and used virtually ignores the problem of storage of the information is symptomatic. Gregory F. Treveron refers to the "real" intelligence cycle in which (1) "Intelligence infers needs," (2) "Tasking and collection" occur, (3) "Raw intelligence" is collected, (4) "Processing and analysis" occur, (5) "Policy receives and reacts" and the cycle starts all over again.[24] Bruce D. Berkowitz and Allan E. Goodman also refer to

---

[21] Sherman Kent, *Strategic Intelligence for American World Policy (*Princeton, NJ: Princeton University Press, 1951).

[22] Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable" 31: 61-80.

[23] Gregory F. Treverton, Reshaping National Intelligence for an Age of Information (New York: Cambridge University Press, 2001) 15.

[24].Bruce D. Berkowitz and Allan E. Goodman, Strategic Intelligence for American National Security (New Haven: Yale University Press, 1989).

"the intelligence cycle" which includes "Step I: Determining the Information Intelligence Consumers Require," "Step II: Collection," "Step III: Analysis and Coordination of Assessments Results," and "Step IV: Dissemination of the Product." Mark M. Lowenthal states a cycle consisting of "Requirements," "Collection," "Processing and Exploitation," "Analysis and Production," "Dissemination," and "Consumption," and even cites a 1993 publication by the CIA, titled A Consumer's Handbook to Intelligence (September 1993), which depicts a cycle consisting of "Planning and Direction," "Collection," "Processing and Exploitation," "Analysis and Production," and "Dissemination."[25] As should be apparent, there is virtually no mention of precisely what happens to the intelligence information after it has been collected but before it is assessed and analyzed.

In the congressional hearings on 9/11, Deputy Secretary of Defense Paul Wolfowitz remarked on September 19, 2002, "We also need to address a relatively new problem, what I'll call "information discovery."[26] Many agencies collect intelligence and a lot of agencies analyze intelligence, but no one is responsible for the "bridge" between collection and analysis. Who in the intelligence community is responsible for tagging, cataloguing, indexing, storing, retrieving, and correlating data or for facilitating collaboration involving many different agencies? Given the volume of information we sift through to separate signal from noise, this function is now critical. We cannot neglect it."

In the congressional hearings on 9/11, Deputy Secretary of Defense Paul Wolfowitz remarked on September 19, 2002, "We also need to address a relatively new problem, what I'll call "information discovery."[27] Many agencies collect intelligence and a lot of agencies analyze intelligence, but no one is responsible for the "bridge" between collection and analysis. Who in the intelligence community is responsible for tagging, cataloguing, indexing, storing, retrieving, and correlating data or for facilitating

---

[25] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, (Washington, DC: CQ Press, 2003).

[26] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (New York: W.W. Norton & Co, n.d.).

[27] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton & Co, n.d.).

collaboration involving many different agencies? Given the volume of information we sift through to separate signal from noise, this function is now critical. We cannot neglect it."

There is not established linkage between the structures of intelligence organizations and the structure of the resulting intelligence. Most descriptions of the process by which information is gathered and used virtually ignore the problem of storage and retrieval of information. For example, Gregory F. Treverton, refers to "real intelligence cycle in which (1) Intelligence infers a need, (2) Tasking and Collection occur, (3) Raw intelligence is collected, (4) Processing and analysis occurs, and (5) Policy is obtained and reaction is given.[28] The cycle starts again. There is no mention of what happens to the intelligence information after it is collected but before assessed and analyzed.

Observation from Senator Richard Shelby (Republican-Alabama), Vice Chairman of the Senate Select Committee on Intelligence, in an extensive set of "Additional Views" submitted along with the Joint Inquiry's "Findings and Conclusions" and "Recommendations"[29] on December 10, 2002 which were critical of many different elements of the intelligence community and were echoed by the Joint Inquiry staff reports. Senator Shelby focused on the FBI and the problem of storage and cataloguing of information which inhibited information retrieval by the FBI and other agencies. Senator Shelby concluded the FBI's approach to intelligence analysis was unsuited to any long-term strategic analytical work and is inappropriate to counterterrorism analysis. Exacerbating these problems were what the Senator called the FBI's "Technological Dysfunctions" since the FBI never took IT seriously thus finding itself with an obsolete IT infrastructure totally inadequate to the FBI's current operational needs much less in support to all-source intelligence fusion and analysis. So the problem of organizational design is to confront and manage what Steve Chan noted about the nature of warming

[28] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, 16.

[29] These materials are all available on http://intelligence.senate.gov/hr107.htm (Accessed June 12, 2006).

signs about surprise attack, "In the real world of strategic analysis, warning signs are usually scattered across individual and bureaucratic units."[30]

To avoid future scattering of information and the unrecognized warning signs of a surprise attack, a seamless environment was needed. The RIMS mission requirement was to provide an environment that was seamless regardless of seams created by the national security classifications of information or the physical separation of existing networks (FBI offices). RIMS was a cross-domain (counterterrorism, counterintelligence, cyber and criminal programs) solution for the exchange of information between the different security levels and programs within the FBI.

[30] Steve Chan, "The Intelligence of Stupidity: Understanding Failures in Strategic Warning." *American Political Science Review* (1979), 73: 171-180.

III. TENTATIVE SOLUTIONS — RIMS

On January 1, 2006, the RIMS code was initiated on all communications containing intelligence information within the Pittsburgh Field Office of the FBI. On February 16, 2006, the RIMS system was briefed to four other FBI field offices: San Francisco, Miami, Charlotte, and Little Rock. Training by Pittsburgh personnel was provided the field offices. Additionally, FBI Headquarter personnel from the Directorate of Intelligence were also provided a briefing and training on the RIMS code. The four field offices agreed to test the RIMS codes on future communications. Members from FBI Headquarters, Directorate of Intelligence, received the RIMS code positively, agreeing to study it further at the FBI Headquarters level.

The following assumptions can be made from the use of the RIMS code:

* With the proper governance, the use of the RIMS code will capture, catalogue, and retrieve information with increased accuracy and effectiveness while decreasing the probability of uncertainty.

*The use of the RIMS code is cost effective and will have minimal impact on the FBI's current Information Technology structure and not radically affect the FBI's future Information Technology structure, SENTINEL.[31]

*The use of the RIMS code can be adapted for use by the entire USIC for commonality and uniformity in retrieval, cataloguing, and collecting of intelligence information.

*The use of the RIMS code can be manipulated into a non-classified code for utilization by state, local, and tribal law enforcement and intelligence entities.

This paper will verify if the RIMS code will be an effective and efficient method to capture, catalogue and retrieve intelligence information within the FBI.

[31] No new hardware or software is needed and there are minimal new equipment costs to the FBI.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. METHODOLOGY

The thesis is composed of eight chapters. The first chapter, the introduction, describes the motivation for the thesis. The second chapter is a review of the literature available on the topic of information sharing and collaboration. Chapter III defines the proposed solution to the thesis – the Requirements and Information Metadata System. The fourth chapter is the chapter overview while Chapter V goes into the history of the FBI, its current mission and homeland security function. The chapter also addresses the FBI's cultural resistance and current information sharing and collaboration topics. Chapter VI includes and extensive analysis and discussion of the FBI and Information Technology. The seventh chapter provides extensive information concerning the Requirements and Information Metadata System (RIMS). The eighth chapter presents a summary of the thesis findings along with future research topics.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE FEDERAL BUREAU OF INVESTIGATION

A. HISTORY

On July 26, 1908, Attorney General Charles J. Bonaparte ordered a small force of permanent investigators to report to the Department of Justice's Chief Examiner, Stanley Finch. Except for certain bank frauds, all Department of Justice (DOJ) investigations were reported to his new group of detectives. Initially, little seemed to come of Bonaparte's reorganization.[32]

This small special agent force evolved into the FBI, the primary federal law enforcement agency in the U.S.[33] Initially staffed to investigate antitrust matters, copyright violations, land fraud, and twenty one other matters, the FBI today investigates criminal and security threats within the U.S. along with the emerging international face of crime by aggressively building bridges between U.S. and foreign law enforcement. The FBI expanded its Legal Attache program; provided professional law enforcement education to foreign nationals through the International Law Enforcement Academy in Budapest and other international education efforts; and created working groups and other structured liaisons with foreign law enforcement. On September 4, 2001, former U.S. Attorney Robert S. Mueller III (2001 to present) was sworn in as Director with a mandate to address a number of challenges such as upgrading the FBI's information technology infrastructure, addressing records management issues, and enhancing FBI foreign counterintelligence analysis and security in the wake of the damage done by former Special Agent and convicted spy Robert S. Hanssen.[34]

---

[32] FBI Public Website. http://www.fbi.gov/libref/historic/history/test.htm (Accessed September 30, 2006).

[33] Ibid.

[34] Athan G. Theoharis, Tony G. Poveda, Susan Rosenfeld, and Richard Gid Powers, *The FBI: A Comprehensive Reference Guide* (New York: Oryx Press, 2000).

B. TODAY'S FBI: CHANGING TO MEET EVOLVING THREATS

On September 11, 2001, terrorist attacks were launched against New York and Washington, D.C. On October 26, 2001, the president signed into law the U.S. Patriot Act, which granted new provisions to address the threat of terrorism. On May 29, 2002, the attorney general issued revised investigative guidelines to assist the FBI's counterterrorism efforts. To support the FBI's change in mission and to meet newly articulated strategic priorities, Director Mueller called for a reengineering of FBI structure and operations that would closely focus the FBI on prevention of terrorist attacks, on countering foreign intelligence operations against the U.S., and on addressing cyber crime-based attacks and other high technology crimes. Additionally, the FBI remained dedicated to protecting civil rights, combating public corruption, organized crime, white-collar crime, and major acts of violent crime. The FBI continued to strengthen its support to federal, county, municipal, and international law enforcement partners. Also, it is dedicated to upgrading its technological infrastructure to successfully meet each of its priorities, as noted below.

Over the past five years, the FBI has transformed itself to meet evolving threats. The FBI enhanced its operational and intelligence capabilities, and adopted a strategic approach to human resources, IT, science and technology, facilities and budget. These changes, highlighted below, have aided the FBI emerge within the Homeland Security[35] field as a viable partner in the defense of America.

