THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 8 NUMBER 11

MAY 2010

INFORMATION SHARING

Contact: CIPP02@gmu.edu
703.993.4840

This month's issue of *The CIP Report* highlights the critical yet challenging task of improving information sharing between the public and private sectors.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, the U.S. Department of Homeland Security's (DHS) Office of Emergency Communications (OEC) discusses the development of the National Emergency Communications Plan (NECP). The Markle Foundation then explains why the virtual reorganization of the government is necessary to improve national security. Next, an Assistant Professor of Law at the George Mason University School of Law reviews the challenges that are related to information sharing and provides suggestions for improving information sharing. A Professor of Marketing at the George Mason University School of Management also assesses the lessons that were learned from September 11, 2001. Then, the Director of the University of Maryland Center for Advanced Transportation Technology Laboratory provides information on the Regional Integrated Transportation Information System (RITIS), an automated data sharing, dissemination, and archiving system. Finally, the Director and Managing Editor of the Central Intelligence Agency's (CIA) World Intelligence Review (WIRe), a relatively new information sharing tool within the U.S. Intelligence Community (IC), describes the evolution of this innovative initiative.

This month's *Legal Insights* examines the post-9/11 national security legal environment. This month's issue also features a new partnership between James Madison University (JMU) and the Drug Enforcement Administration (DEA) and provides a brief update on the attempted bombing of Northwest Airlines Flight 253 on Christmas Day 2009. This issue also announces our next conference to be held on June 17. Lastly, we developed a timeline that chronologically lists relevant information sharing legislation.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

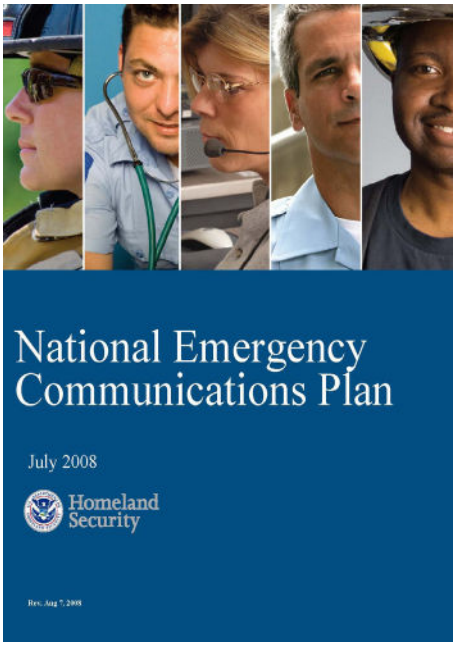
We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Implementing a National Plan to Improve Emergency Communications

by Chris Essid
Director, U.S. Department of Homeland Security, Office of Emergency Communications

When Hurricane Katrina devastated the Gulf Coast in 2005, emergency response personnel around the country quickly found that the Hurricane had destroyed the vital communications infrastructure needed for emergency responders to effectively communicate during the disaster. Emergency responders rely on the ability to share vital voice and data information across disciplines and jurisdictions to respond to day-to-day incidents as well as catastrophic events such as Hurricane Katrina. To strengthen interoperability across the country and avoid future communications failures, such as in the response to Hurricane Katrina, Congress established the Office of Emergency Communications (OEC) as part of the U.S. Department of Homeland Security (DHS) in April 2007.



One of OEC's initial interoperability initiatives was to develop the National Emergency Communications Plan (NECP) as the first national strategic plan to address the shortfalls of emergency communications and serve as a strategy for improving emergency communications across all levels of government. Since its release, the NECP has proven to be an effective tool for building, sustaining, and improving emergency communications across the country.

As emergency responders know, an emergency does not always result in a tragedy — a strategic response can save lives and minimize damage. But without a strategy, confusion and lack of coordination can lead to efforts wasted and lives lost. Developed with the input of more than 150 stakeholders representing Federal, State, local, and tribal responders as well as the public safety association community, the NECP was delivered to Congress on July 31, 2008. The ambitious Plan includes three strategic goals, seven objectives, and 92 milestones, which provide a guide for emergency responders and relevant government officials to make measureable improvements in emergency communications over a three-year period. The NECP is a living document, developed *by* public safety practitioners *for* public safety practitioners who work in the field every day. Successful implementation requires the same kind of commitment from practitioners to become a true functioning plan. We have a shared responsibility to implement the NECP through a nationwide, cross-discipline, cross-jurisdictional, and intergovernmental effort. The emergency response community is seeing the benefits of the plan through more targeted policies, grant funding, and technical assistance. Since the release of the NECP, the Nation has achieved over 80 percent of the 73 milestones recommended for Federal, State, and local agencies and their partners. Over 75 percent of all 56 States and territories now have full-time interoperability coordinators. Ensuring a single source of accountability, responsibility, and coordination to realize efficiencies, establish partnerships, and reduce duplication of efforts will achieve strengthened emergency communications capability within States. To further coordinate and to provide a forum for discussion and innovation, OEC developed a council for all statewide coordinators to interact and learn from one another. Although the needs of States vary greatly, accessing model policies and lessons

(Continued on Page 3)

NECP *(Cont. from 2)*

learned through the council makes an impact on improving governance within the States.

The NECP puts a strong focus on governance as it provides a foundation for coordinated implementation of statewide initiatives. Good governance provides a unified approach for decision-making across multiple disciplines and jurisdictions. It is especially important to have a strong governance structure in place when planning for large-scale events. In 2009, the Tampa Bay urban area hosted the Super Bowl, requiring 20 Federal, State, and local public safety agencies to coordinate communications and resources to ensure the oversized crowds remained safe. Using the established governance structure within the State, the urban area set up an emergency communications subcommittee that met frequently leading up to the Super Bowl. The planners implemented the National Incident Management System/ Incident Command System structure as recommended in the NECP and released detailed standard operating procedures ahead of time. Federal agencies aligned planning and staging of mobile resources with State and local needs. On the day of the event, this cross-discipline, multi-agency planning paid off — all those involved understood the command structure.

But how does having a strategic plan like the NECP and governance structures help improve communications for emergency responders? The most noticeable benefits of NECP implementation happen when a disaster or emergency actually strikes. Every State and territory has requested and received technical assistance to support their interoperable communications efforts. OEC conducted 66 All-Hazards Type III Communications Unit Leader (COML) courses — at least one in each State and territory — and trained over 1,600 personnel to coordinate on-scene emergency communications during a multi-jurisdictional response. The training has had an immediate impact on the Nation. In several cases, participants of the COML course were immediately deployed to both local and regional incidents. For example, in August 2008, several COML participants at a training session in Houston, Texas went immediately from the COML class to prepare and respond to Hurricane Gustav, as it barreled down on the Gulf Coast region. Similarly, in January 2009, a severe ice storm disabled emergency communications in Kentucky and surrounding States. COML students — who had been trained just a week before the storm — deployed to Kentucky to assist local responders with incident communications coordination. The training received in COML class helped the graduates assist other agencies in restoring communications infrastructure and therefore providing the critical communications emergency responders need.

The impact of the NECP is also being felt outside of the U.S. borders. Just hours after a 7.0 magnitude earthquake struck the Caribbean nation of Haiti on January 12, 2010 urban search and rescue teams from the United States were alerted and prepared for deployment. Once in Haiti, communications experts relied on their COML training to maintain communications throughout the devastated area. COML training prepared these emergency responders to use traditional and non-traditional communications to be prepared for anything during response to large-scale disasters. Despite the destruction and despair surrounding them, OEC-trained COMLs used all means possible to establish a reliable path to share information among those responding to the disaster.

The NECP has helped to prepare emergency responders by directing training and resources where they are needed most. While OEC continues to work with stakeholders to fully implement the NECP, the office is also updating the plan. Following the advice of the public safety community, OEC is collaborating with working groups to engage new voices and recognize the partnerships between the emergency response community and the health, emergency management, transportation, utilities, and industry sectors that are necessary for keeping our Nation safe. In addition, we will further enhance the NECP by adding a vision and strategy for employing emerging technologies. As technology continues to evolve, it is more critical than ever to focus

(Continued on Page 21)

Meeting the Threat of Terrorism: Information Sharing and a Virtual Reorganization of Government to Improve National Security

by The Markle Foundation

The importance and the need to mobilize information to prevent terrorism became clear on September 11, 2001. For all the Nation has invested in national security since that date, it is equally clear that the terrorist threat and the need for knowledge about that threat have not abated. The failed Christmas Day attack on a Detroit-bound passenger jet coming from Amsterdam is a clear reminder that America remains vulnerable. For all that has been done, we simply have not adequately improved our ability to know what we know about these threats. If there is another successful terrorist attack on the United States, the American people will neither understand nor forgive a failure to have taken this opportunity to get the right policies and structures in place.

