July 2004
Volume 52
Number 4

United States
Department of Justice
Executive Office for
United States Attorneys
Office of Legal Education
Washington, DC
20535

Mary Beth Buchanan
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bi-monthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201. Periodical postage paid at Washington, D.C. Postmaster: Send address changes to Editor, United States Attorneys' Bulletin, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Technical Editor
Nancy Bowman

Law Clerk
Carolyn Perozzi

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201.

First Responders

In This Issue

Focus on First Responders

Stan Harris
First Assistant U.S. Attorney and Antiterrorism Advisory Council Coordinator
United States Attorney's Office
Southern District of Mississippi

I. Introduction

In October 2001 the Attorney General directed the district offices to form Anti-Terrorism Task Forces, now known as Anti-Terrorism Advisory Councils or ATACs. Building on the well-established training programs of the Law Enforcement Coordinating Committees (LECCs), and staffed with a new Intelligence Research Specialist (IRS) in each federal judicial district, ATACs are designed to promote better information sharing among federal, state, and local agencies and to help prevent future terrorist attacks.

In addition to the Executive Office of the President and the federal court system, the U.S. Attorney's Office (USAO) is the primary outlet for federal agencies to combine efforts to prosecute criminal cases and assist in federal civil cases. ATACs ensure that an official appointed by the President, and confirmed by the U.S. Senate, directly oversees day-to-day counterterrorism efforts in each judicial district throughout the United States and its territories. Each federal judicial district is staffed with an IRS, who works closely with Joint Terrorism Task Forces (JTTFs), led by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS).

ATACs have become a major component in the information sharing effort, specifically reaching out to the broader first responder community for a more holistic approach to prevention. ATACs, together with JTTFs and the DHS, work each day to foster better cooperation and coordination between traditional law enforcement and other members of the first responder community.

This issue of the *USA Bulletin* focuses on information-sharing and outreach efforts to the first responder community. Traditionally, first responders are made up of the following personnel:

- law enforcement agencies;
- fire fighters and emergency medical teams;
- public health, hospitals, and emergency management agencies;
- hazardous material (haz-mat) teams;
- 911 operators;
- military security and force protection experts; and
- security professionals for private infrastructure facilities.

II. Contents of this issue

In this issue, you will find:

- An article by Assistant U.S. Attorney Tom Taylor, who is presently assigned to the Executive Office for U.S. Attorneys as the IRS program coordinator, giving an overview of the new IRS program.
- An article by Dr. Mary Victoria Pyne, Communications Unit Chief for the FBI Criminal Justice Information Services Division, explaining the new relationship between the two Department of Justice (Department) funded systems of Law Enforcement Online (LEO) and the Regional Information Sharing System (RISS™).
- Another FBI-sponsored information network is discussed in an article about InfraGard, a program that provides access to sensitive information for private sector security professionals in an effort to protect the Nation's critical, privately held infrastructure. The controlled inclusion of private security professionals in the information-sharing arena is one of the most significant post 9/11 changes, and is designed to enhance information sharing and terrorism prevention. To become part of the network, InfraGard companies must fill out and submit a security questionnaire to facilitate a basic background check.
- An article on RISS addresses the new Anti-Terrorism Information Exchange (ATIX) program, which is designed to include a broad spectrum of first responder agencies.

- Other Department programs that address the interoperability of first responder communications are outlined in an article reprinted from Tech Beat about the AGILE program. This program has brought a coalition of experts together to address this critical issue.
- First Assistant U.S. Attorney for the Eastern District of Wisconsin and ATAC Coordinator Francis Schmitz writes about training first responders to work together. This article highlights the Forensic Epidemiology course curriculum that is available for use by any ATAC. This course is designed to train law enforcement and health and medical officials on investigative responses to bioterrorism. The field delivery course is a partnership between the Department and the Centers for Disease Control, U.S. Attorney Offices in the Northern District of Georgia, the Eastern District of North Carolina, and numerous federal, state, and local agencies in Maryland, North Carolina, Georgia, Florida, California, and Oregon.
- Training first responders to work together to prevent terrorism is the focus of the article, PATRIOT Counter-Terrorism Training Program, which was written by U.S. Attorney Jim Greenlee, LECC/ATAC Chief Information Officer David Crews (N.D. Miss.), Antiterrorism Coordinator Tom Bartlett for the southern Regional Public Safety Institute, and Intelligence Research Specialist Max Fenn (S.D. Miss.). The Preventive Anti-Terrorism Recognition & Interdiction Operational Techniques (PATRIOT) program is a collaborative effort led by the two Mississippi District ATACs. They used federal, state, and local officials to provide premium quality field training to first responders.
- Tom Bartlett, the Antiterrorism Coordinator for the Southern Regional Public Safety Institute, assisted Bob Arndt, Port Security Specialist for the Coast Guard Marine Safety Office in Mobile, Alabama in preparing an article on the IMPACT field training program. IMPACT (Intensive Marine Port Area Counter Terrorism) is a prevention program led by the Coast Guard's Regional Port Security Committee, and the ATACs of the Northern and Southern Districts of Mississippi, the Southern District of Alabama, and the Northern District of Florida. Like the PATRIOT Program, IMPACT uses federal, state, and local officials to provide field training to a diverse first responder audience. IMPACT places special emphasis on port security issues and features on-site port tours.
- Specialized Department counterterrorism training for law enforcement first responders is presented in an article on the Bureau of Justice Assistance State and Local Anti-Terrorism Training (SLATT) Program. Domingo S. Herraiz, Director of the Bureau of Justice Assistance, discusses both in-residence and field training programs which are provided by SLATT to federal, state, and local law enforcement officials.
- An article on the Cocoanut Grove Night Club Fire provides a specific example of first responder involvement in a real-world situation. Written by Beverly Ann Jones, Executive Office for United States Attorneys, Employee Assistance Program (EAP), the article highlights the situations and solutions that first responders encountered in the first documented major accident requiring the cooperation of all first responders.
- An article which identifies and answers some of the American Library Association's questions concerning the USA PATRIOT Act, written by Assistant U.S. Attorney Gaines Cleveland of the Southern District of Mississippi, provides insight into the PATRIOT Act and how libraries are addressing issues of information sharing and terrorist prevention. In so doing, Cleveland clears up several misconceptions concerning the PATRIOT Act.