1. Prevention/Investigation of Terrorist Acts

- Lead law enforcement agency for all terrorism investigations; as same time, committed partner who works with host of federal, state, local agencies
- Preventing terrorist attacks is the FBI's number one priority. Strategies: Root out & shut down sleeper cells in U.S. using all available tools; Identify individual sympathetic with terrorists but not part of organized group; Disrupt terrorist logistical structures, including financial support; Help track down terrorist leaders/operatives worldwide; Provide security/support for major special events (Olympics etc.)

[35] FBI Public Website. http://www.fbi.gov/fbihistory.htm (Accessed September 30, 2006).

- When attacks do occur, the FBI quickly responds: Sends teams of agents, bomb technicians, etc. to the site to assist victims, manage crime scene, launch investigations; agents worldwide to run down leads; and activates command posts to coordinate FBI efforts
- The FBI leads numerous inter-agency Joint Terrorism Task Forces, which pool expertise and resources and are a key weapon in fighting terrorism in the U.S.

2. Intelligence/Information Sharing

- Gather, analyze, and share intelligence on terrorists, terrorist activities, and terrorist groups with government leaders, intelligence community, and national/international law enforcement entities.

3. Weapons of Mass Destruction

- Lead federal agency for investigating threats/use of WMD (anthrax)
- Conduct threat assessments, deploy Hazmat teams, collect evidence etc.
- WMD Coordinators in each field office serve as focal point for local response
- Strong partnerships at a federal, state, local levels including with the military, law enforcement, fire, emergency, public health, and medical communities
- Conduct field/table top exercises and provide training to a variety of officials

4. Threat Analysis and Warning

- Analyze threats against U.S. in partnership with intelligence community
- Work closely with DHS to determine national threat level and response
- Share threat information/alerts with government/law enforcement/ private sector

5. FBI Priorities[36]

In executing the following priorities, the FBI will produce and use intelligence to protect the nation from threats and to bring to justice those who violate the law.

- Protect the United States from terrorist attack.
- Protect the United States against foreign intelligence operations and espionage.
- Protect the United States against cyber-based attacks and high-technology crimes.
- Combat public corruption at all levels.
- Protect civil rights.
- Combat transnational and national criminal organizations and enterprises.

[36] FBI Public Website. http://www.fbi.gov/priorities/priorities.htm (Accessed September 30, 2006).

- Combat major white-collar crime.
- Combat significant violent crime.
- Support federal, state, county, municipal, and international partners.
- 10. Upgrade technology to successfully perform the FBI's mission.

In summary, the FBI is changing to meet evolving threats. Infrastructure changes within the FBI included the modernization of the FBI Information Technology Infrastructure (SENTINEL) with new networks. The FBI centralized databases with modern search tools and improved connectivity with law enforcement and intelligence community partners. The FBI institutionalized the strategic information technology planning processes and utilized performance-based contracting and centralized information technology contract management.

Furthermore, FBI process changes include moving beyond case-focused intelligence gathering and analysis to knowing the FBI's domain thus centralizing and enhancing the management of national programs. The FBI utilizes a full range of investigative tools against criminal and terrorist elements by enhancing human source reporting, modernizing records management, improving security practices, training and education and establishing clear lines of accountability to ensure day-to-day operations support the FBI's strategies.

C. THE FBI'S CULTURAL RESISTANCE TO INFORMATION SHARING

There is a continuing and heightened need for better and more effective and comprehensive information sharing.[37] The intelligence community needs to move from a culture of "need to know" to "need to share." The 9/11 Commission made observations regarding information sharing, and recommended procedures to provide incentives for sharing and creating a "trusted information network." Many Commission recommendations address the need to improve information and intelligence collection, sharing, and analysis within the intelligence community itself. It is imperative that the purpose of improving information analysis and sharing is to provide better information

[37] Comptroller General of the United States, David M. Walker, Statement before the Committee on Government Reform, House of Representatives, August 3, 2004 (See GAO-04-1033T).

throughout the federal government, and ultimately also to state and local governments, the private sector, and our citizens.

The FBI was one of several government entities that portrayed cultural resistance after September 11, 2001, to sharing information and collaborating.[38] Differing terminologies initially caused problems in communicating the appropriate information to outside agencies which included the severity or immediacy of the information. Other cultural resistance factors included: lack of trust when information is shared; fear that shared data will be misused; fear that shared data will be misinterpreted; fear that shared data will be used to beat collector to wider dissemination; low trust that they are receiving all available information; do not trust reliability of information shared; do not trust products, want raw data and ability to conduct own/alternative analysis; and fear of sharing data in violation of privacy laws.[39]

D. INFORMATION SHARING AND COLLABORATION

With the FBI's dual mission, it is increasingly important to have effective information sharing within the FBI and across organizations such as law enforcement and intelligence agencies with different objectives and perspectives This "means sharing the right information, at the right level of detail, using the right language, at the right time, in the right context, with the right people. A failure related to any one of these factors can lead to an information-sharing breakdown. Supporting the effective use of shared information is even more complex because access to information does not necessarily lead to effective knowledge sharing and collaboration. When users from different communities share information, they interpret that knowledge in new contexts, transforming and creating new knowledge, while at the same time contributing toward the development of the communities grounding that knowledge."[40]

---

[38] Partial Recall, "Effective Culture Change in the FBI," http://robfay.com/2005/06/15/effective-culture-change-in-the-fbi/ (Accessed December 15, 2006)

[39] CIO Executive Council, The Professional Organization for CIOs, "Why the G-Men Aren't I.T. Men," http://www.cio.com/archive/061505/gmen.html (Accessed January 3, 2007)

[40] Peter A. Kind and J. Katharine Burton, "Information Sharing and Collaboration Business Plan," *Institute for Defense Analysis*, June 2005.

In a document prepared by Peter Kind and Katharine Burton for the Institute for Defense Analyses, the authors note information sharing and collaboration is a daunting challenge within the U.S. Intelligence Community. There is a full range of stakeholders throughout all government agencies and levels, private sector and cooperating allies and at appropriate levels of information security classification approaches. Nonetheless, it must be done to accomplish effective homeland security. Kind and Burton state:

> Enabling, encouraging, and facilitating information sharing and collaboration require different supportive mechanisms culturally and technologically. Enabling information sharing is the first step, involving cross-organizational access to information according to sharing policies and procedures. But access to information does not necessarily lead to effective knowledge sharing and collaboration. When people share knowledge, they are not just sharing information; they are also sharing cultural and social references. Likewise, when people seek knowledge, they are not just seeking information; they are seeking information grounded in, and carrying different meanings to different social communities. Information is viewed, perceived, and used differently by each community.
>
> When users from different communities share information, they interpret that knowledge in new contexts, transforming and creating new knowledge, while at the same time contributing toward the identity of the communities grounding that knowledge. The role of the information-sharing environment, then, is to encourage, support, mediate, and guide this cyclic process of community development through knowledge seeking, sharing, joint understanding, and social knowledge building. In this way, data is contextualized and transformed into information, which is in turn shared, interpreted, and socially transformed into knowledge. As this knowledge is developed and integrated and used by components that operate collaboratively, it is understood and given different meanings and applications.[41]

For the FBI to be an effective member of the U.S. Intelligence Community and to partner with various law enforcement entities, the FBI must effectively share information across the FBI and with organizations such as law enforcement and intelligence agencies with different objectives and perspectives. The use of RIMS will allow the different

[41] Kind and Burton, "Information Sharing and Collaboration Business Plan," 7-8.

communities, inside the FBI and outside, to share information, interpret the information in a similar way, and create cooperative knowledge banks based upon the common shared information provided by RIMS.

E. FLEXIBILITY

The culture of the FBI is now and always has been a culture of hard work, integrity, and dedication to protecting the U.S., no matter the challenges facing the FBI. The FBI was created 99 years ago to fight the spread of traditional crime across county and state lines. Today, the FBI faces a world in which crimes are as diverse as terrorism, corporate fraud, identity theft, human trafficking, illegal weapons trade, and money laundering across international boundaries. The FBI now deals with organized crime groups that launder money for drug groups that sell weapons to terrorists, who commit white-collar crime to fund their operations. With the terror attacks on September 11, 2001, it became clear that the FBI must be more flexible, agile, and mobile in the face of these new threats. As a result, the FBI refocused its mission and revised its priorities; realigned its workforce to address these priorities; shifted its management and operational environment to strengthen flexibility, agility, and accountability; restructured FBI Headquarters; and initiated many projects aimed at reengineering the FBI's internal business practices and processes.

The FBI's new refocused mission and revised priorities allowed creative processes to be explored by field divisions to address the FBI's new threats. The RIMS system was a new system that promoted an immediate interoperable terrorism information-sharing environment. This system was created by the investigators who worked the threats and understood the importance of a system that would not inhibit their current workloads, but add value to their investigations. It was important that this system be available to FBI personnel without added cost, new technology, or security roadblocks. It effectively supported the detection, prevention, disruption, preemption, and mitigation of the effects of terrorism against the territory, people, and interests of the U.S.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. INFORMATION TECHNOLOGY AND THE FBI

A. INFORMATION TECHNOLOGY ADVANCEMENTS

FBI Director Robert S. Mueller III, in a statement before the Senate Appropriations Committee, advised that in September 2001, the FBI's technology systems were several generations behind industry standards; existing legacy systems were nearly 30 years old. Information Technology (IT) equipment was inadequate.

> For example, our personnel were working on hand-me-down computers from other federal agencies. We had little to no Internet connections in our field offices, and our networks could not do something as simple as transmit a digital photo.[42]

> Following the September 11 terrorist attacks, we were required to make an in-depth assessment of our information technology systems. This assessment determined that we needed to address some key areas including the lack of databases that contained current information, limited analytical tools, continual dependency on Automated Case Support (ACS), and outdated equipment.[43]

The U.S. Government Accountability Office (GAO) completed a study concerning the FBI's process of modernizing its information technology (IT) systems. Replacing much of its 1980's-based technology with modern system applications and a robust technical infrastructure, this modernization is intended to enable the FBI to take an integrated approach—coordinated agency-wide—to performing its critical missions, such as federal crime investigation and terrorism prevention. The GAO conducted a series of reviews of the FBI's modernization management. The objective of this review was to determine whether the FBI has an enterprise architecture to guide and constrain modernization investments.[44]

---

[42] FBI Director Robert S. Mueller III, Statement before the Senate Appropriations Committee, Subcommittee on the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, March 23, 2004.