Information sharing must be considered an urgent national priority. Information sharing must be considered an urgent national priority not just among intelligence agencies but throughout all levels of government, with foreign governments, as well as the private sector. The goal is to create a trusted environment that fosters information sharing and collaboration among those with information useful to understand potential terrorist threats; where policies and technologies are developed in tandem; and where security is enhanced and civil liberties are protected.

It will take a transformation — a virtual reorganization — of how our government works and trust among participants, policy makers, and the public. Each must be confident that information will be collected and handled in a way that both enhances national security and protects civil liberties.

Since 2002, the Markle Task Force on National Security in the Information Age has recommended ways to improve national security decision-making by transforming business processes and how information is shared.[1] The Task Force brings together a diverse and bipartisan group of experienced former policy makers from the Carter, Reagan, Bush, Clinton and Bush administrations, senior executives from the information technology industry, and privacy advocates. Task Force proposals have been adopted by Executive Order and codified in two pieces of legislation, The Intelligence Reform and Terrorism Prevention Act (IRTPA) and The 9/11 Commission Recommendations Implementation Act of 2007.

Leadership is critical to continued progress: leadership from the President, the Congress, and State and local government. Important steps have been taken. For example, IRTPA created the Office of the Director of National Intelligence (ODNI) and, within the White House, a new position has been established, a Senior Director for Information Sharing Policy. But overall, implementation efforts have slowed by a lack of clarity and confusion over responsibility as well as institutional resistance and bureaucratic delays.

Information Sharing

Too often information sharing has become simply passing information to another agency where it is amassed but not properly analyzed. The problem is not the failure to share, but the belief that the job is done once the information is shared. We can succeed in "collecting" or sharing intelligence but not in "connecting" or understanding the intelligence.

Successfully "connecting and understanding" information demands the transformation of how government does business and the creation of an information sharing framework that enables collaboration not just between computers but among teams of

(Continued on Page 5)

[1] All the reports and recommendations can be found at http://www.markle.org/.

Virtual Reorganization *(Cont. from 4)*

people. Real-time virtual collaboration promotes agile decision-making by eliminating the seams between departments and agencies that are often exploited by our enemies.

The Task Force is proposing a "virtual reorganization" of government — a broad, immediate transformation across government — to change how people and technology work together to ensure we can meet today's challenges and are agile enough to meet future challenges. It recognizes that neither people nor technology alone will succeed but that data must talk to data and people must collaborate more. Our national security depends on the ability of our government to be flexible enough to adjust to circumstances as they come and to meet the challenge of enemies who will continue to adapt. The next attack may not come from the air, and the United States must be prepared, whether our enemies are attempting to attack our critical infrastructure in cyberspace, deploy biological weapons, or smuggle explosives through airport security, as in the recent, unsuccessful attempt on Christmas Day 2009.

Taking Action

The Task Force has offered specific recommendations to overcome the significant cultural and bureaucratic hurdles that impede information sharing. These recommendations include:

Discoverability: All information related to national security should be made "discoverable" to facilitate quickly piecing information together across a distributed network. Authorized users must have the capacity to discover and locate relevant information quickly and efficiently. Data should be tagged with standardized information that can be indexed and searched, the same way a library card catalogue is indexed. A decentralized system like this allows an arriving piece of data to be placed automatically in the right hands, improving security and minimizing privacy risks by avoiding bulk transfers of data.

Authorized Use: Discoverability should be combined with an Authorized Use standard to determine whether a user is authorized to see information that has been discovered. This Authorized Use standard would overcome obstacles in the present system of classification and permit an agency or its employees to obtain information based on their role, mission, and a predicated purpose.

"Risk Management:" A "risk management approach" to classified information would better balance the risks of disclosure with the risks of failing to share information. This requires an information architecture that emphasizes *pull* technology, permitting participants to locate and access information they need, over *push* technology, which distributes information broadly, whether recipients need it or not.

Dispute Resolution: A government-wide dispute resolution mechanism is needed to facilitate responsible, consistent, and lawful information sharing. No matter how clear and consistent the guidelines for information sharing, disputes will be inevitable and a timely, easy to use and efficient process is necessary.

Improving Decision-Making: The information sharing environment should consider the particular needs and practical constraints of senior decision-makers. It should facilitate a more robust two-way exchange between analysts and decision-makers for tasking and analysis, provide decision-makers a more nuanced understanding of the strengths and weaknesses of information underlying finished analysis, include divergent perspectives, and reduce the dependence of policy makers on stove-piped intelligence units within their organizations.

Tools, Training and Procedures should be developed to enhance senior officials' use of the information sharing environment and its technological capabilities: Significant attention should be paid to human capital by expanding community-wide training on a common set of skills, best practices, and the rules and guidelines applicable to information sharing.

Audit Systems should be used to facilitate both accountability and better coordination of analytical activities.

Privacy and Civil Liberties protection require government-wide privacy policies for information sharing to match the

(Continued on Page 22)

Information Sharing and Agency Self Interest

by Nathan A. Sales*
Assistant Professor of Law, George Mason University School of Law

It didn't take long after 9/11 for the conventional wisdom to crystallize: The devastating terrorist attacks were almost immediately, and almost universally, blamed on the intelligence community's failure to share information. While virtually everyone agrees that information sharing is a good thing, it has proven harder to put that consensus into practice. The feds still haven't figured out how to connect the dots.

Congress has spent years trying to goad our cops and spies into sharing more. In 2001, the USA PATRIOT Act allowed Federal prosecutors to give data that is uncovered through grand-jury investigations and wiretaps to spies in the intelligence community. A year later, Congress directed Federal agencies to swap homeland-security information with each other. In 2004, the government established an "information sharing environment" to encourage the free flow of national security data.

Despite a decade of effort, however, our information sharing system remains a work in progress. The attempted Christmas Day bombing is only the most recent fumble. Intelligence officials compiled an impressive array of clues that Al-Qaeda was planning something big. But we missed the chance to detect and disrupt a potentially catastrophic attack because these warning signs weren't widely shared. Why not?

Why, after dozens of statutes, executive orders, academic papers, and op-eds extolling the virtues of information sharing, are our intelligence agencies still hoarding data from one another? Part of the reason, as I argue in a recent law review article, is because it is not in their interest to share. Information sharing threatens two of the things intelligence agencies prize the most — influence and turf.

Intelligence agencies want to influence the President and his advisors. That does not mean that they are out to manipulate the President into embracing any particular policy, but they do want him to rely on their judgment more than he relies on their rivals'. The Federal Bureau of Investigation (FBI) wants the President to accept its assessment that a given Waziristan-based cell represents a grave threat to the national security, not the Central Intelligence Agency's (CIA) assessment that the cell is not much danger at all.

Agencies fear that sharing will cause their influence to wane. It is basically a free-rider problem. If the FBI gives the CIA a piece of data that turns out to be the silver bullet, the CIA will get all the glory for the resulting intelligence breakthrough. Which agency do you think the President is going to call the next time a crisis breaks out?

Intelligence agencies also want to protect their turf. They want to run their operations as they see fit without interference from bureaucratic competitors. Sharing makes that harder. Suppose the CIA tells the FBI that it has uncovered a North Korean mole at the Nuclear Regulatory Commission. The bureau might storm in and insist on prosecuting the spy immediately, preventing the CIA from turning him into a double agent and using him to feed misinformation to Pyongyang.

The intelligence community is not going to start sharing information simply because Congress and the President say please. It is not enough for our nation's lawmakers to tear down the wall; intelligence agencies need to be given reasons to climb over the rubble.

So what can be done? For starters, policymakers could create favorable incentives by offering employees meaningful rewards. Those who share could be given promotions, plum jobs, and cash bounties. Besides the carrots, it would not hurt to have some sticks. Employees who persist in hoarding

(Continued on Page 24)

Information Sharing: Lessons from the Post 9/11 Environment

by Kevin McCrohan*
Professor of Marketing, School of Management
George Mason University

The economy of the United States, in particular its critical infrastructure, is considered to be one of the main target sets for terrorist actions. It has been specifically targeted by Al-Qaeda on numerous occasions over the past fifteen years. In 1998, Osama Bin Laden's Fatwa against the United States urged his followers to kill Americans and plunder their money. Within a short time of the Fatwa, attacks followed against U.S. Embassies in Nairobi and Dar es Salem in 1998 and the USS Cole in 2000. With the 9/11 attacks, Al-Qaeda had succeeded in attacking emblems of U.S. political, military, and economic power.