III. Conclusion

So much has been done since 9/11 to better share information and to improve lines of communication among first responders. However, it is hoped that the information provided here will be helpful to the men and women who will be called on in the event of a disaster. Useful references and points of contact are listed throughout these articles.❖

ABOUT THE AUTHOR

❑**Stan Harris** began service as First Assistant United States Attorney for the Southern District of Mississippi on October 23, 2001. Harris serves as Chief-of-Staff for U.S. Attorney Dunn Lampton, and serves as the Southern District's Anti-Terrorism Coordinator.

Mr. Harris formerly served as Chief Counsel and Deputy Chief-of-Staff for Senator Trent Lott, Minority Leader of the U.S. Senate.

Mr. Harris has handled cases and projects involving virtually every federal department and agency, and has received numerous commendations for work on behalf of local, county, state and federal government.

An Overview of the Intelligence Research Specialist Program

Thomas C. Taylor
Assistant United States Attorney
District of the District of Columbia
Currently on detail to the Executive Office for United States Attorneys

I. Introduction

The primary goal of the Department of Justice (Department) Strategic Plan for fiscal years 2001-2006 is to protect America against the threat of terrorism. To implement this goal, the Attorney General articulated the following three-prong objective for the Department:

- the prevention of future terrorist acts;
- the thorough investigation of threats and incidents; and
- the relentless prosecution of those who commit crimes by terrorist means.

With prevention of future terrorist acts as the preeminent goal, criminal intelligence-driven law enforcement, and thus criminal intelligence-driven prosecution, is the Department's principal method to stop a terrorist incident before it happens. The Intelligence Research Specialist (IRS) is the linchpin between intelligence-driven policing and intelligence-driven counterterrorism prosecution in the United States Attorneys' Offices (USAOs)

After the events of 9/11, the Department quickly saw the need to install an Intelligence Officer in each USAO. This officer, the IRS, is charged with obtaining, coordinating, analyzing, and disseminating information relating to the detection and identification of terrorists, of conspiracies to support or commit terrorism, and of terrorist acts. The IRS provides the U.S. Attorney with access to classified criminal intelligence, as well as unclassified "Law Enforcement Sensitive" intelligence. He or she coordinates intelligence activities with and between the members of a district's Anti-Terrorism Advisory Council (ATAC) (formerly the Anti-Terrorism Task Force) and the Joint Terrorism Task Force (JTTF). The goal of this intelligence effort is to share information and resources needed to detect terrorist networks and to arrest and prosecute terrorists before they act.

The IRS supports the ATAC under the guidance of each district's U.S. Attorney and the ATAC Coordinator. The Attorney General stated that ATACs "provide a central forum for agencies to congregate and identify potential terrorism links among their investigations. As the entities that work regularly with all enforcement agencies, [ATACs] are positioned to bring agencies together which would not otherwise know that their respective investigations are linked." *See Memorandum from the Attorney General to all United States Attorneys, September 24, 2003,* available at http://usanet/usa.doj.gov/site_index/ pdf_memos/atac.pdf. The Attorney General also recognized the role of the IRS in the

FBI's JTTF. He directed the IRSs to "provide [Joint Terrorism Task Forces] with intelligence information generated by [Anti-Terrorism Advisory Council] members who are not JTTF members, as well as intelligence obtained by the USAOs from non-terrorism prosecutions and investigations." *See id*. The IRS not only supports the ATAC, but also works with the JTTF as a representative of both the ATAC and the USAO. The IRS is the linchpin between the ATAC and the JTTF, as well as between the USAO, the national intelligence community, and state and local law enforcement.

While the goals of an ATAC and the JTTF are the same, the two entities have very different functions. An ATAC is primarily organizational, emphasizing the sharing and dissemination of counterterrorism information. The JTTF is largely operational, dealing with intelligence collection, analysis, and investigation. An ATAC's membership is expansive, including:

- federal, tribal, state, and local law and non-law enforcement agencies;
- first responders;
- industry leaders; and
- crisis managers.

The JTTFs have a more restrictive membership, comprised primarily of federal, tribal, state, and local law enforcement agencies, and federal intelligence agencies. ATAC members share Law Enforcement Sensitive information. The JTTF has access to top secret national security information. An ATAC gathers intelligence through local sources, while the JTTF garners information from both local and national intelligence sources. Therefore, the two task forces are complementary, not redundant. An IRS provides advice, information, logistical support, and intelligence analysis to both. The IRS is pivotal to intelligence-driven prosecution and the Department's goal of preventing terrorist acts.