[43] Ibid.

[44] U.S. Government Accountability Office, *FBI Reorganization: Information Technology: FBI Needs An Enterprise Architecture To Guide Its Modernization Activities, GAO-03-959.* Washington, D.C: September 2003.

The report noted that in order for the FBI to become an intelligence-driven organization it must have the IT and information-based capabilities in place to support an enterprise-wide intelligence focus. IT must be available to support established and validated intelligence requirements including the collection, fusion, storage, retrieval, analysis, exploitation, and dissemination of both raw and finished intelligence products. Full support for these capabilities must occur for all missions and lines of business; these include analysis, investigation, audit, security, and internal management operations and initiatives.

The FBI must develop an expanded, technologically-oriented infrastructure and increase its abilities to plan, acquire, manage, and deploy information-based capabilities in order to maximize the FBI's operational effectiveness, yet conserve scarce resources. Innovation should be encouraged with outsourcing of IT services, and capabilities should be used to leverage industry capabilities and optimize the available resources to develop and deploy needed capabilities and infrastructure.[45]

The FBI's Strategic Plan[46] notes the FBI's greatest challenges will be to further improve its intelligence capabilities and strengthen its information technology infrastructure. To achieve its vision of becoming a proactive, threat-based organization, the FBI must upgrade its technology infrastructure and capabilities to meet the pace of its adversaries. It must also provide enterprise-wide threat-prioritized access to data and information from a resilient infrastructure which is resistant to attacks, disasters, and other circumstances which could negatively impact operations and mission success. The FBI must implement enterprise architecture that requires shared data storage and multiple access mechanisms. It must support access to information at all security levels and classifications, by properly authorized individuals and organizations at all times. This would include the need for data storage, user identity management, and interoperable

[45] U.S. Government Accountability Office, GAO Highlights, "Information Technology — FBI is Building Management Capabilities Essential to Successful System Deployments, but Challenges Remain," http://www.gao.gov/highlights/d051014thigh.pdf.

[46] FBI Public Website. http://www.fbi.gov/publications/strategicplan/stategicplantext.htm#it (Accessed January 15, 2007).

information-sharing systems across a global information infrastructure of networks and systems. Some of these networks and systems are not owned or operated by the FBI.

The FBI Strategic Plan further notes the FBI's IT structure must allow the sharing of information quickly, easily, and appropriately within the FBI and with its partners. Interoperability with the information systems and networks of the FBI's partners must facilitate the sharing of information by providing search, request, and retrieval capabilities that are accessible to its partners for both intelligence and operational purposes. RIMS provides quick access to specific information through a simple search of available FBI databases. Retrieval capabilities are simple and quick, mimicking a Google word search.

B. SENTINEL AND INFORMATION MANAGEMENT

The Trilogy Information Technology Modernization Program (Trilogy) did not further the FBI's ability to integrate its information thus continuing to limit the FBI's ability to partner with other U.S. intelligence entities and fully share homeland security information. The well publicized FBI Trilogy Program did not provide an effective return on the FBI's IT investment (measured in operational terms—more and better results, increased responsiveness and agility, and improved efficiency of operations). Trilogy limited the FBI's ability to partner with other U.S. intelligence entities and fully share homeland security information. A new system, SENTINEL, under development by the FBI plans to transform the way the FBI does business, allowing the FBI to move from a paper-based reporting system to an electronic system of records, as well as eliminating the redundancy in maintaining multiple systems and bottlenecks. It will leverage technology to improve the FBI's ability to use the information in its possession. SENTINEL will provide a versatile capability to locate different types of information contained within SENTINEL. It will support the preparation and execution of a multitude of different search queries. This capability will be both flexible and powerful to accommodate the substantial volume and wide variety of information available for retrieval in SENTINEL.

In a March 16, 2006, press release by the FBI Press Office, FBI Director Robert S. Mueller III said, "SENTINEL will strengthen the FBI's capabilities by replacing its primarily paper-based reporting system with an electronic system designed for information sharing. SENTINEL will support our current priorities, including our number one priority: preventing terrorist attacks. At the same time, the system will be flexible and adaptable, to address future technological advances and changes in our mission and threat environment."

SENTINEL will deliver an electronic information management system, automate workflow processes for the first time, and provide a user-friendly web-based interface to access and search across multiple databases. SENTINEL will help the FBI manage information beyond the case-focus of the existing ACS, and will provide enhanced information sharing, search, and analysis capabilities. SENTINEL will also facilitate information sharing with members of the law enforcement and intelligence communities.

The SENTINEL program will be developed and deployed over time—in four phases—with each phase introducing new capabilities. Existing information will be migrated to the new system throughout the phases so that selected systems can be retired by the end of the fourth phase.

SENTINEL provides information-based capabilities that support identification, collection, evaluation, analysis, and dissemination of investigative information. Using SENTINEL, the FBI will maximize the sharing of information both internally and externally with its intelligence and law enforcement communities while ensuring that sensitive and classified information is appropriately protected against unauthorized disclosure.

SENTINEL is an enterprise system which, when fully implemented, will benefit all FBI operational divisions. Information Management applies to all of the systems required by the FBI's operational and support divisions. SENTINEL will allow the FBI's intelligence organization to be "matrixed" across the entire FBI to support its IT structure. System components must be designed to support intelligence functions.

Additionally, the consolidation of existing legacy systems and databases will also be a high priority in the design of new systems and databases which will reduce legacy costs and ensure a wider access of critical data.

C. INFORMATION SHARING

Executive Order 13356, "Strengthening the Sharing of Terrorism Information to Protect Americans," a federal-level information-sharing mandate, has changed the ways in which information is obtained, processed, and used within the law enforcement and intelligence communities. Increased requirements for implementation and integration of information assurance and access controls to protect FBI information and repositories from unauthorized access or exploitation has provided increased access to information-sharing partners. The successful implementation of this plan is a key step toward achieving the FBI's vision for secure, interoperable, any time, any location access to information products and services both internal (FBI) and externally with the FBI's partners across the federal government, including the Intelligence Community, and with state, local, and tribal governments.

Information-sharing mandates levied by the U.S. Congress, the president, the director of national intelligence (DNI) and the attorney general created new challenges for the FBI, as a member of the U.S. intelligence community, to use IT infrastructure to share information both internally and externally in support of investigative, intelligence, and law enforcement missions and national intelligence priorities established by the DNI. External information sharing includes state, local, tribal, and international organizations that are authorized to receive FBI information. The FBI's information infrastructure must provide pathways and network interconnections for transmitting and receiving information to and from these external partners. This infrastructure must also provide the technologies and procedures necessary to provide requisite levels of information assurance. Of course, protected or sensitive information must be made available to authorized partners in accordance with established procedures and agreements. The RIMS system provides the requisite level of information assurance by standardizing the

meta data, which is necessary for an accurate and faster search. RIMS is already available to authorized partners and uses the existing software and hardware, which eliminates any need to establish new procedures or agreements.

VII. REQUIREMENTS AND INFORMATION METADATA SYSTEM

A. GENESIS OF THE REQUIREMENTS AND INFORMATION METADATA SYSTEM (RIMS)

In the fall of 2005, the FBI embarked on a Domain Management Initiative (DMI) wherein five FBI field offices were provided authority by FBI Headquarters to find innovative methods or systems to understand the offices' domain using new technology methods to include "thinking outside the box." To understand an office's domain, massive amounts of information had to be gained from numerous sources and from field work of investigators and analysts. This information had to be formally catalogued, analyzed, and again retrieved in full in order to complete threat assessments involving an office's domain or territory. With time constraints to complete the domain projects along with no additional capital expenditures by the FBI on the projects, a new method to capture, catalogue, and accurately and fully retrieve intelligence information had to be developed. Visionary leadership and innovative thinking in one field office led to the initial development of a ten to thirteen metadata code called the Requirements and Information Metadata System (previously called "RICS" by one field office). The use of the RIMS code was a method to identify, catalogue, and retrieve intelligence information within the FBI.

The RIMS code design had to be simple and easily adapted for quick use and understanding by FBI personnel. The RIMS code is a method to capture, catalogue, and retrieve intelligence information within the FBI. It would provide results from a central search platform and enable the ACS user to data mine within a genre of information. Currently, there are no formal cataloguing, metadata, or retrieval methods approved within the FBI. Agents and analysts rely on searching paper files or using unstructured text searches within the current ACS system. The use of the RIMS metadata to capture, catalogue, and retrieve intelligence information within the FBI would improve information assurance by eliminating misspelled words and poor indexing. RIMS would

reduce the probability that a user of ACS would not retrieve vital information in a timely manner for analysis and making that link to a possible terrorist threat.

The RIMS code aids in cataloguing the huge amounts of information the FBI collects on a daily basis and in the rapid retrieval of information. To simply explain, the RIMS metadata system is similar to a Vehicle Identification Number (VIN). It should be no less than 10 digits and as much as 13 digits and is alpha-numeric.

With an eye to the future and a possible expanded national use, the RIMS code used a variety of documents from numerous agencies to create specific codes, designed to start with a broad category or topic area and end with a very specific target group, activity, or area. Each alpha-numeric space holder holds critical information which identifies specific information to be used in research and analysis. The codes, guides, and charts used to create RIMS reflected the sources of information needed throughout the intelligence and law enforcement communities to complete the national security and defense mission while sharing information and intelligence information throughout the FBI and with its participating national security partners.