Al-Qaeda's intent to attack the inherently private sector owned and operated critical infrastructure of the United States led to the release of an October 9, 2002 National Infrastructure Protection Center (NIPC) Infrastructure Sector Notification, which reads, in part, as:

Potential [Al-Qaeda] Threats to Economic Targets in the United States and Abroad Infrastructure Sector Notification:

The U.S. intelligence community continues to assess that Al-Qaeda plans to attack targets which they believe would be readily recognized as representing U.S. economic interests. The U.S. intelligence community continues to receive general threat reporting on such sectors as financial institutions and other market related facilities, the airline and maritime industries, and government facilities and installations.[1]

Additional warnings and sector notifications focused on specific infrastructure as details of Al-Qaeda's planning, tactics, techniques, and procedures followed successive captures of Al-Qaeda's leadership.

In addition to the importance of these private sector entities to the functioning of the U.S. and global economies, they have significant national security (NS) and emergency preparedness (EP) functions. They are interdependent and many are dependent in large part on resilient and robust telecommunications services to support their normal operations as well as their NS/EP services.

We now know that at the same time the 9/11 attacks were in their final operational phases, the physical and virtual reconnaissance for the post 9/11 attacks planned for the United States was ongoing in New York City and Washington, DC. The declassified information in the Dhiren Barot (AKA Bilal, Abu Musa al-Hindi, Abu Eissa al-Hindi) surveillance tapes identified five targets, detailed information on the Banking and Finance Sector, the merging of virtual and physical reconnaissance, and recommendations for attack vectors.

The critical infrastructure of the United States was first identified by Presidential Decision Directive-63 (PDD-63) in May 1998. Subsequent Executive Orders, Executive Order 13231 (EO-13231) in October 2001 and Homeland Security Presidential Directive-7 (HSPD-7) in October 2003, reconfirmed the initial eight and added an additional five critical infrastructure sectors. In February 2006, the National Infrastructure Protection Plan (NIPP) identified four more; the 2009 NIPP now identifies 18 critical infrastructure/key resource (CIKR) sectors.

The value of public-private sector information sharing has been accepted since before the President's Commission on Critical Infrastructure Protection and has been part of every plan or review since the Commission. However, its success appears to remain

(Continued on Page 8)

[1] The complete notification is available at: http://www.rmra.ws/rmra_news_021024.html.

Post 9/11 Environment *(Cont. from 7)*

idiosyncratic and timely analysis and dissemination of information remains difficult as evidenced by the successful terrorist attack by Major Hassan at Fort Hood on November 5, 2009 and the attempted attack on Christmas Day 2009 by Umar Farouk Abdulmutallab.

Introduction

The following comments note examples of information sharing in the immediate post 9/11 environment and conclude with some suggestions for effective information sharing for risk management.

A significant issue in information sharing is the difference in the value proposition between public and private sector entities. The private sector functions in an overwhelmingly benign, diverse, democratic environment and the role of the firm includes innovation, profits, and employment; it is not self protection.

Public sector agencies involved in public safety, defense, intelligence, and homeland security function in bureaucratic, comparatively slower, more nuanced environments that still struggle with the conflict between the need to share and the need to protect information as well as the sources and methods from which the information was developed.

In the private sector, more realistic firms understand that they face a low probability/catastrophic consequence attack so their goal is maximum protection for minimum cost, consummate with the threat. That obviously requires actionable and timely information sharing if resources and trust is not wasted. Unfortunately, information sharing in the public sector is constrained by the limited, opaque, and broad nature of threat information that limits the value of information sharing and frequently results in the belief on the part of the private sector that information is being withheld.

Yet, in spite of these issues, the value of information sharing is accepted; a strong desire exists in both sectors for it to work. When it works, it identifies, deters, and helps to respond to potential threats of terrorist or natural disasters.

Please note one caveat. The experiences and effective strategies for information sharing are those of the immediate post 9/11 world. They were shaped by intense feelings of patriotism on the part of private and public sector actors, a shared vision of an immediate threat, and an unusual degree of autonomy and commitment among the participants. They also reflect the author's experiences at the FBI's NIPC shortly after 9/11.

Major Lessons

The major lesson from this environment was that four factors contribute to successful public-private sector information sharing:

- Empowerment-parties must be enabled to act without approval by multiple layers of bureaucracy.

- Trusted relationships-parties must engage in activities that develop mutual respect and trust.

- Speed-parties must be able to react in a timely fashion.

- Mutual education-parties must understand the infrastructure and the intelligence process.

Empowerment, Trust, Speed, and Education

Empowerment

In the months following 9/11, government agencies, including the Department of Defense, cooperated with staff agencies such as NIPC. That resulted in an influx of personnel far more concerned with preventing the next terrorist attack than in the codification of reporting relationships. Activities were under staffed; the workload was extremely heavy; individual responsibilities were very broad (for example, "develop our (NIPC's) relationship with the financial sector"); and individuals responsible for relationships with specific sectors had great latitude in their relations with their private sector counterparts.

On the private sector side there was understandable concern over sharing information with Federal agencies. Concerns voiced by the private sector included, but were not limited to, how would the information be used, how would it be protected, how would the Federal partner share information, and many others. Fortunately, the Banking and Finance Sector had a functioning Information Sharing

(Continued on Page 9)

Post 9/11 Environment *(Cont. from 8)*

and Analysis Center (ISAC) and many in the Sector came forward to work with NIPC, first individually and then through a Financial Services (FS)-ISAC-NIPC Memorandum of Understanding (MOU). The result was that a comparatively small number of individuals were empowered to share threat information in a timely fashion.

Trusted Relationships

Trust can be achieved by meetings, training, and exercises, but to quote Samuel Johnson, "[n]othing focuses the mind like a hanging." Until the capture of Abu Zubaydah and reports in April 2002 that Al-Qaeda was planning to attack banks in the United States, the opportunity for personnel to work together in a high threat environment had not occurred. While there were some issues in the time line for the warning, the relationships that developed among NIPC and FS-ISAC personnel quickly led to a MOU for information sharing and preparations for the first anniversary of 9/11.

Speed

The dissemination of the threat information that resulted from the capture of Abu Zubaydah had suffered from delays due to the receipt of more detailed information about the planning for the attacks as well as coordination issues with the Sector. Some of these issues involved relationships among participants within the Sector as well as the appropriate time to allow for reviews of warning materials.

The outcome of these concerns was a memorandum of understanding among public-private sector parties that allowed for information/ warnings to be developed and disseminated in a timely fashion.

Mutual Education

Certainly in 2002, and possibly even today, there appeared to be a belief on the part of the private sector that the intelligence community had very specific information about planned attacks, the target, timing, etc., while those in the community were well aware of the vacuous nature of indicators of a possible attack. That misperception needed to be addressed. On the part of those in the public sector detailed to help protect the infrastructure, while they brought some expertise on the working of the sector with them, they lacked detailed information about what were the most critical systems and potential targets. This lack of knowledge also needed to be addressed.

An excellent example of this was provided by the efforts of the law enforcement and intelligence communities out reach to senior business executives following an array of threats in fall 2002. During that time, numerous threats against economic and financial targets in the United States were made on al-Jazirah by Osama bin Laden and Ayman al-Zawahiri. These threats indicated that imminent high profile attacks were planned and that personnel were in place awaiting an optimal on debriefings of a senior Al-Qaeda operative, of tactical situation for the attacks. At that time, research had shown that there was approximately a 1 in 3 chance that an attack would follow a major bin Laden or al-Zawahiri speech.

The response to this heightened threat environment was teleconferences by DHS, CIA, and FBI senior executives with thousands of senior executives in the private sector. These teleconferences noted latest information on targets, explained the terrorist surveillance cycle and need for counter surveillance teams, and the need for randomness in physical security. The NIPC responded with efforts to educate the private sector on low cost solutions for physical security.

Success

As the first anniversary of 9/11 approached, NIPC and FS-ISAC established a team that relied on operational (military personnel with training in small unit tactics) and intelligence personnel so that intelligence could be processed and analyzed from the perspective of operators and Sector experts. The partnership was effective at that time and in the heighted threat environment that immediately followed.

Information Sharing for the First Anniversary of 9/11

The U.S. intelligence community had received information, based on debriefings of a senior Al-Qaeda operative, of possible terrorists

(Continued on Page 10)

Post 9/11 Environment (*Cont. from 9)*

attacks timed to coincide with the anniversary of the September 11th attacks on the United States. While the information was predominately focused on attacks in South Asian countries, concern on the part of U.S. officials over attacks in the United States on the anniversary of 9/11 resulted in the first increase in the threat level to Orange on September 10, 2002. Even absent this action, there was concern on the part of the Banking and Finance Sector that attacks could occur.