II. Responsibilities of the Intelligence Research Specialists

An IRS is essential to every USAO's counterterrorism program. Each district, however, is different and faces unique challenges. An IRS' duties vary depending on the composition of each district. For example, whether a district is large or small, coastal or inland, has a military base, a large tourist attraction, or an international airport hub, can affect how an IRS discharges his responsibilities. Nevertheless, the specialists share many common responsibilities.

All IRSs are tasked with identifying possible terrorist-related incidents or cases in their district and briefing their ATAC coordinator or U.S. Attorney. They review pending cases within the USAO, looking for terrorist connections. An apparently straightforward drug case may contain an overlooked nexus with a conspiracy to provide material support to a terrorist. The trail of money in a Social Security fraud case might lead overseas to a foreign terrorist organization. IRSs review declined cases to ensure that the subject has been checked against the proper databases for possible terrorism connections or other current wants or warrants. They also help identify particular defendants whose cases deserve closer scrutiny.

All IRSs are directed to analyze investigations at the JTTF, searching for perplexing links in otherwise inscrutable relationships. Well-versed in intelligence analysis tools, data mining programs, and information sources, IRSs have access to national intelligence information contained in classified networks or reports. They compile local information, compare selected identifiers with large amounts of data, and select potential prosecution targets. They can review Suspicious Activity Reports (SARs) for actions that alone may be meaningless, but to an informed eye are revealing. The IRSs may attend intake briefings, and they post summaries and review case files to establish connections between investigations. The IRS is often a resource available to the FBI, supplementing the capabilities and supporting the efforts of new field intelligence groups. An IRS' goal, in short, is to ensure that information within the Department is properly analyzed and referred to the appropriate investigating agency.

All IRSs share Law Enforcement Sensitive counterterrorism information with state, tribal, and local law enforcement. Some work primarily through the ATAC, while others produce counterintelligence bulletins for distribution. These bulletins focus on specific topic areas of interest to their district. Some specialists have created secure Web sites for regional alerts and for Law Enforcement Sensitive information exchange. IRSs may also participate in:

- Intelligence Fusion Centers, combining the resources of the Department of Homeland Security, National Guard, state police, and other national and state entities;
- State Information Sharing Centers;
- Joint Operations Centers;
- State Crisis Management programs;
- Security Task Forces; or
- Regional Intelligence Exchange networks.

Specialists work with their district's Law Enforcement Coordinating Committee (LECC), maintaining address rosters, phone trees, and adding counterterrorism training and information to supplement other crime prevention programs.

All IRSs, in cooperation with the LECC, have a responsibility to provide counterterrorism training to tribal, state, and local law enforcement officers. They organize conferences and classes on specific counterterrorism subjects, teaching ATAC members to:

- identify potential targets of attack in the district;
- plan for contingencies;
- identify biological or explosive components of terrorists' weapons; and
- spot seemingly innocuous items and expeditiously report suspicious activities to the intelligence community.

IRSs also show local law enforcement officers how to identify threats, provide security, and garner evidence, while working in the course of their daily duties. They encourage local law enforcement agencies to build trust within immigrant communities and increase awareness of cultural differences. An IRS enables local law enforcement intelligence officers to contact other regional, state, and international organizations, and create networks of counterterrorism intelligence, training, and assistance.

All IRSs are the U.S. Attorneys' liaison to national intelligence agencies such as the Central Intelligence Agency (CIA), National Security Agency (NSA), and the FBI. They have access to secure Law Enforcement Sensitive networks, such as the Regional Information Sharing Systems (RISS) and the FBI's Law Enforcement Online (LEO). Many are establishing links to the Department of Homeland Security's Joint Regional Information Exchange System (JRIES), and within a year, all IRS workstations will be directly connected with the Secret Internet Protocol Router Network (SIPRNET), a classified information sharing and distribution system.

Some districts with Secured Compartmentalized Information Facilities will have access to the Joint Worldwide Intelligence Communication System (JWICS). In a system like the SIPRNET, the JWICS is cleared for top secret national security information. Through their contacts with the intelligence community, the IRSs can brief the U.S. Attorney on current threat analysis and serve as a conduit of information to other local law enforcement agencies' intelligence personnel and state Homeland Security offices. The IRSs use this information to research local groups that may have a relationship to terrorism and to contact informants and cooperators to reveal otherwise unknown links to terrorism. IRSs filter a plethora of intelligence bulletins and alerts for distribution to the appropriate ATAC or JTTF members. Foremost, IRSs maintain an informal network of USAOs' Intelligence Officers, drawing on the combined experience and talents of all.

III. Specific examples

The contributions of all the IRSs have launched an unprecedented move within the Department toward intelligence-driven prosecution, and have enhanced the security of all Americans. While acknowledging that equally worthy programs are absent, a few accomplishments are noted here to demonstrate the contribution of the IRS to the Department's goal of prevention of terrorist attacks.