B. DESCRIPTION OF THE RIMS SYSTEM

The RIMS code aids in cataloguing the huge amounts of information the FBI collects on a daily basis and in the rapid retrieval of information. The RIMS metadata system is similar to a Vehicle Identification Number (VIN). It should be no less than 10 digits and as much as 13 digits and is alpha-numeric. When a document is created, the author places the RIMS code in the Administrative section of the document. Wrong codes or typographical errors can happen but when found, the errors can be quickly corrected by an edit to the document. Even after the document is in ACS, if an error is found in the RIMS code, the document can be removed from the system and re-entered with the adjusted RIMS code.

The first five characters alone should immediately determine the type (counterintelligence, counterterrorism, or criminal) of intelligence or investigation you are looking at. If “RQPG1” is written, automatically the document contents pertain to a Pittsburgh counterintelligence matter. If “RQPG2” is written, it is automatically known

that this document is counterterrorism-related. If you want to know if the document pertains to international terrorism (INTERR) or domestic terrorism (DOMTERR), simply look at the Alpha Terrorism character to determine if it is INTERR or DOMTERR. "RQPG3" designates the document to either a non-National Security Program matter or a DOMTERR "Lone-wolf" individual. The beauty of the RIMS code is that, if coded correctly, the reader can look at the code and determine what type of information is covered in the document before even reading it. This would allow for streamlining of analysis and quick retrieval of specific documents pertaining to specific intelligence.

The following are the digit definitions of the code:

RQ: Short form for "Requirements" (There are no words that begin with "RQ" which would automatically narrow the search perimeters for documents housing "RQ" within the text of the document.)

Two-digit alpha code for each FBI field office (i.e., PG for Pittsburgh. It should be noted, this section could be changed to state codes such as "CA" for California, which would be beneficial to a national type tagging code.)

TYPE: One-digit numeric code. The "Type" denoting a State, Group, Individual or Other (i.e., Business)

1 Counterintelligence Interest Only

2 Counterterrorism (International and Domestic Groups)

3 Criminal (Non-National Security Program) and "Lone-wolf" types in Domestic Terrorism cases

TOPIC: One-digit alpha code for the various intelligence collection initiatives within the U.S. government. (The documents used to create the code used in the FBI system are classified.)

ALPHA TERRORISM One-digit alpha code for the FBI's Classification Code for International Terrorism matters and Specific Domestic Terrorism entities. If not a terrorism matter, a zero ("0") is placed here as a space holder.

ACTIVITY	One-digit numeric code for groupings of activities based upon a joint FBI-DHS Initiative, "TerroristThreats to the US Homeland, Reporting Guide." (Some examples are: Personnel/Organization Information, Capabilities, Operations, or Criminal Activities)
MAIN INDICATOR	One-digit alpha code for specific types of sub-activities under each main identified activity. (Some examples are Leadership activities, Logistics/Infrastructure activities, Targeting, or Illegal Acts within the U.S.) This code is based upon a joint FBI-DHS Initiative, "Terrorist Threats to the US Homeland, Reporting Guide."
SPECIFIC INDICATOR	One-digit alpha code for detailed activities under the main indicator sub-activities to further identify the activity. (If no specific indicator is given, a zero "0" is placed here to keep the space. Some examples are Cyber, Finances, and Mobility) This code is based upon a joint FBI-DHS Initiative, "Terrorist Threats to the US Homeland, Reporting Guide."
SPECIFIC CODES	This is an optional expansion of the RIMS ten-digit identified by a three-digit alpha or numeric code. Specific countries/states, terrorist groups, Criminal Crime Problem Indicator Codes, and Specific Cyber crimes are used and based upon a variety of government documents.

Since RIMS is a field office initiative, no approved reference documents are available to define RIMS. Intra-office documents were created by the field office trainers for use in RIMS training to field personnel, other field offices, and FBI Headquarters. The training document is classified due to the RIMS code identification markers. During all training of RIMS, the following information was provided for guidance and explanation of the FBI's RIMS code:

The beginning two-alpha designators, "RQ" stand for Requirements. In looking at large English language dictionaries, no words start with the two letters "RQ." In initial text word searches on ACS or other FBI databases, only communications with "RQ" surfaced or on occasion some misspelled words had the "RQ" letters within the

communication. The standard use of "RQ" begins all RIMS tagging code and quickly identifies all documents with the two alpha designations.

The next two alpha designations are FBI two digit division codes. There are 56 field offices within the FBI, each with a two digit division code. Within U.S. intelligence and law enforcement national security communities, these codes are known, accepted, and identifies when information or intelligence arrives from the FBI. Each FBI document must have identifying case file numbers which use the two digit division code. The standard use of the two digit FBI division code as the third and fourth space holder within the RIMS tagging code identifies all documents originating from the division. If additional information is needed or similar occurrences are witnessed in other divisions, coordination can quickly occur between the divisions which "connects the dots" in analysis through the RIMS code. For example, up to the events involving the terrorist acts on September 11, if the RIMS code was in use, all divisions who noted unusual events involving Middle Easterners and aircraft flight schools throughout the country would have been able to place the specific RIMS code on their communications. Strategic analysts both at the field or headquarters level may have caught the similarities and possibly alerted officials of unusual activity involving a finite group of individuals. Armed with that information, agents could have been dispatched to interview the school officials or even the flight school candidates, thus possibly revealing the September 11th plot. Although we will never know if the use of the RIMS code could have alerted U.S. officials to the September 11 plot, the possibility exists that this small measure of information sharing and collaboration and the subsequent directed actions by agents and/or analysts could have saved countless lives on September 11, 2001.

The fifth place marker is a numeric number, one through three which aids in the identification of programs. Type "1" (State) should only be used in counterintelligence cases. Type "2" (Group) should only be used in international terrorism cases, as well as domestic terrorism cases involving a group. Type "3" should only be used in "lone-wolf" type domestic terrorism cases and non-National Security program cases (i.e., criminal and cyber).

The sixth place marker is an alpha marker and originated with classified U.S. government documents which pertain to intelligence collection initiatives. Besides the use of the classified documents, additional alpha designators have been added to this section to identify issue specific items such as international finance, weapons of mass destruction, or other criminal programs such as cyber, violent crimes, white collar crimes or drugs.

The seventh designator signifies the FBI's terrorism investigative alpha classification. It is classified and includes states and groups within the international and domestic terrorism realm. A similar document, on the Department of State website, lists all foreign terrorist organizations.

Specific information identification and tagging comes with the eighth, ninth, and tenth place designators. The three markers tell the reader exactly what information or intelligence has been collected. Of course, perception and classification of information is a subjective matter, but the clear groupings of information can lead users in the right direction in amassing information from a variety of areas.

The "Activity," "Main Indicator," and the "Specific Indicator" designators originated from a review of an UNCLASSIFIED/FOR OFFICIAL USE ONLY document entitled, "Terrorist Threats to the U.S. Homeland Reporting Guide" (TTRG). This document was jointly produced by the FBI and the Department of Homeland Security. The purpose of this document was to "leverage the vast information collection and reporting resources of our state, local and tribal law enforcement partners, as well as other first responder partners, in recognizing activities and conditions that my be indicative of terrorist activity."[47] The report notes "state and local organizations are on the front line in the war against terror and therefore have a critical role as primary sources of information. Timely and relevant information from the "front lines" is critical to the identification of terrorists and their supporters, development of insights into their plans and intentions, and subsequent disruption of their operations."[48] This guide can be found

[47] Terrorist Threat to the US Homeland Reporting Guide, October 21, 2004. 3.

[48] Ibid., 3.

on LEO at http://www.leo.gov and by clicking on the TTRG tab on the following Homeland Security Information Network (HSIN)/ Joint Regional Exchange System (JRIES) portals:

— Law Enforcement (LE): https://jries.dhs.gov
— Combating Terrorism (CT): https://ct.jties.dhs.gov
— Emergency Operations Center (EOC): https://eoc.jries.dhs.gov

The "Activity" numeric designator is a grouping of four main activities as noted in the TTRG as they relate to terrorism activities. If the activity noted is not terrorism-related, then a zero, "0" is placed in the eighth spot to hold the place.

The "Main Indicator," the ninth spot, is an alpha designation and identifies specific types of sub activities under each main identified activity (eighth spot). The information here would reveal leadership or membership information or logistic or financing information to name a few indicators.

The final mandatory RIMS identifier, the tenth spot, is also an alpha designator and provides specific information pertaining to the ninth indicator. At this time, this alpha code specifically deals with logistics and infrastructure indicators or specific types of attacks (i.e., Cyber, CBRNE, or non-CBRNE). If no specific indicator is noted for this designation, a zero, "0" is placed in the tenth spot to hold the place and complete the RIMS code with ten digits.

The optional three designators are three-digit numeric codes which expand the RIMS code to identify specific countries or states, terror groups, the FBI Criminal Crime Problem Indicator (CPI) Codes, and Cyber crimes. These specific codes were created from various documents to include the United Nations Country Code List, the U.S. Department of State List of Identified Foreign Terrorist Organizations, the FBI's Domestic Terrorism Operational Unit's List of major Domestic Terrorism investigations, the FBI's FY 2005 CPI Code list, and a list of FBI Cyber violations.

It should be noted; more than one RIMS code can be used on communications to designate the crossover of intelligence and information into more than one program or areas.

Below are examples of the RIMS code in use:

EXAMPLE: Source reporting revealed Main Street Gang leader, John Smith, 123 Main Street, Pittsburgh, Pennsylvania was involved in the murder of a rival gang member, John Brown of the 10th Street Gang, over drug trafficking into the Pittsburgh area from Canada.

RIMS Code: RQPG3X01A0-CAN - Requirement (RQ) from Pittsburgh (PG) concerning an individual (3) involved in violent crimes (X). Specific information pertains to the individual's participation in an organization (1) and denotes he is a leader (A) in the organization. Information possibly involves Canadian interests (CAN). (Note: Two place holders of zero where used here in the seventh and tenth positions)

AND

RIMS Code: RQPG3O01A0-CAN - Requirement (RQ) from Pittsburgh (PG) concerning an individual (3) involved in drugs (O). Specific information pertains to the individual's participation in an organization (1) and denotes he is a leader (A) in the organization. Information possibly involves Canadian interests (CAN).