The response of NIPC and FS-ISAC was to provide communications systems to trusted partners, develop a communications plan, provide for 24/7 on call availability, and conduct two scheduled contacts per day to share information. These contacts followed the process noted below:

- Infrastructure liaisons reviewed threats in Operations Center for overall threats and Sector specific threats.
- Infrastructure liaisons met, discussed threats to all infrastructure.
- Infrastructure liaisons reported significant findings, if any, to Sector liaisons.
- Sector liaisons were prepared to report results of sector reports.
- Infrastructure liaisons met immediately after all contacts had been made, discussed any potential threats reported by the respective infrastructures and reported back to the Operations Center.

This process was repeated at the end of the day and continued until the threat level was reduced on September 24, 2002.

The results of this activity cemented the relationships among the public and private sector partners and prepared them for the threats that followed after the first anniversary of 9/11.

Information Sharing during Fall 2002

As noted above, the Banking and Finance Sector experienced numerous threats against economic and financial targets by Osama bin Laden and Ayman al-Zawahiri during October 2002. These threats indicated that imminent high profile attacks were planned and that personnel were in place awaiting an optimal tactical situation for the attacks.

Information discovered in July 2004 linked to Dhiren Barot (AKA Bilal, Abu Musa al-Hindi, Abu Eissa al-Hindi) found well developed surveillance documents of financial and other sites. These documents had been collected in spring 2001 and appeared to suggest psychological and kinetic objectives. Although the attacks were never executed, the relationships forged during the standup for the September 10, 2002 increase in threat level for the anniversary of the 9/11 attacks served the Nation well during this time period. As evidenced by the information publicized in 2004 concerning the files, the surveillance of financial sites conducted pre 9/11 was professionally done, contained detailed targeting information, and if attacks had been successful, would have resulted in catastrophic consequences. However, information sharing before, during, and after the threats recorded in October 2002 allowed the Nation to deter what with 20/20 hindsight may have been the execute order for attacks on financial sites in New York City and Washington, DC.

Conclusion

Lessons learned from the immediate post 9/11 environment appear to remain as important today as they were at that time. Empowerment — personnel must be able to overcome internal bureaucratic barriers and share threat information before "consensus" — is reached. Trusted relationships — as personnel work together in the face of general or specific threats, they will understand the constraints of each others' environments — are established. They may also be more willing to expend resources for a finite period of time on the basis of information from a trusted private or public sector individual knowing full well that they may never know if the funds were wasted or if they had compromised terrorist plots. Speed — the change in attitude from need to protect to need to share — must move beyond buzz words. Mutual education — intelligence analysts are good, good intelligence analysts working with operators are better, and teams that include cleared, knowledgeable, private sector participants — provide the expertise and focus for significantly better products. ❖

(Continued on Page 24)

Regional Situational Awareness through Transportation Systems Integration

Michael L. Pack, Director
Center for Advanced Transportation Technology Laboratory, University of Maryland

Transportation is the backbone of our civilization and the reason for our economic prosperity for the past 50-plus years. Accompanying this massive transportation system are significant challenges, opportunities, and even serious risks. Getting into an automobile is the most dangerous activity most of us do every day. Approximately 1.3 million people die each year on the world's roads; between 20 and 50 million sustain nonfatal injuries.[1] In the United States, over 40,000 people die, 2.5 million people are injured, and over 4 million are involved in property-damage crashes annually. Our transportation system is even deadly for first responders, including firefighters, police, and emergency medical technicians. Surprisingly, most firefighters or police officers who are injured or killed on the job meet their fate on the side of the road.

In Washington, D.C., it is estimated that congestion alone costs over $2.7 billion annually, including 134 million person-hours of time and 91 million gallons of gasoline.[2] Nearly half of this congestion is due not to traffic volume but to the effects of incidents such as crashes, disabled vehicles, and weather-related hazards. This congestion costs individual motorists time and money, reduces the region's economic competitiveness, and decreases air quality by increasing vehicle idling time and emissions. So, what is being done to try to solve some of these massive issues? Most State, county, and city departments of transportation (DOTs) have created traffic management centers (TMCs) and emergency operations centers (EOCs) whose responsibilities include the real-time monitoring of traffic conditions, incident response, weather operations, and traveler information. Traffic controllers monitor freeways and secondary roads via a massive array of sophisticated sensors, cameras, roving patrols, scanners, and other technologies. When a problem is detected, the appropriate responders are dispatched to the scene to help unblock lanes, setup traffic control to protect first responders, and notify the public. Studies have shown that for every 1-minute that a lane is blocked, the chances of a secondary incident occurring increases by 3%. Therefore, these traffic management programs can have significant and long-lasting social and economic benefits for a metro area. Unfortunately, each TMC has procured its own separate software solution to manage traffic and notify the public. Each of these systems was created by separate vendors, all classify incidents and events differently, and none are capable of sharing real-time information with one another, especially in any meaningful way. For the Washington D.C. region, this means that Virginia, Maryland, and the District of Columbia are wholly unaware of incidents and traffic conditions directly across their borders. Commuters in the D.C. region do not care about political and jurisdictional boundaries. They simply want a seamless transportation network from State-to-State and freeway-to-arterial. Yet, interagency coordination has been ad-hoc at best. Local traffic management centers, EOCs, police departments, and other agencies are in the same boat.

This need for regional management of Washington, D.C.'s

(Continued on Page 12)

[1] World Health Organization, Global Status Report on Road Safety: Time for Action (2009), www.who.int/violence_injury_prevention/road_safety_status/2009/en/index.html.

[2.] D. Schrank and T. Lomax, 2009 Urban Mobility Report, Texas Transportation Institute, 2009, http://tti.tamu.edu/documents/mobility_report_2009_wappx.pdf.

Transportation Systems *(Cont. from 11)*

transportation system was impetus for creating the Regional Integrated Transportation Information System (RITIS). RITIS is an automated data fusion and dissemination system that compiles transportation data from each participating agency, standardizes it, and makes it available to other participating agencies back through each agency's existing transportation management systems (Figure 1). RITIS is a true data integration and dissemination platform, the goal of which is to foster coordination, cooperation, and analysis through real-time and archived transportation system data sharing. RITIS strives to encourage maximum use and dissemination of transportation data sets while still protecting the individual data rights and security of each of the contributing agencies. RITIS has three major components:

1. **RITIS Real-time Data Feeds**: Secure, real-time push and poll standardized data feeds that can include traffic, transit, event, incident, geospatial, and weather data.

2. **RITIS Real-time Website**: Secure website that allows users to view real-time RITIS data in a single location.

3. **RITIS Data Archive**: Includes access to tools that allow users to download historical RITIS data, run reports, performance measures, and analysis.

RITIS Data Feeds

The RITIS data feeds are services that provide direct access to real-time incident, event, detector, probe, and other ITS device data and status. The RITIS data feeds are designed to facilitate integration of RITIS data back into legacy and third party systems. The secure data feeds provide for implementation flexibility, both in data format and retrieval method.

The RITIS Website

Proper decision-making during an incident depends on a person's ability to understand all the data gathered by sensors, cameras, phone calls, and dispatch information. Existing systems have failed to make this task easy. Managers must analyze pages of text, tables, and maps to understand what is being done to manage an incident. This can be time-consuming, and the consequences of misinterpreting information can be life-threatening. The RITIS website was designed with these challenges in mind and has created an impressive suite of interactive visualizations that make situational awareness and data interpretation quick and easy. Users can interact with live events, incidents, weather, sensors, and other data sources and devices in maps, lists, graphics, and even a four-dimensional animated virtual helicopter. Users can apply a rich set of filters, access contact information, and communicate with other users. An example of one such visual is the Incident Timeline (click here to view an example). This interactive graphic shows who is at an accident scene, who has been notified, or who has departed. It also includes real-time and historical lane status and traffic queue buildups, closed-circuit TV camera feeds, dynamic-message-sign deployments, and even communication logs between managers. More screenshots of the RITIS components and visualizations can be found at http://tinyurl.com/ritis.

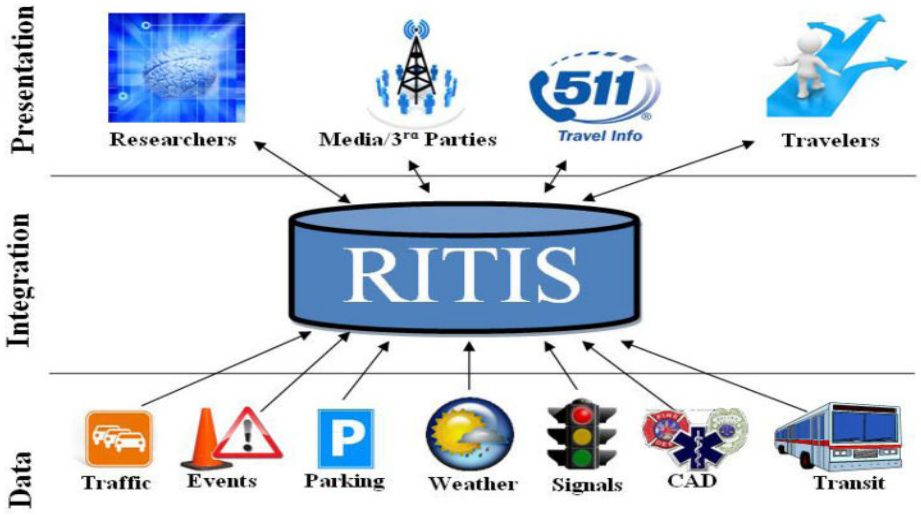


Figure 1: Overview of the RITIS data, integration, and presentation layers.