In one district with a large number of military installations, the ATAC identified the potential threat caused by the numerous Department of Defense subcontractors who had access to military bases. The ATAC wanted to curtail the ability of a possible terrorist to acquire access to the military facility and to identify individuals making and selling false documentation. The IRS, under the operational control of the JTTF, spearheaded the Department of Defense Contractor Initiative, which received information on military subcontractors and analyzed, combined, and summarized the large amount of data into formats that the JTTF could easily pass to FBI Headquarters, the National Crime Information Center (NCIC), the Social Security

Administration, and U.S. Immigration and Customs Enforcement. The program has already resulted in the identification of fourteen individuals with outstanding warrants, nineteen individuals using false Social Security numbers, and seventy-seven individuals using Social Security numbers issued to other individuals.

In another district, the ATAC supported the creation of a Statewide Intelligence Fusion Center. The IRS helped to map and track leads for further investigation and analysis. The Center produces weekly Intelligence Summaries for both law enforcement and non-law enforcement partners. This cooperation has generated good will between the agencies and fostered intelligence-driven policing and prosecution at all levels. Similarly, an IRS in a large northern district makes quarterly visits to law enforcement agencies along the border with Canada, meeting with local service personnel and border patrols to open the lines of communication for local contacts to report any suspicious activity in an area remote to the IRS and the JTTF.

The IRS in a large western district helped organize a General Aviation Working Group within his ATAC. That working group, in partnership with the U.S. Transportation Security Administration, the State Department of Transportation, and the Governor's Office of Homeland Security, tackled the security concerns generated by the numerous smaller general aviation airports throughout the state. Through the efforts of their General Aviation Security Project, the ATAC's participants developed a Memorandum of Understanding which addressed the potential security concerns that would have been outside the scope of traditional federal security measures. The agreement is currently under review by the U.S. Transportation Security Administration and could eventually be used as a national model.

In another large western district, the IRS is assigned as the analyst for the JTTF's International Terrorism squad. On the days detailed to the JTTF, the FBI Supervisory Special Agent in charge of the International Terrorism squad acts as the IRS's supervisor. In addition to his other duties as an intelligence officer, the IRS is also the liaison to his state's Antiterrorism Information Center and is the Assistant District Office Security Manager. This type of integration is possible only through the support of the U.S. Attorney, the District's ATAC Coordinator, and the FBI's Special Agent in Charge.

IV. Conclusion

As top professionals in their field, the Intelligence Research Specialists are the latest arrivals in the USAOs. Most have moved to the Department of Justice after serving in the armed forces, the civilian intelligence community, or other law enforcement. There are also Assistant United States Attorneys, Certified Public Accountants, and others assigned as IRSs. The IRSs have, on average, fourteen to nineteen years experience in intelligence and seventeen to twenty-four years in law enforcement. Although diverse, they all share a common trait: a dedication to their role in combating terrorism in America. The IRSs remain the linchpin of a new model of information exchange, forging essential relationships with other law enforcement agencies, supporting the ATACs in their districts, representing the USAOs on the Joint Terrorism Task Forces, and enabling the USAOs to conduct intelligence-driven prosecution in the Department's fight against terror.❖

ABOUT THE AUTHOR

❑**Thomas C. Taylor** serves as an Assistant United States Attorney for the District of Columbia. He is currently detailed to the Executive Office for United States Attorneys supporting the Intelligence Research Specialist program, Law Enforcement Information Sharing initiatives, and other counterterrorism efforts.✠

LEO and RISS Are a Virtual Single System

This article was reprinted from the CJIS Link, Volume 7, No 3 (April 2004) with permission from the FBI.

By now, nearly every member of law enforcement is aware of a general national effort to increase information sharing and collaboration among the various entities that bear the responsibility for public safety. Since September 11, 2001, the criminal justice community has set a high priority on improving and expanding its communications network as quickly as possible. But many may not be aware of the specific programs in place to make that happen. One significant advance occurred on September 1, 2002, when the FBI's Law Enforcement OnLine (LEO) and the Regional Information Sharing Systems (RISS) established an electronic interface that enables registered users to access both systems with a single log-on.

A major benefit of the LEO/RISS partnership is a secure e-mail system for all users with a riss.net or leo.gov address. As the systems exchange e-mail messages, the information is encrypted and then routed across a private circuit. Both LEO and RISS use the V-ONE SmartPass software, which has made the task of developing a transparent interface less daunting. The two systems update their virus scanning software every hour, which provides another assurance of security.

LEO—background and resources

First established in 1995, LEO is a secure system for e-mail communication, information sharing and collaboration, and training designed exclusively for the law enforcement, criminal justice, and public safety communities. LEO offers e-Learning courses, chat rooms, and membership in special interest groups (SIGs). SIGs are controlled-access areas for organizations or disciplines in law enforcement to exchange and disseminate information. For instance, many of the Criminal Justice Information Services (CJIS) Division's training manuals, handbooks, and technical and operational updates are available to users on the CJIS SIG for downloading.

LEO experienced rapid growth in terms of the number of users and the amount of content following the terrorist attacks on September 11, 2001. This growth occurred just as LEO was replacing its modem dial-up connectivity with Virtual Private Network (VPN) software, enabling users to access the system through any Internet connection. By December 2003, nearly 28,000 individuals were logging on to the FBI's VPN. LEO provides access to a number of databases that are crucial to various groups in the law enforcement community. Of note are the Bomb Data Center, the Hostage/Barricade System, and the Law Enforcement and Intelligence Agency Linguist Access.

Additionally, LEO recently completed interconnectivity with the U.S. Department of Homeland Security (DHS) Information Network so that the DHS and the FBI can share tips. LEO has also initiated a National Alert System that provides the law enforcement community with time-sensitive alerts concerning national security information within minutes of transmission from FBI Headquarters.