AND

RIMS Code: RQPG3O01A0-533 - Requirement (RQ) from Pittsburgh (PG) concerning an individual (3) involved in drug (O). Specific information pertains to the individual's participation in an organization (1) and denotes he is a leader (A) in the organization. Information possibly involves drug trafficking (533 – FBI CPI code).

The simple criminal example above shows the ability of RIMS to be used across programs and to unite programs where in the past some information could be lost or not noted as important. Simplicity is the key — breaking down the various factors into succinct facts. If several communications or documents appear within the RIMS coding system from several offices with similar information such as the use of Canada for drug trafficking into the U.S. then border offices of the FBI along with other federal, state, local, and tribal law enforcement communities can be notified along with the commencement of liaison with the Canadian government concerning an sudden increase in drug trafficking between the two countries. (Note: It is highly important that the RIMS code be thoughtfully placed on the documents by in investigators or analysts in order to build the catalog of information and intelligence to make the connections and "connect the dots."

EXAMPLE: Source reporting indicates a Seattle group calling themselves the Animal Liberation Front (ALF) completed a computer intrusion which gained them the names and addresses of stockholders in a small but flourishing pharmaceutical company known to use animals for testing purposes.

RIMS Code: RQSE2SU3A0 - Requirement (RQ) from Seattle (SE) concerning a group (2) involved in terrorism (S), who promote animal rights (U). Specific activity of the group was an operation (3) to obtain the names and addresses of stockholders (A – Objectives of Attack). (Note: One place holder of zero where used here in the tenth position)

AND

RIMS Code: RQSE2SU3BC - Requirement (RQ) from Seattle (SE) concerning a group (2) involved in terrorism (S), who promote animal rights (U). Specific activity of the group was an operation (3) that involved cyber intrusion activity (B – Type of Attack) (C – Cyber).

AND

RIMS Code: RQSE2SU3A0-672 - Requirement (RQ) from Seattle (SE) concerning a group (2) involved in terrorism (S), who promote animal rights (U). Specific activity of the group was an operation (3) to obtain the names and addresses of stockholders (A – Objectives of Attack). The cyber (600 series designation) specialty involves the Public Health and Healthcare Industry. (Note: One place holder of zero where used here in the tenth position)

Additional RIMS codes can be created based upon the simple information provided above and the thoroughness of the investigator or analyst. The RIMS code here is showing that a domestic terrorist group is using cyber crimes in their activities which will affect an infrastructure group critical to the welfare of America. By crossing programs and activities we can connect the vast amount of daily intelligence that arrives within the FBI and provide strategic value to the U.S. intelligence and law enforcement communities along with U.S. policymakers.

As seen above, the RIMS code can be generated by an analyst or investigator when initially creating a document for the FBI based upon active investigative work or completed analysis. The RIMS code is the raw form of intelligence which when combined during a specific RIMS search, could yield previously unknown links, anomalies, or patterns for further investigation or research/analysis.

C. FBI PERSONNEL MAKE USE OF RIMS

Since January 2006, FBI personnel in the Pittsburgh FBI Field Division used RIMS on a trial basis with support from the division's executive management. Searches conducted by FBI personnel using the RIMS metadata code were inherently quicker with a higher degree of accuracy due to the exact nature of the RIMS code. A single RIMS search would return all relevant documents on a specific subject. Without RIMS, an analyst or investigator would randomly search various databases on topical subjects using word phrases and common spellings. One specific RIMS code when entered into search criteria of any FBI computer would yield, in a matter of seconds, all documents which held the specific RIMS code. No questionable documents would be retrieved and any misspelled or non-standard words would not be overlooked. Only information requested that matched the code was provided, eliminating extraneous information caused by poor indexing or misspelled names. Information relevance and accuracy was improved. RIMS would reduce the probability that a user of ACS would not retrieve vital information in a timely manner for analysis and making that link to a possible terrorist threat. This innovative system is cost effective, having minimal impact on the FBI's current information technology structure. There are zero new equipment costs to the FBI, and the system uses existing alpha and numeric codes familiar within the USIC and the U.S. government. Additionally, since there are no formal cataloguing, metadata, or retrieval methods approved within the FBI, this cataloguing and retrieval system was an immediate improvement to current FBI information tagging methods.

In the fall of 2005, the FBI embarked on a Domain Management Initiative (DMI) wherein five field offices were provided authority by FBIHQ to find innovative methods or systems to determine the offices' domain using new technology methods to include "thinking outside the box." On January 1, 2006, the RIMS code was initiated on all communications containing intelligence information within the Pittsburgh Field Office of the FBI. On February 16, 2006, the RIMS system was briefed to the four other FBI field offices: San Francisco, Miami, Charlotte, and Little Rock. Training by Pittsburgh personnel was provided the field offices. Additionally, FBI Headquarter personnel from the Directorate of Intelligence were also provided a briefing and training on the RIMS

code. The four field offices agreed to test the RIMS codes on future communications. Members from FBI Headquarters, Directorate of Intelligence, received the RIMS code positively.

D. WHY THE NEED FOR RIMS?

The FBI is not alone within the realm of national security and defense. Numerous other agencies, organizations, groups and individuals contribute to the security of the U.S. The FBI's role in Homeland Security, as mentioned previously, is the prevention/investigation of terrorist acts. As the lead federal law enforcement agency for all domestic terrorism investigations, the FBI must gather, analyze, and share intelligence on terrorists, terrorist activities, and terrorist groups with government leaders, intelligence community, and national/international law enforcement entities. Currently, the FBI does not have the means, other than liaison efforts and joint participation in the NJTTF, JTTFs and Regional Fusion Centers, to have total transparency with its national security partners concerning information sharing and collaboration. This simple information tagging system, RIMS, provides a structured and standardized approach to initially share information throughout the FBI and with its participating national security partners. Finally, this system can be expanded to cover the identification, cataloging and retrieving of non-national security information which would benefit other federal, state, local and tribal law enforcement and intelligence communities in criminal, cyber-based, or intelligence investigations.

E. RIMS AS A CORPORATE PROJECT?

Since January 1, 2006, the Pittsburgh Division used RIMS (called RICS) on all intelligence communications. Success was measured on how quickly information and intelligence could be recalled by agents and analysts and the ease of learning the RIMS system. Investigators, analysts, and professional support were trained to use RIMS in a minimal time period (less than one day). This coding system was cost effective, having minimal impact on the FBI's current information technology structure. There were minimal new equipment costs to the FBI, and the system uses existing codes familiar within the USIC and the U.S. government. Pittsburgh Executive Management was

supportive of the coding system and saw the system as an improvement on the way the FBI and Pittsburgh managed intelligence.

An informal discussion/focus group was created in Pittsburgh which consisted of investigators, analysts, and professional support personnel who had worked with and been trained on the RIMS coding system since January 2006. This group consisted of fifteen Intelligence Analysts, six Special Agents, three Supervisory Special Agents, and two professional support personnel who were responsible for FBI files. The length in government service ranged from over twenty five years to two years. Both men and women were in the discussion group with age ranges from the mid 20s through mid 50s. All personnel worked within the FBI's Intelligence Program (Counterterrorism, Counterintelligence, and Field Intelligence Group personnel) for more than two years. All but one had completed advanced education degrees or certificates after high school.

The Pittsburgh Division's Field Intelligence Group Manager, Supervisory Special Agent Erin M. Beckman, shepherded the discussion group, asking the questions below. The group's results from December 7, 2006, were forwarded to FBI Headquarters for review.

- Is the name ("RICS" by the field office) adequate to describe the system?
- How much training is necessary to personnel for understanding of the system?
- Should the system be expanded to more than 10-13 characters? If so, why?
- Describe the ease or difficulty to use the system?
- What errors would occur when using the system?
- When tagging information, does this aid the agent or analyst in focusing efforts on what is actually being collected?
- Does this system aid agents or analysts in understanding the U.S. Intelligence Community priorities and the FBI priorities?
- What other uses is there for this system?
- Who would benefit from the use of this system?
- Any hidden costs in the use of this system that have surfaced since using the system?

- How can this system be marketed to FBI Headquarters as a possible near term solution to information management?

When discussed within the group[49], all commented that it was easy to use (takes very little thought once trained). The group described the system as a tool that refers back to the Intelligence Community priorities. By tagging information with RIMS codes at the outset (preparation of the document), the information can be retrieved with relative ease. They added the retrieval can be in a very broad sense (if you only is the first five or six characters of a RIMS code as a search term), down to the retrieval of extremely specific information (if you use the entire expanse of characters, including the country or terrorist group specific, 11-13 characters).

The group further added that RIMS can also be searched in ACS and other FBI databases. Results of retrieved information using RIMS versus current accepted search styles with paper file reviews and ACS record checks showed RIMS to be physically effortless (no pulling files) and less time consuming for RIMS users. Knowing the information needed, creating the RIMS code(s) and typing it/them into ACS and other FBI databases, took a small amount of time. The results from the existing enterprise architecture structure within the FBI IT system were presented in seconds as opposed to paper file reviews and numerous (exact) word searches which could take hours. The more exact the RIMS code identification, the more specific the search results which amounted to increased analytical output through less time completing the accepted search styles with paper file reviews and ACS record checks. Additionally, linkages (source reporting from various programs) of reporting were captured where in the past, different programs (criminal versus intelligence or terrorism) did not compare similar information.

Tagging the information also forced the investigators and analysts to think about what they are actually collecting, investigating, and analyzing. In so doing, the group

[49] Discussion Group results from December 7, 2006, were forwarded to FBI Headquarters for review. It should be noted, other field divisions (Miami) have implemented information tagging systems of a similar nature. FBI Headquarters is currently developing a system, called "iMark," with the design based upon the RIMS tagging system. Further development by FBI Headquarters is pending with a possible release in 2007.

began to think about whether their information was being collected, investigated, or analyzed in accordance with the Intelligence Community priorities.

RIMS was also useful to the analysts when drafting Intelligence Assessments: one can search in both broad and limited fashions regarding the topic at hand rather than attempt to use keyword database searches. An example given was when preparing a division counterintelligence threat assessment; the analyst could use RIMS to search the division's information for operatives associated with their countries of interest. With a broader search perspective, the analyst could look at operatives across all countries present within the division and conduct a trend analysis based on the findings. Such information would be much more difficult to extract if the analyst was conducting keyword searches in ACS etc. For the same reasons, RIMS could benefit FBI Headquarters and the researching of information for strategic analyses.