The RITIS Archive

All data within RITIS is archived indefinitely. A number of on-line tools have been developed to allow

(Continued on Page 13)

Transportation Systems *(Cont. from 12)*

users to query, analyze, and derive performance measures from the RITIS archive. Many of these tools are highly interactive and dynamic. They have been developed with the user in mind and afford a high degree of freedom to explore the data with minimal training needed. Data within the archive can also be downloaded and/or exported so that users can perform their own, independent analysis. These tools can allow users to identify accident hot-spots, analyze queue lengths and traffic congestion/bottlenecks at specific areas, and evaluate the effectiveness of transportation operations strategies. An example of one such tool is seen in Figure 2; however, more examples and limited live demos of select RITIS tools and performance measures can be seen at the following link: http://www.cattlab.umd.edu/demo.

The Virginia Department of Transportation, the Maryland Department of Transportation, the District Department of Transportation, and the Washington Metropolitan Area Transit Authority have entered into a formal partnership now known as the Metropolitan Area Transportation Operations Coordination (MATOC) Program. The mission is to provide situational awareness of transportation operations in the National Capital Region through the communication of consistent and reliable information that allows operating agencies and the traveling public to make effective and timely decisions. RITIS is one tool by which MATOC endeavors to achieve this mission. In addition to these four original participating agencies, other agencies in the region regularly use the RITIS website and tools. These other agencies range from researchers and planners at universities and metropolitan planning organizations to police departments to Federal agencies, including the Federal Emergency Management Agency, the National Security Agency, the Transportation Security Administration, DHS, the military, and even private sector traveler information providers.

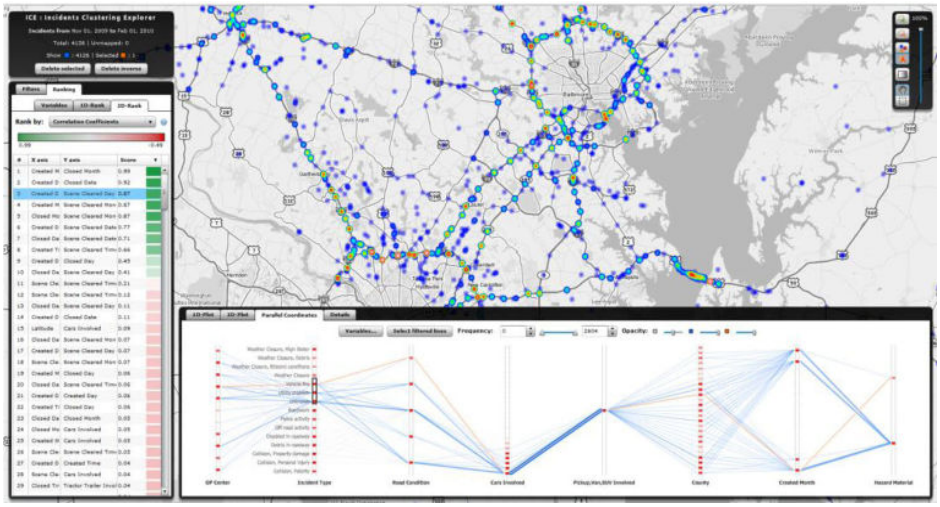


Figure 2: The incident clustering explorer lets analysts explore incident hotspots and trends.

Advancing National Capabilities

A number of other States and agencies have become aware of the RITIS platform and have requested participation. The State of Maryland is considering leading a Federal Pooled Fund Study that will enhance many of the existing features of RITIS, add new functionality, but most importantly allow for geographic expansion of RITIS from a regional system to a National Integrated Transportation Information System (NITIS). NITIS would provide significant social and economic benefits to the Nation from day one; however, the future benefits resulting from new discoveries, safety enhancements, or other key programming decisions that will be made based on the ease of access to this new wealth of information at one's fingertips are seemingly endless.

As has been seen with other agencies already involved in the RITIS program, one consolidated location for transportation systems data, information gathering, etc., allows the agencies to better report on their achievements to decision makers and the public. It places a spotlight on transportation operations, Intelligent Transportation Systems, transportation data collection efforts, and ultimately helps to garner support and much needed funding for programs.

The new avenues of research that such a system would open up to university researchers, city, State,

(Continued on Page 24)

CIA: A Leader in Information Sharing

by Geoffrey Fowler*

An oxymoron you say? A bad joke perhaps? Think again. Say it again. CIA is a leader in information sharing. Read on to find how one of America's most secretive agencies, whose raison d'être is to acquire and maintain secrets, has transformed itself into a leader in information sharing.

Let's start by rolling back the clock.

In 2006, CIA's then Director for Intelligence (the Director, or DI, heads CIA's analytic effort) turned to one of his executive assistants and said, "The SEIB is broken, go fix it." The SEIB, short for Senior Executive Intelligence Brief, was CIA's daily printed intelligence journal provided to senior customers — a partner journal of sorts to the President's Daily Brief (PDB), which was reserved for the President and a handful of his most senior cabinet members and staff. The PDB had recently been placed under the auspices of the new Director of National Intelligence (DNI) as part of the reorganization of the Intelligence Community (IC). The DI also noted that CIA needed to enhance its analytic credibility with its customers, to focus on what it means to be central to their needs, to pioneer during a time of significant change in the community, and to reaffirm one of its core reasons for existence — informing national security decision-making. In short, he provided direction to share intelligence more effectively with those who needed it.

First one, then two, and then a small group of CIA officers were set to the task of fulfilling the DI's direction. They looked at the current publication, its process, how intelligence reached customers, and how those customers consumed information. They tinkered on the margins for a bit to see if small changes would address the issue. And then, realizing that the problem was as much cultural and institutional as it was anything else, they did a remarkable thing — they put the past aside and started again by adopting a visionary approach to providing intelligence more akin to leading private sector technology companies and news organizations than traditional intelligence organizations.

In just a few months, they proposed to the DI a content management initiative that called for the replacement of the SEIB and the launching of a new effort — the World Intelligence Review (or WIRe). The WIRe vision was a significant departure from the tired structures that inhibited presenting the best of CIA's intelligence — bending to the breaking point well meant, but constraining rules on form and structure and approach that had inhibited analysts' ability to convey important intelligence stories. The initiative called for embracing dynamic online conveyance of intelligence rivaling private sector news organizations. Central too was the notion that robust metrics on customer use and data driven decision-making were needed for good program management (a "no duh" concept to be sure, but often enough lacking in government and thus important in its establishment as a core WIRe principle). And, finally, they proposed that the social concepts and tools embodied in "web 2.0" craze be embraced.

Given the go-ahead, the team retired the SEIB and launched the WIRe in hardcopy, thus joining the 60-year history of CIA daily intelligence publications. With the WIRe, they adopted new concepts for intelligence, noting in its inaugural edition the WIRe's departure from the traditional "current intelligence" model, eschewing the chasing of news, and instead committing to customers that the journal would provide "intelligence with currency;" that is to say, current value to the reader drawing insights from the richness of CIA's experts, its research efforts, and its daily production cycle. It was a breath of fresh air.

But they did something else as well. By leveraging existing technology

(Continued on Page 15)

CIA *(Cont. from 14)*

developed in part as a result of CIA's In-Q-Tel effort (a sort of venture capital activity promoting technology development helpful to intelligence) they also deployed an online prototype of the WIRe for agency-wide internal beta testing. They asked the most critical and discerning of people — the Agency's own officers — to critique the program and to offer ideas. This was fitting, they reasoned, as the WIRe was to be CIA's presence online. It was effective too, as involving everyone helped create the buy-in and cultural transformation needed for success. Over the next few months this web-based means for disseminating intelligence was refined and less than a year from the DI's original direction, it was deployed to Intelligence Community, military, and policy customers; it was an immediate hit with all.