Another recent enhancement was the interconnectivity between LEO and the Counterterrorism Reporting on Suspicious Surveillance system to capture cumulative knowledge of suspicious surveillance incidents reported by regional law enforcement and intelligence agencies.

RISS—background and resources

RISS, which was created by Congress in 1974, consists of six regional centers that share intelligence on various criminal enterprises that typically operate across many jurisdictions. Each of the centers operates within its own multistate geographic region by helping member agencies combat terrorism, narcotics trafficking, organized crime, cybercrime, and other illegal activities. Together, the regional centers serve almost 6,800 local, state, tribal, regional, and federal agencies, reaching all 50 states, the District of Columbia, U.S. Territories, Australia, Canada, and England. The RISS resources include, among others, the RISS criminal intelligence databases, other criminal-specific and officer safety databases, an

investigative leads bulletin board, and analytical data visualization tools. Users access RISS resources via the secure Intranet, RISSNET, for nationwide law enforcement communication and information exchange.

During May 2003, RISS initiated the Anti-Terrorism Information Exchange (RISS ATIX) to provide a secure means to disseminate national security, disaster, and terrorist threat information to an additional group of users. Participants in the ATIX include governmental and nongovernmental executives and officials involved with homeland security, including but not limited to fire departments, emergency management, utilities, the transportation industry, and law enforcement.

These users are provided access to specific resources available via RISSNET, including an online real-time bulletin board for posting information, an ATIX Web site, and secure e-mail. In addition, all LEO and RISS law enforcement users have access to the ATIX resources.

Conclusion

The LEO/RISS hookup received strong endorsements at the October 2003 conference of the International Association of Chiefs of Police (IACP). At the meeting, the U.S. Attorney General announced his approval of the National Criminal Intelligence Sharing Plan developed by the Global Intelligence Working Group (GIWG). (The GIWG operates under the auspices of the Department of Justice and the Global Justice Information Sharing Initiative [Global].) Included in the Plan is a recommendation that LEO and RISS, functioning as a virtual single system, "provide the initial sensitive but unclassified secure communications backbone for implementation of a nationwide criminal intelligence sharing capability."

The FBI Director, the Secretary of the DHS, and other law enforcement agencies have publicly endorsed the Plan. The DHS has announced plans to use RISSNET to post its daily reports and warnings.

Importantly, the LEO and RISS connection supports bidirectional information sharing; that is, information flows seamlessly between the two systems. The GIWG views this achievement as a major step in the process of developing nationwide information sharing among law enforcement and public safety agencies. A pilot project is already underway to test a transparent interface between RISS and the National Law Enforcement Telecommunications System, Inc.

The goal of the GIWG is to convince all local, state, tribal, regional, and federal agencies to develop connectivity to this nationwide secure communication network.

Last August, the FBI's National Joint Terrorism Task Force (JTTF) program directed every JTTF member, irrespective of the parent organization, to acquire a LEO account. Further, the U.S. Attorneys, the Organized Crime Drug Enforcement Task Forces, and other law enforcement agencies at every level have followed the recommendation of the National Criminal Intelligence Sharing Plan: join both RISS and LEO in order to maximize information sharing and collaboration.

Law enforcement personnel interested in participating in LEO can contact Ms. Stacey Davis at (304) 625-2618 to request a LEO User Application Form or e-mail stdavis@leo.gov.

Agencies interested in participating in RISS should contact their regional center. Contact information is available on the Internet at: www.iir.com/riss/RISS_centers.htm.❖

The National InfraGard Program: Partnership for the Future

Multiple authors
InfraGard Programs Staff

I. Introduction

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland FBI Field Office in 1996. The program began as a local effort between the technology industry and academia to gain support for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices and, in 1998, the FBI assigned the former National Infrastructure Protection Center (NIPC) responsibility for the national InfraGard program. Since then, InfraGard and the FBI have been seen as trustworthy and credible sources for the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

InfraGard, a partnership between the FBI and the private sector, is an information-sharing and analysis effort serving the interests of its members and combining the knowledge base of a wide range of participants. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants, dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard chapters are geographically linked with FBI Field Office territories. Each InfraGard chapter is assigned an FBI Special Agent Coordinator who works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After 9/11, NIPC expanded its efforts to include combating physical, as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly. In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI kept InfraGard as an FBI sponsored program, and will work with DHS in support of its CIP mission, facilitating InfraGard's role in CIP activities, and further developing InfraGard's ability to support the FBI's counterterrorism and cybercrime investigative missions.

II. Goals and objectives

The goal of InfraGard is to promote ongoing dialogue and timely communication between program members and the FBI. InfraGard members gain access to information that enables them to protect their assets; members in turn give information that facilitates the government's responsibilities to prevent and address terrorism and other crimes. The relationship supports information-sharing at national and local levels and its objectives are to:

- increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime, and other major crime programs;
- increase interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies;
- provide members value-added threat advisories, alerts, and warnings;
- promote effective liaison with local, state, and federal agencies, including DHS; and
- provide members a forum for education and training on counterterrorism, counterintelligence, cyber crime, and other matters relevant to informed reporting of potential crimes and attacks on the United States and its interests.