The group felt RIMS also has value with respect to collection management (i.e., assigning RIMS codes to requirement sets.)

The bottom line, according to the FBI discussion group, is implementation across FBI field offices and FBI Headquarters could be quick. The RIMS string itself is not complicated and it costs nothing. As long as it is standardized and users are properly trained in how to code the documents, RIMS could be very effective and time-saving. The group did note that to get a better idea as to its practicality and usefulness, RIMS could be implemented in selected offices (pilot project) for a six-month period.

F. BENEFITS AND POTENTIAL PROBLEMS WITH RIMS

Zalmai Azmi, Chief Information Officer (CIO) for the FBI and personnel within the Office of the CIO have a mission[50] to provide leadership, policy guidance and strategic direction for the FBI's information technology enterprise, to include developing the FBI's IT strategic plan and operating budget; developing and maintaining the FBI's

[50] Information pertaining to the FBI's Office of the Chief Information Officer and his mission statement and goals can be found at http://www.fbi.gov/hq/ocio/mgo.htm (Accessed December 3, 2006).

technology assets; and providing technical direction for the reengineering of FBI business processes. In order to accomplish the FBI CIO's mission, the following goals and objectives were established:

- Actively support the priorities of the FBI.
- Foster and enrich employee productivity and morale.
- Identify and strengthen our core competencies.
- Build and strengthen the key processes that will enable us to successfully fulfill our mission.
- Seek out and leverage external feedback to make changes needed in our organization (i.e., Inspection Findings, customer satisfaction surveys etc.).
- Be responsive to customers (i.e., Inspections Findings, requests for work etc.).
- Aggressively migrate to standard configurations and products.
- Promote the Equal Employment Opportunity (EEO) program, Employee Assistance Program (EAP) and the Upward Mobility (UM) program.

The FBI is involved in information acquisition and the workflow of information management—how information is acquired, who must act on it, how information of all types flows within the FBI, how it must be processed and analyzed, and what types of inferences must be drawn. For information-intensive missions such as criminal investigation and counterterrorism, modern IT and its proper design and exploitation are critical contributors to truly effective processes. Data must be organized and managed in a way to promote the effectiveness of FBI agents and intelligence analysts. Access capabilities required for intelligence analysis in order to determine possible events in the future are crucial to the FBI as it continues to build a viable domestic intelligence agency and supports the U.S. intelligence and law enforcement communities.

In multiple Congressional testimonies[51] before and after 9/11, the director of the FBI, along with other senior FBI executives, acknowledged the need to replace the established FBI information technology (IT) enterprise framework which stove-piped

[51] FBI Director Robert S. Mueller III, Statement before the Senate Appropriations Committee, Subcommittee on the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, March 23, 2004, and Testimony of Bob E. Dies, Assistant Director, Information Resources Division, FBI, Before the Senate Judiciary Committee July 18, 2001, titled "Information Technology and the FBI."

investigative applications. An improved approach to collect and manage FBI case and investigative information was needed. Additionally, the new system must support the operational mission of the FBI by enhancing its information management capabilities. The collection, dissemination, and availability of data and investigative tasking across the entire organization will enable the assembly and management of case information for intelligence and investigative activities and will support rapid and effective information sharing among FBI personnel and with authorized external agencies.

Currently, there is no central search platform to gather information or data mine within a genre of information. Training on data mining and searching the various databases is minimal. Some FBI field offices have taken formative steps to establish structured, relational databases to facilitate robust case management and intelligence support to operations. These offices have elected to use a commercially available, off-the-shelf software analytical application called iBase, which is produced by i2 INC. In addition, several operational units at FBI Headquarters have adopted similar approaches using structured, relational database packages. Ultimately, the FBI must establish an enterprise-wide standardized approach for classifying investigative information into a structured, relational database environment to benefit fully from this technology. One approach would be the use of the RIMS code in order to facilitate case management and process intelligence and share information with approved individuals.

Successful government leaders realize that a key part of their success is leaving a powerful and positive mark through their work. These actions have a profound effect on individuals and society. The FBI is charged with proactively investigating and prosecuting crimes against America to include terrorism along with protecting America from those who would harm America's way of life. An important part of the FBI's success is linked to the powerful and positive impact that the FBI has in their communities (U.S. intelligence and law enforcement communities along with the American public). Therefore, an FBI coding system must be designed to capture, catalogue, and retrieve FBI intelligence information for sharing within the U.S. intelligence and law enforcement communities. The use of the coding system will better capture, catalogue, and retrieve information at a higher success rate and more quickly

within the FBI's current databases. The use of this system is cost effective and will have minimal impact on the FBI's current IT structure and not radically effect the FBI's future IT structure, SENTINEL. The use of the RIMS coding system can be adapted for use by other U.S. intelligence and law enforcement communities for commonality and uniformity in retrieval, cataloguing, and collecting of intelligence information. The use of this system can be manipulated into a non-classified code for utilization by state, local, and tribal law enforcement and intelligence entities. Finally, the use of the coding system within the intelligence community will consolidate and integrate information and intelligence and reduce delays in detecting and retrieving pertinent intelligence obtained and shared across the intelligence community.

G. IMPLEMENTATION PLAN FOR RIMS

1. Blue Ocean Strategy and the Strategy Canvas[52]

Blue Ocean Strategy is a book that provides a blueprint on how to create uncontested corporate market space ripe for growth. Such strategic moves create powerful leaps in value for the firm and its buyers, rendering rivals obsolete and unleashing new demand. If we look at the FBI as a corporation, the creation and use of the RIMS coding system provides the FBI with a new market which has unlimited profitable growth in security of its citizens, increased value in the FBI's ability to manage intelligence and in turn collaborate and share intelligence which in the end will render terrorists and criminals ineffective in the U.S.

As stated by the authors of the Blue Ocean Strategy, "the strategy canvas is both a diagnostic and an action framework for building a blue ocean strategy."[53] It captures the current state of the program or activity under scrutiny and allows for the understanding where the current investment is in products, services, delivery, and what customers receive from the existing activity or program. The canvas enables companies to see the future in the present.

---

[52] W. Chan Kim & Renee Maugorgne, *Blue Ocean Strategy* (Boston, Massachusetts, Harvard Business School Press, 2005).

[53] Kim & Maugorgne, *Blue Ocean Strategy*, 25.

In the case of information sharing by the FBI internally and with the U.S. intelligence and law enforcement communities, an FBI information coding system must be designed to capture, catalogue, and retrieve FBI intelligence information for sharing. From previous testing, it is expected this system will detect and retrieve pertinent intelligence obtained by the FBI. This proposed system will improve the FBI's ability to share information within the FBI and with members of the U.S. intelligence and law enforcement communities and as warranted, with state, local, and tribal entities who aid in the defense of America. There are eight principal factors that the law enforcement and intelligence communities compete on and invest in. They are:

- Source information and intelligence (A)
- Information and intelligence from investigations and operations (B)
- Information and intelligence gained from domestic liaison efforts (C)
- Information and intelligence gained from foreign liaison efforts (D)
- Information Technology Systems and Equipment (E)
- Databases and Software Capabilities (F)
- Information and intelligence gained within accepted federal, state, and local regulations, laws, and accepted practices (G)
- Information and intelligence gained from U.S. intelligence and law enforcement communities along with the public through training and experiences (H)

The following chart captures the above list of factors within the federal, state, and local/tribal sectors, along with the offering level that the sectors receive across the eight key factors. A high score means that the sector offers, invests, and supports more in the sector.

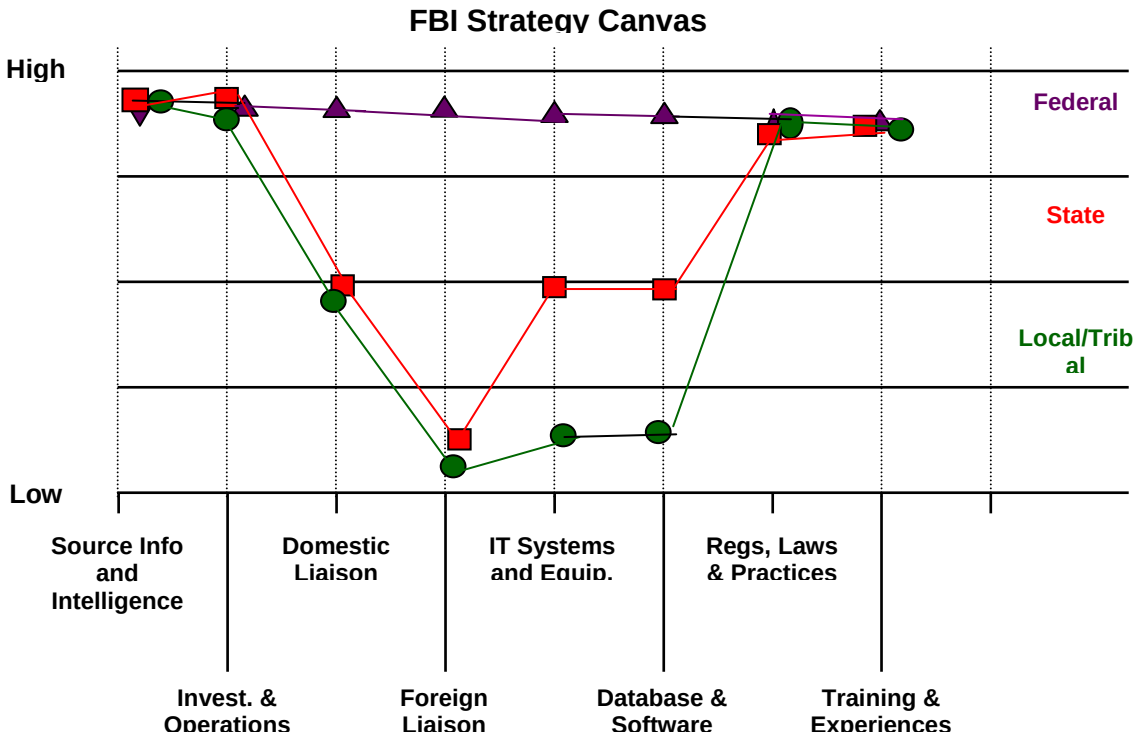
Table 1. Strategy Factors—Competition of Eight Principal Factors.