In its first 100 days, the WIRe "went gold" — surpassing by three fold the daily number of users an earlier effort CIA had deployed for accessing intelligence online. Taking notice of its success and cutting edge nature, the then Director of CIA called for the WIRe's expansion to more broadly incorporate CIA's disseminated intelligence — including analysis, open source reporting, and raw intelligence. Through a series of what in the business world would be termed "mergers and acquisitions," the WIRe first absorbed several other efforts and then, utilizing an agile technical development approach, quickly became CIA's corporate face for online intelligence; an expansion in scope that was completed in less than a year. Now just four years from its birth, the WIRe is providing intelligence to the secure online community across the globe — an orders of magnitude expansion in information sharing aiding the decision-making of the Nation's leaders, intelligence professionals, and war fighters. And it continues to grow.

Rounding out this dramatic expansion in availability are a series of other important information sharing breakthroughs:

• **Squaring the Circle on Information Sharing and Information Security.** The truth of the intelligence business is that information sharing and information security need to coexist. Share too broadly and people can die. Hold your information too closely, decisions can be ill-informed and people can die. With WIRe, CIA developed a robust system that enabled both broad and secure dissemination of information — an approach that is now at the heart of like efforts elsewhere in the community.

• **Solving the "You Don't Know What You Don't Know" Problem.** This familiar issue which has dogged everyone at some point — how do I find something that is relevant to me if I do not know it exists — is particularly challenging in a world where securing information is also important. With WIRe, CIA developed a means for providing insight into the existence of its disseminated intelligence. Now WIRe users can discover the existence of content on a topic, even if their access to the material itself is restricted because of classification, for example, and readers are told what they need to do to access the information.

• **Establishing a Framework of Intelligence Relationships.** A truism in information sharing and support to decision-making is that information is best presented in context of related information. This simple but powerful principle is at the heart of a good briefing, sound analysis, and the linking of knowledge on the web. CIA leverages this principle in WIRe with robust linking of analysis to related analysis, citations, references, and commentary. Links are bi-directional as well, making it easy to navigate among related content.

• **Embracing New Ways of Conveying Intelligence.** While paper has a unique and enduring role in the creation and sharing of intelligence, by changing its focus and directing emphasis to online dissemination, CIA was able to leverage the new medium to present intelligence in richer and more integrated ways. WIRe content regularly includes video and interactive multimedia allowing users to access and assess information across a range of senses.

• **Leveraging Collaboration.** In recent years, the social web has brought the private sector a variety of capabilities; CIA has embraced many of these concepts bringing the best of the web to WIRe's online

(Continued on Page 22)

Legal Insights

Post-9/11 National Security Information Law

by Reza Mahmoodshahi, Law Intern

The agencies responsible for intelligence collection and dissemination have been reorganized as a result of the September 11 attacks. In 2004, based upon the recommendations of the 9/11 Commission, Congress passed and the President signed the Intelligence Reform and Terrorism Prevention Act, which calls for the creation of an Information Sharing Environment (ISE). The ISE is a partnership between all levels of government, the private sector, and foreign partners in an effort to combat the threat of terrorism through the "effective and efficient sharing of terrorism and homeland security information."[1]

While the lawful sharing of collected information regarding terrorism and other criminal activity is a legitimate government need, increasing government authority to collect and disseminate personal information about Americans poses risks to individual privacy and civil liberties. Moreover, as ISE is being used to expand information sharing *with the government*, the government is concurrently suppressing information sharing *with the public*.[2] These developments highlight the importance of information in national security strategy, but also raise government transparency concerns.

In what follows, I discuss some of the most significant post-9/11 cases in national security information law. These include not only constitutional and statutory challenges, but also Freedom of Information Act (FOIA) lawsuits to publicize government-controlled information. In the post-9/11 national security environment, the openness-inducing scope of FOIA — the first federal statute to establish a right of public access to executive branch information — has been narrowed by congressional amendments to broaden the class of national security disclosure exemptions.

In *Center for National Security Studies v. U.S. Department of Justice*, the D.C. Circuit upheld, in a 2-1 vote, the Department of Justice's (DOJ) categorical denial of FOIA requests for the names and circumstances of arrest for hundreds of individuals detained in the immediate aftermath of the 9/11 attacks.[3] The Supreme Court dismissed an appeal challenging the secrecy surrounding these arrests, letting stand the majority's holding that "the judiciary owes some measure of *deference* to the executive in cases implicating national security (emphasis mine)." The dissenting judge said the majority had "converted deference into acquiescence" by accepting a categorical secrecy policy.

In a separate case affecting many of the same detainees, *North Jersey Media Group v. Ashcoft*, Chief U.S. Immigration Judge Michael Creppy issued a memo closing the deportation hearings of "special interest" detainees to the press and the public. As a result of the "Creppy Memo," despite a long-standing history of openness, the months after 9/11 were witness to hundreds of secret deportation hearings involving individuals who had not yet been cleared of

(Continued on Page 17)

[1] Implementation Plan for the Information Sharing Environment (Nov., 2006), available at http://www.ise.gov/docs/reports/ise-impplan-200611.pdf.

[2] The government is increasingly invoking so-called "mosaic concerns" to justify withholding information from the public. This is the idea that two individually innocuous and seemingly unrelated pieces of information can be combined to yield new information that is potentially threatening to national security interests.

[3] 331 F. 3d 918 (D.C. Cir. 2003).

Legal Insights *(Cont. from 16)*

connections to terrorism by the FBI. A consortium of New Jersey newspapers challenged the policy of blanket closings, and the District Court in Newark issued an injunction in 2002 against the policy, ruling that blanket closing of hearings, without individualized determinations that national security interests warrant the closing of a particular hearing, violate the First Amendment right of free speech.[4] The Supreme Court granted a stay of that ruling, and eventually the Third Circuit overturned the District Court's decision holding that newspapers did not have a First Amendment right of access to deportation hearings when those hearings were determined by the Attorney General to present national security concerns.[5]

The conflict between the government's desire for secrecy in the interest of national security and the public's desire for information to evaluate the activities of the executive branch is not unique to the foregoing pair of cases. In particular, the government's new authorities to conduct secret domestic surveillance under the USA PATRIOT Act have also come with a host of new legal challenges.[6]

In the case of *Doe v. Holder*, an anonymous Internet Service Provider (ISP) challenged the FBI's authority to issue National Security Letters (NSLs), essentially an administrative subpoena, to businesses without judicial review. Under the USA PATRIOT Act, the FBI can use NSLs to demand personal customer records from ISPs, financial institutions, and credit companies without prior court approval or probable cause. The NSLs also contained so-called "gag" provisions, permanent non-disclosure orders prohibiting the recipients from ever revealing to any third party that he has been served with an NSL. In 2008, because it imposed a nondisclosure requirement on NSL recipients without any form of judicial oversight, the Second Circuit found the NSL "gag" provision in violation of the First Amendment.[7]

The mere act of disseminating information can also implicate an individual's First Amendment rights if the information is collected and disseminated by an agency participating in the ISE without a legitimate law enforcement or national security purpose. In 2008, the American Civil Liberties Union (ACLU) obtained documents — through a Maryland Public Information Act (MPIA) and FOIA lawsuit — that revealed that the Maryland State Police engaged in covert surveillance of Baltimore peace and anti-death penalty groups.[8] The information obtained through the FOIA lawsuit revealed that for over a year, without any indication of unlawful activity, agents from the Maryland State Police's Homeland Security and Intelligence Division continued surveillance on the groups' lawful activities, shared their reports with at least seven Federal, State, and local law enforcement agencies, labeled many of the peaceful activists "terrorists," and uploaded the activists' personal information into certain ISE databases.

In *ACLU et al. v. National Security Agency (NSA)*, the ACLU sued the NSA in District Court claiming that the NSA's Terrorism Surveillance Program (TSP), designed to intercept the international telephone and internet communications of persons in the United States without warrants, was unconstitutional and in violation of the Foreign Intelligence Surveillance Act (FISA). The District Court granted summary judgment to the plaintiffs upon finding that the TSP violated FISA and "undisputedly violated the Fourth [Amendment] in failing to procure judicial orders."[9] The Sixth Circuit stayed the decision in 2006 on appeal, because the plaintiffs lacked standing to bring suit.

(Continued on Page 21)

[4] 205 F.Supp.2d 288 (2002).
[5] 308 F.3d 198 (2002).
[6] RECLAIMING PATRIOTISM. A Call to Reconsider the Patriot Act (Mar., 2009), available at http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf.
[7] 549 F.3d 861 (2008).
[8] ACLU-MD's original FOIA and MPIA requests, available at http://www.aclu-md.org/aPress/Press%202006/082906_FOIA.html.
[9] 438 F. Supp. 2d 754 (Dist Court, ED Michigan. 2006).