III. Local chapter activities

Each FBI Field Office has a Special Agent Coordinator who gathers interested companies from a variety of industries to form a chapter. Any company can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats, and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited. Local chapters offer various activities, including: training and

education initiatives, a local newsletter, and a contingency plan for using alternative systems in the event of a successful large scale attack on the information infrastructure.

IV. InfraGard executive board

InfraGard members are represented nationally by an elected board of seven representatives who serve voluntary two-year terms. InfraGard Executive Board (IEB) elections are held annually at the InfraGard National Congress. The IEB conducts weekly conference calls, and board members travel to various chapters, participate in chapter activities, and attend conferences promoting InfraGard and other issues pertinent to the program.

The IEB established several committees to address membership, incorporation, and partnership issues. Special Interest Groups (SIGs) have also been established to investigate the challenges America faces in protecting itself against criminal, terrorist, and intelligence threats. One such SIG involves InfraGard, the National Institute of Standards and Technology (NIST), the Small Business Administration, and the FBI.

V. InfraGard secure Web site

The InfraGard secure Web site provides members with information about recent intrusions and research related to critical infrastructure protection. Members have the capability to communicate securely with other members. Louisiana State University has a contract to support the operation of a secure Virtual Private Network (VPN), which includes e-mail and a Web site that enables InfraGard members and the FBI to exchange sensitive, but unclassified, information. Some of the Web site's features include: new items of interest, sector news, chapter news, discussion groups, archives and libraries, contract information, and feedback requests.

VI. InfraGard public Web site

Please visit the InfraGard public Web site at www.infraguard.net. This site provides the most complete picture of the latest InfraGard initiatives and activities as well as helpful contact information for local InfraGard chapters across the country.❖

The Regional Information Sharing Systems (RISS) and the Anti-Terrorism Information Exchange (ATIX)

Multiple authors
Institute for Intergovernmental Research
Tallahassee, Florida

I. Introduction

Help has arrived! The Regional Information Sharing Systems (RISS™) Program has implemented the Anti-Terrorism Information Exchange (ATIX). Following the terrorist attacks of 9/11, a need for a secure method to timely disseminate information regarding terrorist threats and homeland security information to government and nongovernmental executives and officials became clear. To meet this need, RISS recently implemented ATIX, available through its secure intranet, as the means to exchange national security, disaster, and terrorist threat information to law enforcement, first responders, and key community officials.

RISS traditionally supports the investigative and prosecution efforts of law enforcement and criminal justice agencies. Six RISS centers operate in distinct geographical regions throughout the country, assisting law enforcement and criminal justice member agencies with investigation and prosecution efforts. RISS

utilizes its secure intranet, RISSNET™, as an information-sharing and communications capability for member agencies and participants of other systems connected to RISSNET, such as the FBI Law Enforcement Online (LEO) system.

II. History of RISS

RISS began approximately twenty-five years ago when cooperation and secure information sharing among law enforcement agencies was needed to respond to specific regional crime problems. Since then, RISS has expanded, continuing to foster cooperation, communication, and information sharing between law enforcement and criminal justice member agencies throughout the country. RISS personnel share intelligence and coordinate efforts to combat criminal networks that operate across jurisdictional lines. The regional orientation allows each center to offer support services that are tailored to the investigative and prosecution needs of member agencies, though the centers also provide services and products that are national in scope and significance. Typical targets of RISS member agencies' activities are terrorism, drug trafficking, violent crime, cybercrime, gang activity, and organized crime.

RISS is a federally-funded program administered by the U.S. Department of Justice's Bureau of Justice Assistance (BJA). Each RISS center must comply with the Department's Program Guidelines and the Criminal Intelligence Systems Operating Policies, 28 C.F.R. Part 23 (2003). The executive director and policy board chairperson of each center make up the RISS Directors National Policy Group, which has direct control over the policies and operations of RISSNET and related resources.

Since inception, RISS membership has grown to serve nearly 7,000 law enforcement and criminal justice agencies representing more than 700,000 sworn officers. Membership includes local, state, federal, and tribal law enforcement member agencies in all fifty states, the District of Columbia, U.S. territories, Australia, Canada, and England.

In 1997, RISSNET was implemented. Today, many resources, in addition to the RISS databases, are available for electronic access by member agencies. RISSNET features include online access to a RISS bulletin board, databases, RISS center Web pages, secure e-mail, a RISS search engine, and other center resources. Member agency officers must obtain a security package and enroll on RISSNET. As of April 2004, 16,000 users nationwide have access to RISSNET.

During 1999, RISSNET expanded to electronically connect state and federal law enforcement agency systems in order to provide additional resources to all users. In April 2004, sixteen High Intensity Drug Trafficking Areas (HIDTAs), fifteen state agencies, and eight other federal and regional systems had established connection to RISSNET.

The FBI LEO system interconnected with RISS in September 2002. In October 2003, the *National Criminal Intelligence Sharing Plan* recommended the RISS/LEO system as the initial sensitive but unclassified (SBU) communications backbone for implementation of a nationwide criminal intelligence-sharing capability. The Plan encourages agencies to connect their system to RISS/LEO.

Traditionally, RISS has focused on serving investigative and prosecution efforts of multi-jurisdictional criminal activity. In 2003 RISS implemented ATIX to provide additional users with access to homeland security, disaster, and terrorist threat information. RISS member agencies, as well as executives and officials from other first responder agencies and critical infrastructure entities, can access ATIX.