KEY FACTORS	FEDERAL LEVEL	STATE LEVEL	LOCAL/TRIBAL LEVEL
A	High	High	High
B	High	High	High
C	High	Medium	Medium
D	High	Low	Low
E	High	Medium	Low
F	High	Medium	Low
G	High	High	High
H	High	High	High

The above chart shows federal entities investing and supporting all the key factors within the information-sharing/intelligence initiative in order to maximize the federal government's response to national security. The state and local/tribal levels of support and investment are lower due to current organizational hurdles that need to be overcome in order to execute a new system. The new coding system could provide information sharing and "connecting the dots." This would immediately allow for a visible increase in safety and the lowering crime rates and violence.

In the chart form below, the same information is portrayed. An extreme discrepancy is shown concerning IT matters and liaison which with the implementation of a national information/intelligence tagging system would be decreased.

Table 2. Strategy Canvas—Competition of Eight Principal Factors.



2. Four Action Framework[54]

The second analytic underlying Blue Ocean is the four actions framework. There are four key questions that challenge communities' strategic logic and business model. They are:

- Which factors should be *reduced* well below the industry's standard?
- Which factors should be *created* that the industry has never offered?
- Which of the factors that the industry takes for granted should be *eliminated*?
- Which factors should be *raised* well above the industry's standard?

[54] Kim & Maugorgne, *Blue Ocean Strategy*, 29-35.

The following lists provide answers to the above four questions in regards to a coding system design to capture, catalogue, and retrieve intelligence information for sharing within the U.S. intelligence and law enforcement communities:

Table 3. Four Action Framework

REDUCE	**CREATE**
Equipment complexity Incompatibility of databases	Single database for national intelligence tagging Ease in use Rules/Regulations mandate cooperation Electronic data interchange Speed and Accuracy in use Security of information
ELIMINATION	**RAISE**
Source competition Investigative and Operational competition Personnel competition (positions)	Domestic Liaison Cooperation (Relationship Management) Foreign Liaison Cooperation (Relationship Management) Speed of sharing information/intelligence Compatibility of IT systems and databases

When the four actions framework is applied to the strategy canvas, a new look is revealed at old accepted practices. In the case of information-sharing initiatives within the FBI and the U.S. government, new alternatives and new customers can be analyzed and new factors created within the information-sharing initiative — ease of use, speed of sharing information, compatibility of IT systems and databases, and liaison cooperation. This results in a broad cross section appeal within all levels of the FBI and the U.S.

government in the capturing, cataloguing, and retrieving of intelligence information for sharing within all the U.S. intelligence and law enforcement communities.

3. Value Curve Comparison

According the authors of the Blue Ocean Strategy, the value curve is a basic component of the strategy canvas and "is a graphic depiction of a company's relative performance across its industry's factors of competition."[55] As mentioned earlier, the strategy canvas enables companies to see the future in the present. Embedded in the value curves of an industry is a wealth of strategic knowledge on the current status and future of a business.[56]

The value curve of the FBI's coding system differs distinctively from those of its competitors in the strategy canvas. The FBI coding system has focus which can be seen at once. The system emphasizes speed, interoperability, and feasibility. By focusing in this way, the FBI's coding system is cost effective and an immediate enhancement to current FBI retrieval methods. The system will have minimal impact on the FBI's current information technology structure, have zero new equipment costs to the FBI, and uses existing alpha and numeric codes familiar within the U.S. intelligence and law enforcement communities.

Post 9/11, the FBI's strategy for information sharing was formed reactively as the FBI tried to keep up with other agencies and their information-sharing practices. In order for the value curve for the blue ocean strategists to diverge from the reactive strategists, the four action framework analytic must be applied – eliminating, reducing, raising, and creating. Using this framework would differentiate the FBI's strategy from the other agencies and their practices. For example, the FBI's coding system would pioneer the use of a single database for national intelligence tagging; previously, the government's various intelligence and law enforcement communities operated under separate and distinctive databases with little interoperability and minimal information sharing across agencies.

---

[55] Kim & Maugorgne, *Blue Ocean Strategy*, 27.

[56] Ibid., 41.

A good strategy has a clear-cut and compelling tagline. It delivers a clear message but also advertises truthfulness. The FBI's coding system has new factors such as a single database for national intelligence tagging, ease in use, electronic data interchange, and speed and accuracy in use. Whether the FBI can attain sustained consolidation and integration of information through a new coding system depends largely upon whether the FBI can continuously stay in the forefront during future rounds of blue ocean creation. Lasting excellence is scarcely achievable for any company or agency over the long run. However, the FBI is a powerful agency that is capable of reinventing itself by repeatedly creating new initiatives and projects to meet the U.S. intelligence and law enforcement communities along with the American public's needs.

H. OVERCOMING KEY ORGANIZATIONAL HURDLES

According to the authors of the blue ocean strategy, "once a company has developed a blue ocean strategy with a profitable business model, it must execute it."[57] The challenge of such execution exists and companies can have a tough time translating thought into action. "Blue ocean strategy represents a significant departure from the status quo."[58] There are four hurdles that must be faced when diverging from the status quo. "One is cognitive: waking employees up to the need for a strategic shift."[59] The second hurdle is limited resources. The third hurdle is motivation. "How do you motivate key players to move fast and tenaciously to carry out a break from the status quo. That will take years and managers don't have that kind of time."[60] The final hurdle is politics. To make blue ocean strategy succeed, the company must overcome these key organizational hurdles. To achieve this effectively, "companies must abandon perceived wisdom of effecting change. Conventional wisdom asserts that the greater the change, the greater the resources and time you will need to bring about results."[61]

---

[57] Kim & Maugorgne, *Blue Ocean Strategy*, 147.

[58] Ibid.

[59] Ibid.

[60] Ibid., 148.

[61] Ibid.

I. IMPLICATIONS OF A BLUE OCEAN STRATEGY EXECUTION

The FBI must overcome key organizational hurdles such as the departure from the status quo. The motivation by key FBI personnel to move forward to change the status quo is paramount to make this system operational. FBI employees also need to understand the need for a strategic shift and more or less agree on the contours of the new strategy. Second, the FBI has limited resources. Instead of focusing on getting more resources, the FBI should concentrate on multiplying the value of the resources the FBI has. Finally, politics affect any new initiative. Organizational politics is an inescapable reality of government work. Powerful vested interests within the FBI will resist the impending changes and will fight to protect their positions. Their resistance can damage and even derail a strategy execution process such as a new coding system and/or search platform within the FBI.

For success in this new FBI strategy[62] to occur, the FBI must shift customers' (U.S. intelligence and law enforcement communities) perception of the FBI and the FBI's ability to perform this IT function. The FBI must broaden information sharing among U.S. intelligence and law enforcement communities. In hand, there must be an increase in the communities' confidence in the FBI's IT system. The FBI must employ and train knowledgeable people and provide convenient access and superior service to its customers. Additionally, the FBI must build strategic information and develop strategic skills through the creation of innovative products, focused resources and improved employee effectiveness. Finally, the FBI must understand their customers and work in partnership with them to protect the American public and way of life.

Successful government leaders realize that a key part of their success is leaving a powerful and positive mark through their work. These actions have a profound effect on individuals and society. The FBI is charged with proactively investigating and prosecuting crimes against America to include terrorism, along with protecting America from those who would harm America's way of life. An important part of the FBI's success is linked to the powerful and positive impact that the FBI has in its communities

[62] Federal Bureau of Investigation, "Strategic Plan 2004-2009, FBI Public Website. http://www.fbi.gov/publications/strategicplan/stategicplantext.htm#it (Accessed January 15, 2007).

(U.S. intelligence and law enforcement communities, along with the American public). Therefore, an FBI coding system must be designed to capture, catalogue, and retrieve FBI intelligence information for sharing within the U.S. intelligence and law enforcement communities. The use of the coding system will better capture, catalogue, and retrieve information at a higher success rate and more quickly within the FBI's current databases, using current FBI IT. The use of this system is cost effective and will have minimal impact on the FBI's current IT structure and not radically effect the FBI's future Information Technology structure, SENTINEL. The use of the coding system can be adapted for use by other U.S. intelligence and law enforcement communities for commonality and uniformity in retrieval, cataloguing, and collecting of intelligence information. The use of this system can be manipulated into a non-classified code for utilization by state, local, and tribal law enforcement and intelligence entities. Finally, the use of the coding system within the intelligence community will consolidate and integrate information and intelligence and reduce delays in detecting and retrieving pertinent intelligence obtained and shared within the intelligence community.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. SUMMARY

This thesis set out to determine if the RIMS metadata could be developed and implemented in the FBI in order to have a central search platform for use by FBI analysts or investigators to gather or data mine existing information in furtherance of the FBI's Priorities. A secondary effect would include whether the RIMS code would be an effective and efficient method to capture, catalogue and retrieve intelligence information within the FBI. Validation of this system occurred through actual field use, using the code in specific searches versus the current accepted search styles with paper file reviews and ACS record checks. Results from a RIMS user discussion group solicited comments and suggestions that were in turn forwarded to FBI Headquarters. Additionally, other FBI field divisions implemented similar information tagging systems within their own divisions for a cost-effective and immediate remedy to ensuring FBI information is catalogued and analyzed in a more thorough manner. FBI Headquarters is currently developing a system, called "iMark," with the design based upon the RIMS tagging system. Further development by FBI Headquarters is pending with a possible release to the field divisions in 2007.

The following results are being presented:

* The use of the RIMS code will capture, catalogue, and retrieve information with increased accuracy and effectiveness while decreasing the probability of uncertainty.

* The use of the RIMS code is cost effective and will have minimal impact on the FBI's current Information Technology structure and not radically effect the FBI's future Information Technology structure, SENTINEL.