The Drug Enforcement Administration and James Madison University: Partnering for a Brighter Future

by Sami Nuristani*
Graduate Fellow, Institute for Infrastructure and Information Assurance, James Madison University

January 27, 2010 marked the beginning of an exciting partnership between James Madison University (JMU) and the U.S. Intelligence Community. Anthony Placido, Assistant Administrator and Chief of Intelligence at the Drug Enforcement Administration (DEA), and Dr. Sharon Lovell, Interim Dean of JMU's College of Integrated Science and Technology, signed a Cooperative Agreement between the two institutions. The Agreement includes two major elements: 1) the establishment of an Intelligence Analyst intern program at DEA, specifically for students enrolled in the Information Analysis program at JMU, and 2) mutual support for analytic education and training between the two organizations. The Information Analysis major is designed for students seeking critical thinking, geo-political, and technological skills to further the capabilities of the U.S. Intelligence Community. Students chosen to participate in the intern program will spend two consecutive summer semesters at DEA to fulfill the program requirements.

DEA is scheduled to receive the first cohort of students in the summer of 2010. The intern assignments will include rotations at both a DEA field office and at DEA Headquarters in Arlington, VA. Between the first and second summers, the interns will be processed for Top Secret clearances, and upon graduation, will be well-positioned to gain full-time employment at DEA. The benefit of two summers' worth of work experience prior to a potential job offer is an opportunity not common in many degree programs.

The Institute for National Security Analysis (INSA) at JMU played a major role in bringing the internship program to fruition. INSA is the research arm of the Information Analysis major, providing direction in both the content and pedagogy of the degree program. Throughout the past three years, INSA has recruited students to conduct complex research assignments pertaining to intelligence analysis, and in some cases, provided a platform for the students to present their research findings to an audience comprised of professionals from the Intelligence Community. ❖

**Sami Nuristani will complete his Master of Public Administration degree in May of 2011.*

(Front row, left to right) Assistant Administrator and Chief of Intelligence Anthony Placido and Dr. Sharon Lovell, Interim Dean of James Madison University's College of Integrated; Science and Technology (back row, left to right) Jonah Goobic, DEA Intelligence Analyst and JMU alumnus; Doug Poole, Deputy Chief of Intelligence, Office of National Security Intelligence; Judith Bertini, Deputy Chief of Intelligence; Mr. Raymond Pagliarini, Chief of Human Resources; Dr. Joe Marchal, JMU Faculty; Dr. Noel Hendrickson, Director, JMU Institute for National Security Analysis; Ms. Amy Ballard, Operations Coordinator, JMU Institute for National Security Analysis; and DEA Special Agent K. Erik Ellenes, JMU Alumnus.

Update on the Attempted Christmas Day Bombing

by Hasan Aijaz, Law Intern

On December 25, 2009 Umar Farouk Abdulmutallab boarded a plane bound for Detroit, Michigan, despite his father's warnings to a U.S. embassy that his son may be associated with Yemeni Al-Qaeda.[1] While Abdulmutallab failed in his attempt to blow up the airliner and no one was harmed, the incident demonstrated that information sharing is necessary to effectively utilize information that has already been gathered. The U.S. government responded to this event with Congressional hearings to understand how this event happened with the hope that this type of event can be prevented from occurring again.

Immediately after the attempted bombing, the Transportation Security Administration (TSA) issued a directive implementing additional security measures for U.S. flights originating abroad. The measures included: (1) a pat down of all passengers at the boarding gate; (2) prohibiting passengers from getting out of their seat in the last hour of the flight; (3) prohibiting passengers from having anything on their lap, including blankets or pillows, during the last hour of the flight; (4) prohibiting flight crews from making announcements on flight paths or land sights when flying over the United States; and (5) requiring individuals from 14 countries considered high risk to undergo enhanced screening.[2,3] On April 2, 2010 a new directive was implemented. Although the details of the plan have been kept classified, the press release mentioned that passengers may "notice enhanced measures including the increased use of the technology and processes such as explosives trace detection, canine teams, advanced imaging technology, and behavior detection among other measures."[4] Also of significance is that these measures will apply to flights originating from all countries and supersedes the prior directive which required enhanced screening for people from the 14 high risk countries.

While TSA's response was the most immediate and widely felt by the flying public, other government bodies also quickly moved into action. On March 24, 2010 Patrick Kennedy, Under Secretary of State for Management at the Department of State (DOS), testified before Congress that the DOS was "incorporating new technology, increasing data sharing and enhancing operational cooperation with partner agencies."[5] In order to prevent the specific mistake that contributed to the oversight that allowed Abdulmuttalib to board the December flight, the Visas Viper cable reporting system, which did not flag Abdulmuttalib due to a misspelling of his name, will operate on a "fuzzy search" paradigm which will identify visa records despite variations in the spelling of names. Beyond this, the DOS is "implementing a new generation of visa processing systems that will further integrate information gathered from domestic and overseas activities."[6] He noted that the unprecedented scale of information requires a new approach to collecting, filtering, and delivering that information.

In 2003, the Terrorist Screening Center (TSC) was established to organize the dozen watch-lists that various governmental organizations maintained. The TSC, under the auspices of the FBI, maintains the Terrorist Screening Database (TSDB), which is the primary terrorist screening watch-list. Individuals are "nominated' to the list by governmental agencies that provide information to either the FBI or the National Counterterrorism Center (NCTC). After a vetting process, these individuals are then added to the

(Continued on Page 23)

[1] http://blog.dhs.gov/2010/01/morning-roundup-january-8th.html.
[2] http://www.tsa.gov/press/happenings/010310_statement.shtm.
[3] http://www.elliott.org/blog/full-text-of-sd-1544-09-06-authorizing-pat-downs-physical-inspection/.
[4] http://www.tsa.gov/travelers/airtravel/guidance_international_flights.shtm.
[5] Patrick Kennedy House of Representatives Committee on the Judiciary, Hearing on Sharing and Analyzing Information to Prevent Terrorism (March 24, 2010).
[6] Ibid.

June 17, 2010

Achieving Enterprise Resilience: The Convergence of Government and Private Sector Risk Management Interests Across the Homeland Security Enterprise

One-Day Conference

at

George Mason University's Arlington Campus Original Building, Room 329 3401 Fairfax Drive Arlington, VA 22201

For more information, click here. To register, click here.

Co-hosted by:

GEORGE MASON UNIVERSITY Center for Infrastructure Protection and Homeland Security

SARMA Security Analysis and Risk Management Association

NECP *(Cont. from 3)*

our efforts on advanced planning, partnerships, and training and exercises.

Despite a greater focus on emerging technology in the updated NECP, OEC will continue to focus on assisting State and local agencies in their efforts to improve their communications infrastructure, governance, and planning capabilities. The Office will also continue to strengthen its partnerships with Federal, State, and local agencies through grants, training, and technical assistance. The needs of our stakeholders remain our priority and we continue to seek feedback and guidance from the emergency response community to meet challenges of interoperable emergency communications. ❖

Chris Essid is the Director of the Department of Homeland Security's Office of Emergency Communications. He can be reached at OEC@hq.dhs.gov. For more on OEC, visit www.dhs.gov keyword OEC. The National Emergency Communications Plan is available at http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf.

Legal Insights *(Cont. from 17)*

Although the plaintiffs claimed a "well-founded belief" that they were targeted by the TSP due to a history of communications with the Middle East, the court found that "the plaintiffs do not — and because of the State Secrets Doctrine cannot — produce any evidence that any of their own communications have ever been intercepted by the NSA, under the TSP, or without warrants."[10]

Despite increasing denials of FOIA and pre-trial discovery requests for information, with the establishment of 72 Fusion Centers, local centers that conduct "information-sharing, collection, and analysis," by DHS around the country, public access to information may yet be further bottle-necked by new non-federal restrictions intended to safeguard information funneled through these State and regional Fusion Centers.

A recent example of FOIA litigation, *Electronic Privacy Information Center (EPIC) v. the Virginia Department of State Police, et al.*, involves a Virginia FOIA request to the Virginia State Police for public records related to alleged federal involvement with HB 1007, a bill that would exempt the Virginia Fusion Center from Virginia privacy and transparency laws.[11] The information requested in the EPIC FOIA lawsuit is wanted in order to determine whether DOJ or DHS participated in the development of HB 1007. Generally, the participation of agencies from multiple jurisdictions, the private sector, the military, and the considerable secrecy of the activities of some Fusion Centers have raised public oversight and privacy protection concerns, as well as a critique of the legal framework governing their activities.