RISS has a long, established relationship with the Executive Office for U.S. Attorneys and the U.S. Attorneys' Offices (USAOs). Both are current members of RISS and have access to RISSNET and ATIX resources.

III. Overview of RISS ATIX

Utilizing RISSNET, ATIX provides a secure electronic environment for executives and officials to exchange ideas, documents, news articles, and the latest SBU information. Under the *National Criminal Intelligence Sharing Plan*, the standards-based security methods employed by RISSNET have been approved and endorsed by the U.S. Attorney General, the Director of the FBI, the Secretary of the U.S. Department of Homeland Security (DHS), and other officials involved with law enforcement and homeland security.

A. RISS-ATIX communities

Upon enrolling with RISS to use ATIX, participants choose an ATIX "community" group, which is tailored to their responsibilities in planning and implementing prevention, response, mitigation, and recovery efforts related to terrorism and disasters. The current ATIX communities include:

- state, county, local, and tribal levels of emergency management;
- law enforcement;
- government;
- utility services;
- the chemical industry; and
- the agriculture and food industry.

RISS is continually identifying additional communities for access to ATIX, but current RISS ATIX communities include:

- bioterrorism;
- fire departments;
- emergency medical providers;
- disaster relief organizations;
- special skill rescue units;
- state, county, local, and tribal public health executives;
- environmental protection agencies;
- public and private utility services (water, power, and other);
- National Guard executives;
- agriculture and food industry organizations;
- banking and financing entities;
- chemical industries;
- education organizations (primary, secondary, and universities);
- hotel industries;
- postal and shipping organizations;
- private security industries;
- telecommunication industries;
- transportation industries;
- law enforcement or criminal justice agencies;
- certified police instructors;
- state, county, local, and tribal government executives;
- Federal Government executives and agencies; and
- state, county, local, and tribal emergency management agencies.

B. All ATIX participants have access to secure electronic bulletin boards, Web pages, and an e-mail account.

The electronic bulletin board provides a forum for participants to discuss terrorism, disaster, and homeland security information. Specific discussion conferences are maintained for each ATIX community, and participants can immediately view messages posted on the bulletin board. This feature allows for rapid communication and response to breaking news items. Examples of postings include information on items that people have attempted to pass through security checkpoints and new security measures that have been implemented. Additionally, the bulletin board has a chat feature, allowing for real-time discussion of current news and events. Participants can also request information from others visiting the bulletin board or invite them to join a chat session.

The ATIX Web pages feature recent news articles, documents, a search capability, and the current threat advisory level from DHS. Users are encouraged to submit information to the Web page which would be of interest to other participants, such as preparedness guidelines and plans for response to incidents. The Web pages also provide links to homeland security, terrorism, and disaster-related Web sites. Links are categorized by their corresponding ATIX community and include national associations; police, fire, and public health agencies; and government offices. Participants can subscribe to newsletters published by other organizations to receive additional information. Recently, DHS agreed to establish an interface with RISSNET to post its daily reports and warnings. A participant's contact information is available on the Web page in order to facilitate communication between participants within and outside of the USAOs. Contact information includes each participant's secure ATIX e-mail address, and information regarding each ATIX state point of contact and RISS center.

All ATIX participants receive a secure e-mail address on RISSNET. E-mail can be directed to a specific ATIX participant based on his geographic location, his role with respect to terrorism prevention and disaster relief, or his individual status within ATIX. Additionally, participants can send secure, encrypted ATIX e-mail to all ATIX e-mail addresses and to any other secure RISSNET e-mail address.

IV. How to join ATIX

Currently over 16,000 individuals have access to the ATIX resources. In order to facilitate the vital efforts to exchange information and promote homeland security, participants should visit the ATIX resources often to provide feedback and make contributions that can be shared with other participants.

For additional information regarding RISS and joining ATIX, please contact the ATIX coordinator at the RISS center in your geographic region:

Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN) serving Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, and the District of Columbia. The center also has member agencies in England, and the Canadian provinces of Ontario and Quebec, and Australia.

Phone: (215) 504-4910

E-mail: info@magloclen.riss.net

Mid-States Organized Crime Information Center (MOCIC) serving Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin. The center also has member agencies in Canada.

Phone: (417) 883-4383

E-mail: info@mocic.riss.net

New England State Police Information Network (NESPIN) serving Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont. The center also has member agencies in Canada.

Phone: (508) 528-8200

E-mail: info@nespin.riss.net

Rocky Mountain Information Network (RMIN) serving Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming. The center also has member agencies in Canada.

Phone: (602) 351-2320

E-mail: info@rmin.riss.net

Regional Organized Crime Information Center (ROCIC) serving Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia, as well as Puerto Rico and the U.S. Virgin Islands.

Phone: (615) 871-0013

E-mail: info@rocic.riss.net

Western States Information Network (WSIN) serving Alaska, California, Hawaii, Oregon, and Washington. The center also has member agencies in Canada, Australia, and Guam.