* The use of the RIMS code can be adapted for use by the whole USIC for commonality and uniformity in retrieval, cataloguing, and collecting of intelligence information.

* The use of the RIMS code can be manipulated into a non-classified code for utilization by state, local, and tribal law enforcement and intelligence entities.

A. FUTURE RESEARCH

Vision of an Interoperable Terrorism Information Sharing Environment

> The vision of the interoperable terrorism information sharing environment, created and maintained in full partnership by all levels of Government, effectively supports detection, prevention, disruption, preemption, and mitigation of the effects of terrorism against the territory, people, and interests of the United States of America.
>
> It does so by enabling the interchange of terrorism information among and between appropriate Federal, State, Local, tribal, and territorial authorities, foreign partners and the private sector. It will support the ability of agencies to acquire additional such information, and, it will protect or enhance the freedom, information privacy, and other legal rights of Americans in the conduct of their activities. Initial Plan for the Interoperable Terrorism Information Sharing Environment, prepared by the Information
>
> — Initial Plan for the Interoperable Terrorism Information Sharing Environment, prepared by the Information Systems Council in response to EO-13356, 20 December 2004.

1. Enterprise Architecture

Enterprise architecture is the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's processes, information systems, personnel and organizational sub-units. They must align with the organization's core goals and strategic direction. Enterprise architecture is becoming a common practice within the U.S. federal government to inform the Capital Planning and Investment Control (CPIC) process. The primary purpose of creating an enterprise architecture is to ensure that business strategy and IT investments are aligned. As such, enterprise architecture allows traceability from the business strategy down to the underlying technology. The FBI and other U.S. intelligence and law enforcement agencies have differing IT Enterprise Architecture. Connectivity by and between all members is needed to ensure that the current and future core goals and strategic direction of the U.S. intelligence and law enforcement agencies and the U.S. government are met.

The RIMS system is an effective and efficient information metadata tagging system within the FBI. It has not been used or tested outside the FBI or with differing enterprise architecture structures. Further validation of the RIMS system outside the FBI may allow a regional or nationwide national security system for information sharing.

One way to initially integrate RIMS between various communities may be with Law Enforcement On-Line (LEO)[63] since most agencies involved with national security issues have access to LEO at http://www.leo.gov and by clicking on the Homeland Security Information Network (HSIN)/ Joint Regional Exchange System (JRIES) portals. Further research, liaison, and tighter regulations concerning access and security within LEO must be facilitated and accepted by all entities that work to ensure the safety and security of America and its citizens.

The FBI may be able to showcase RIMS within the Regional Data Exchange (R-DEx), which provides a web-based platform for the law enforcement community to exchange information. R-DEx enables the FBI to join participating federal, state, tribal, and local law enforcement agencies in regional, full-text information-sharing systems to under standard technical procedures and policy agreements. Initial RIMS training and education — highlighting its collaborative abilities — would be essential to active participation by R-DEx members. Further research, liaison, and tighter regulations concerning access and security within R-DEx must be facilitated and accepted by all entities.

The FBI could also develop RIMS to facilitate information sharing within the National Data Exchange (N-DEx)[64], which would provide a nationwide capability to

[63] LEO has over 50,000 users with secure communications and has implemented the FBI National Alert System with the ability to reach over 20,000 members in five minutes; over 240 Special Interest Groups, including host services for the FBI Bomb Data Center Database, the National Center for Missing and Exploited Children, and the Department of Justice Joint Automated Booking System; and 24/7 operational support, including a Virtual Command Center for special events.

[64] Criminal Justice Information Services (CJIS) is developing the N-DEx, which will provide for the integration and discovery of criminal justice information on a national level, serve as an electronic catalog of structured criminal justice information that provides a "single point of discovery," leverage technology to relate massive amounts of data that is useful information, automate discovery of patterns and linkages to detect and deter crime and terrorism, and afford enhanced nationwide law enforcement communication and collaboration.

exchange data derived from incident and event reports from other nationwide agencies. Like R-DEx, N-DEx will require initial training and education to members and liaison, and tighter regulations concerning access and security within N-DEx must be facilitated and accepted by all entities who work to ensure the safety and security of America and its citizens.

2. Extensible Markup Language (XML)

A goal of homeland security is the development of a nationwide capability to exchange data between all levels of government. The ultimate development of RIMS would involve the development of common intelligence schemas and the use of SOA (System Oriented Architecture) including the use of Extensible Markup Language (XML). XML is a markup language for documents containing structured information. XML makes it easy for a computer to exchange and read data, and ensure that the data structure is unambiguous. If used properly, XML tags can identify, validate and describe data. The proper use of XML will allow data to be more thoroughly described, in a richly structured document and separates data from format and computer platform. Both government and business have both adopted XML as the preferred format for information sharing. XML can make information sharing across many platforms and between agencies possible once XML security architectures are in place within the U.S. government.

OASIS (Organization for the Advancement of Structured Information Standards), a consortium that drives the development, convergence, and adoption of web standards, could provide the collaborative platform among the intelligence communities to develop common schemas and metadata standardization, including enhancement,s and possibly the expansion of RIMS that will meet the needs of all intelligence communities.

BIBLIOGRAPHY

Berkowitz, Bruce D and Allen E. Goodman. *Strategic Intelligence for American National Security*. Princeton, N.J.: Princeton University Press, 1989.

Betts, Richard K. "Analysis, War, and Decision: Why Intelligence Failures are Inevitable." *World Politics 31 (1978): 61-89.*

———. "Surprise Despite Warning: Why Sudden Attacks Succeed." *Political Science Quarterly 95 (1980-81): 551-572.*

Chan, Steve. "The Intelligence of Stupidity: Understanding Failures in Strategic Warning." *American Political Science Review 73 (1979): 171-180.*

Federal Bureau of Investigation. *FBI Strategic Plan for Fiscal Year 2004-2009*. Washington D. C: U.S. Department of Justice, Federal Bureau of Investigation, 2004. http://www.fbi.gov/publications/strategicplan/stategicplantext.htm [Accessed April 2006].

———. *SENTINEL – System Requirements Specification (SRS).* Washington, D.C: U.S. Department of Justice, Federal Bureau of Investigation, July 2005.

Frum, David and Richard Perle. *An End to Evil – How To Win The War On Terror*. New York, N.Y: Ballantine Books, The Random House Publishing Group, 2003.

Kent, Sherman. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press, 1951.

Kind, Peter A. and J. Katharine Burton, *Information Sharing and Collaboration Business Plan.* Alexandria, Virginia: Institute for Defense Analysis, June 2005.

Kim, W Chan and Renee Mauborgne. *Blue Ocean Strategy*. Boston, MA: Harvard Business School Press, 2005.

Levite, Ariel. *Intelligence and Strategic Surprises*. New York: Columbia University Press, 1987.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*, 2nd ed. Washington, D.C: CQ Press, 2003.

National Academy of Public Administration. *Transforming the FBI: Roadmap to an Effective Human Capital Program*. Washington, D.C: National Academy of Public Administration, September 2005.

9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* New York: W.W. Norton & Co, 2004.

Office of the Director of National Intelligence. *The National Intelligence Strategy of the United States – Transformation through Integration and Innovation*. Washington, D.C.: Office of the Director of National Intelligence, October 2005. http://www.odni.gov [Accessed May 16, 2006].

Office of the Inspector General, *The Federal Bureau of Investigation's Pre-acquisition Planning For and Controls Over the Sentinel Case Management System,* Audit Report Number 06-14, Washington, D.C.: U.S. Department of Justice, Office of the Inspector General, March 2006.

———. *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project, Audit Report 05-07*. Washington, D.C.: U.S. Department of Justice, Office of the Inspector General, February 2005.

———. *The Internal Effects of the Federal Bureau of Investigation's Reprioritization. Audit Report 04-39*. Washington, D.C.: U.S. Department of Justice, Office of the Inspector General, September 2004.

———. *A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks*. Washington, D.C.: U.S. Department of Justice, Office of the Inspector General, November 2004 (Released publicly June 2005).

108th U.S. Congress, 2d Session. *Intelligence Reform and Terrorism Prevention Act of 2004 Conference Report*. Washington, D.C.: U.S. Senate and House of Representatives, December 7, 2004.

Treverton, Gregory F. *Reshaping National Intelligence for an Age of Information*. New York: Cambridge University Press, 2001.

U.S. Government Accountability Office. *FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed, GAO-02-865T*. Washington, D.C.: U.S. Government Accountability Office, June 2002.

———. *FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Remain, GAO-03-759T*. Washington, D.C.: U.S. Government Accountability Office, June 2003.

———. *FBI Reorganization: Information Technology: FBI Needs An Enterprise Architecture To Guide Its Modernization Activities, GAO-03-959.* Washington, D.C: U.S. Government Accountability Office, September 2003.

———. *FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities, GAO-04-578T*. Washington, D.C.: U.S. Government Accountability Office, March 2004.

———. *9/11 Commission Report, Reorganization, Transformation and Information Sharing,* GAO-04-1033T, Washington, D.C.: U.S. Government Accountability Office, August 3, 2004.

———. *Information Technology: Foundation Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements, GAO-04-842*. Washington, D.C.: U.S. Government Accountability Office, September 2004.

U.S. Government Printing Office. *Commission on the Roles and Capabilities of the U.S. Intelligence Community (Aspin-Brown Commission).* Washington, D.C.: U.S. Government Printing Office, 1995-1996.

White House. *Further Strengthening Federal Bureau of Investigation Capabilities, Memorandum from the President to the Attorney General.* Washington, D.C.: The White House, November 23, 2004.

———. *National Strategy for Combating Terrorism (NSCbT),* February 2003. Washington, DC.: U.S. Government Printing Office, 2003.

———. *National Security Strategy of the United States.* Washington, D.C.: U.S. Government Printing Office, September 2002.

———. *Strengthening the Ability of the Department of Justice to Meet Challenges to the Security of the Nation, Memorandum from the President to selected members of the Cabinet, the Director of National Intelligence, the Assistant to the President for National Security Affairs, and the Assistant to the President for Homeland Security and Counterterrorism.* Washington, D.C.: The White House, June 29, 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California