The issue underlying each of these cases is the correct balance between strategically important national security information and the threat of potentially abusive government intelligence activities. However, this is not to say that security and liberty are inherently at odds with one another. The two can and, indeed, *should* support one another. As the 9/11 Commission put it, "the choice between security and liberty is a false choice, as nothing is more likely to endanger Americans' liberty than the success of a terrorist attack at home…Yet if our liberties are curtailed, we lose the values we are struggling to defend."[12] ❖

---

[10] 493 F. 3d 644 (6th Cir. 2007).
[11] Case No. 08-01357 (Va. Gen. Dist. Ct. 2008).
[12] The 9/11 Commission Report, available at http://www.9-11commission.gov/report/911Report.pdf.

CIA *(Cont. from 15)*

customers. Tagging and social bookmarking are a central part of WIRe, as are RSS feeds and, with a recent deployment, unique user personalization — think an amalgam of CNN.COM and Google News/Reader. Users are also able to openly comment on articles — making the WIRe not just a means for conveying intelligence, but also for promoting discussion and connecting readers with like interests.

Working collaboratively with IC partners has been a central theme for CIA more broadly and some of WIRe's greatest successes have helped ease the way for similar efforts elsewhere in the community. In recognition, the DNI in 2009 awarded WIRe the National Intelligence Reform Medal — a high honor indeed — specifically citing its "extraordinary accomplishment for pioneering online presentations and integration of intelligence, breaking new ground in customer service, and overcoming long standing information sharing challenges."

Praise from other customers has been robust as well, but for this author, one of the most meaningful comments was provided by a CIA officer who noted, "[o]pening the WIRe this morning I was yet again struck with its layout, 'look', use of graphics, varied content, and authoritative tone. It gives me renewed pride in working at CIA. Thank you for all you and your team have done to make this happen."

If one of the most secretive institutions in the world can lead in information sharing, there is hope for everyone. ❖

** The author, Geoffrey Fowler, was the DI's Executive Assistant and is the Director and Managing Editor of CIA's World Intelligence Review (WIRe).*

Virtual Reorganization *(Cont. from 5)*

increased technological capabilities to collect, store and analyze information: Such policies are necessary both for the American people to have confidence in their government and to empower the participants in the information sharing framework so they have confidence that their work is lawful and appropriate.

Leadership

President Obama and Congress have made clear the urgency and importance of this effort. Strong, sustained leadership is required, which connects "authority" with "responsibility." In addition to the DNI and even the new Special Assistant to the President, it is also imperative that there be an official within the White House with adequate horsepower — and budgetary authority — to drive interagency coordination at a senior level. Further, as part of their daily briefing for the President, his top national security and intelligence advisors must stress at every opportunity that the information they are presenting is only as good as the information sharing and analysis that supports it. The President's closest advisors must be held accountable for improving the knowledge we derive from information sharing across the government.

Congress must continue to explore these issues and exercise fully and appropriately its oversight responsibilities, providing adequate funding and developing appropriate methods for measuring progress, considering even greater use of investigative staff or the Government Accountability Office.

State and local governments also have a responsibility to improve information sharing by developing appropriate ways to measure progress, coordinated regional training and deployment exercises, standardized mechanisms for information sharing in coordination with executive branch offices, and unified, top-to-bottom mechanisms for authorized use of information, unifying dispute resolution mechanisms across agencies. ❖

Update *(Cont. from 19)*

TSDB by either the NCTC or the FBI. The TSC then shares this information "downstream" by sending data to other screening systems such as the DOS's Consular Lookout and Support System (CLASS) and TSA's No Fly List and Selectee list.

Although Abdulmuttalib's name was in the Terrorist Identity Datamart Environment (TIDE), the NCTC's list, his name was not passed into the TSDB because of the threshold required for inclusion. An individual will be named in the TSDB if the available information creates a "reasonable suspicion" that they pose a threat to national security. Abdulmuttalib was included in TIDE based primarily on information received by the U.S. Embassy in Nigeria, which comprised of only one sentence of "derogatory information" regarding his possible relationship with Yemeni-based extremists. According to the procedures in place at the time, this information was insufficient for inclusion in the TSDB and therefore also insufficient for inclusion on the No Fly list or Selectee list. Although the information available in TIDE was insufficient for inclusion in the TSDB, additional information on Abdulmuttalib was contained in daily intelligence holdings which would have been sufficient, when combined with the information in TIDE, to support his inclusion in the TSDB and possibly on the No Fly List. On March 10, 2010 Mr. Russell Travers, the Deputy Director for Information Sharing and Knowledge Development, testified to Congress that the information "existed largely 'in the noise' and there was nothing particularly alerting about either 'dot.'"[7] As a result, Mr. Travers testified that "the U.S. Government needs to improve its overall ability to piece together partial, fragmentary information from multiple collectors."[8] In response, the TSC convened its policy board, which is comprised of various intelligence organizations, in order to determine if a review of procedures but to date no normal changes to procedure have been announced.

According to a U.S. Government Accountability Office report analyzing the attempted attack, if Abdulmuttalib's name had been included in the TSDB, there are three separate ways in which he could have been prevented from boarding a U.S. bound flight:

1) The DOS is linked to the TSDB and may have revoked Abdulmuttalib's visa if they had access to the information.
2) Customs and Bereau Protections is also linked to the TSDB and they could have intercepted him prior to boarding had he been on the list.
3) Abdulmuttalib may also have been placed on the No Fly list which would have prevented him from boarding the flight.[9]

Thus, while the TSDB can create multiple checkpoints which can prevent a terrorist attack, if it is not utilized, none of the agencies responsible for protecting our borders will have the necessary information to complete their mission. Effective and appropriate information sharing is therefore absolutely vital to our national security and must be pursued despite existing challenges. ❖

Editor's Note: During the publication of this issue, information was released about an attempted car bombing in New York on May 1. At present, it appears that the suspect, Faisal Shahzad, was permitted to board a U.S. flight bound for Pakistan on May 3. While officials located Shahzad minutes prior to take-off, according to FBI Deputy Director John S. Pistole, Shahzad was placed on the no-fly list around noon on May 3, hours before he boarded the plane. Information about this incident is still forthcoming. As additional information is released, comparisons between this incident and the attempted bombing in December 2009 are inevitable. This is an opportunity for the administration to apply lessons learned from the December attempted bombing to the May attempted bombing.

---

[7] Russel Travers, House of Representatives Committee on the Judiciary, Hearing on Sharing and Analyzing Information to Prevent Terrorism (March 10, 2010).
[8] Ibid.
[9] U.S. Government Accountability Office, Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security, (Washington DC: January 27, 2010).

Transportation Systems *(Cont. from 13)*

and national DOT partners are unfathomable. Questions previously unanswerable would be asked and addressed. Time and funding previously used for tedious data collection, consolidating, and fusing would be freed up to better solve problems and maintain a higher level of real-time situational awareness. Performance measures generation at the local and State levels would be significantly easier and in many cases, completely automated. The cost advantages, or economies of scale, that the Nation will obtain due to expansion to NITIS are enormous. Individual agencies are spending millions in data archiving and data sharing/integration initiatives that are stove-piped and often inadequate to meet more than a few specific local needs. Leveraging on existing technologies, tools, and knowledge acquired through the development of the original RITIS program will ultimately reap significant cost savings to State and local agencies while simultaneously significantly increasing capabilities. ❖

To learn more about RITIS, please contact Michael L. Pack, Director of the University of Maryland Center for Advanced Transportation Technology Laboratory at 301-405-0722 or PackML@umd.edu or visit www.cattlab.umd.edu.

Post 9/11 Environment*(Cont. from 10)*

* *Kevin McCrohan was ordered to active duty with the U.S. Army following the September 11, 2001 attacks and was assigned to the U.S. National Infrastructure Protection Center, Federal Bureau of Investigation, and then with the Department of Homeland Security where he was responsible for information sharing initiatives with the financial sector. He returned to GMU in fall 2003 as a Professor of Marketing.*

Lessons Learned *(Cont. from 6)*

could be sent to the bureaucratic equivalent of Siberia, demoted, or fired.

Next, reformers could insist on new employee performance metrics. Intelligence officials could be evaluated in part based on their citation count — the extent to which others rely on their reports in their own work. Tying career prospects to citations would create powerful incentives to share; other analysts cannot cite your work if they do not know it exists.

Policymakers also should pay attention to the incentives at the agency-wide level. In particular, they could craft compensation mechanisms by which sharing agencies could internalize some of the financial and other benefits that accrue to recipients. That way data exchange would not hurt their bottom lines.

As the war on terror approaches its second decade, solid intelligence will continue to be our first line of defense against Al-Qaeda — and intelligence failures will continue to be our Achilles' heel. Until policymakers recalibrate the incentives within the intelligence community, the need for better information sharing may be a lesson we are condemned to learn over and over again. ❖

**Nathan A. Sales is a Law Professor at George Mason University. He served in the George W. Bush administration at the Justice Department and as Deputy Assistant Secretary of Homeland Security for Policy.*

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1