Phone: (916) 263-1166

E-mail: info@wsin.riss.net

V. Conclusion

The ATIX services can be used to provide secure and rapid information sharing among USAOs and other participants. As breaking news develops, the RISS-ATIX Web pages can be modified to provide information relevant to current events, including news articles and links to additional resources. The ATIX bulletin board allows for real-time communication among all the participants, and participants can direct questions and information to individuals and communities of users using the secure e-mail feature. Participants should actively contribute valuable information, such as bulletins, guidelines, alerts, links, and information related to homeland security, on the ATIX bulletin board and Web site to aid other participants in their homeland security and disaster-preparedness efforts.❖

ABOUT THE AUTHORS

❑**Several staff members** at the Institute for Intergovernmental Research (IIR) contributed to this article. IIR provides training, research, and analysis services to the Regional Information Sharing Systems (RISS) Program through the support of grant awards from the Bureau of Justice Assistance.

IIR is a research and training organization specializing in law enforcement, juvenile justice,

and criminal justice issues. IIR is a nonprofit corporation formed in 1978 and chartered in Florida, with headquarters in Tallahassee, Florida.

IIR is specifically organized to conduct nonpartisan research and management studies regarding the role and function of the branches and agencies of local, state, and Federal Government, and to support the development and enhancement of governmental effectiveness.✠

Interoperability AGILE-ity

Reprinted From Fall 2002 TechBeat

Thirty-plus years ago, when police radios were under-powered and cumbersome, one officer voiced his frustration about his inability to communicate with fellow officers this way: "Mission Control could talk to astronauts on the moon, but we couldn't talk to our partners around the corner, less than a block away."

Today police radios are certainly smaller and much more powerful. But improvements in technology have not eliminated the issue of interoperability—the capacity of public safety agencies at all levels to communicate across jurisdictions. This country's law enforcement agencies, emergency medical services, and fire departments operate on different frequencies, use different equipment, and follow different policies and procedures, making communication and coordination between agencies and across jurisdictions very difficult.

AGILE, a National Institute of Justice (NIJ) project, is trying to make interoperability much less difficult.

"Interoperability is a complex situation that has been evolving over the years," says Tom Coty, AGILE program manager. "It's complex not only because of the sheer number of agencies, but also because they are in different points in the life cycle of their equipment. One may have a brand-new system, while another nearby agency has equipment that is 15 to 20 years old."

According to Coty, most public safety professionals would say they have experienced problems communicating with others in their field. Each agency, however, faces different interoperability issues, such as outdated equipment and no funds to buy new equipment; city police and fire department radios that operate on different frequencies; cell phones that allow different agencies to talk to one another, but have significant access problems during critical events; and existing communication links between agencies, but no policies or procedures that cover when and how to use them.

For most public safety agencies, Coty says, the biggest problems stem from incompatible radio frequencies and lack of funds to buy new equipment.

The Federal Communications Commission (FCC) licenses radio frequencies for all non-Federal users of the radio spectrum, including public safety agencies, commercial radio and television stations, business radios, and more. The spectrum is a range of frequencies used for communications. It is a finite resource divided into bands, 10 of which are for public safety agencies' use. Within those bands, the FCC licenses the frequencies or channels used by each agency. Frequency is measured in terms of millions of cycles per second, or megahertz (MHz).

No commercially available radio operates in all 10 bands available to the public safety community. Some radios made by different manufacturers cannot even communicate with each other within the same band. This leads to temporary "fixes," such as installing numerous radios in ambulances and patrol cars so their occupants can talk to everyone else in an area. Another commonly used fix, the dispatch relay, uses a third party to relay messages from one agency to another. These solutions are

cumbersome and expensive. They use up precious time that could allow a suspect to escape or a fire to spread.

Technology solutions to interoperability problems are becoming more common. One solution employs a cross-band-repeater system, which receives a transmission on one frequency and automatically retransmits it on a different one. Unfortunately, law enforcement and other public safety agencies often do not know which new technologies can help them, or even that these technologies exist.

In 1998, NIJ's National Law Enforcement and Corrections Technology Center (NLECTC)–Rocky Mountain completed an intensive study of interoperability issues, *State and Local Law Enforcement Wireless Communications and Interoperability: A Quantitative Analysis*. NIJ used the study to launch the AGILE program, which consolidates all NIJ interoperability initiatives into a coordinated effort to help federal, state, and local law enforcement agencies communicate and share information. AGILE, originally Interoperability AGILE-ity, stood for Advanced Generation of Interoperability for Law Enforcement, but its target audience has expanded to include all public safety agencies.

"AGILE facilitates information sharing and provides support to professionals, giving them the ability to help themselves," Coty says. Nationally, that can mean providing support to public safety associations and their leaders; locally, it can mean offering one-on-one technology assistance. AGILE uses a three-part approach to implement its mission:

- Research, development, testing, and evaluation of technology solutions.
- Standards identification, development, and adoption.
- Outreach and technology assistance.

No single fix can solve complex interoperability issues for everyone, Coty says. At any point in time, AGILE has more than 30 projects and initiatives in various stages of development. One of them may provide just the solution an agency needs.

Interoperability Technology

Coty says public safety personnel often learn about new technologies by viewing a demonstration at a conference or by reading about new equipment in a journal. Agencies may not know who developed the technology, whether it will work with their systems, or where to find out more about it. They can begin their research on the AGILE website at www.agileprogram.org.

The AGILE site includes a section that lists site updates and the latest interoperability news. The site provides access to AGILE reports and printed materials and offers information on grants and funding, interoperability standards, the National Task Force on Interoperability, and a list of related links. It also provides updates on AGILE research projects, including the following:

- **ACU–1000 Testbed Program.** The City of Alexandria (Virginia) Police Department has served as a testbed for several potential interoperability communications solutions, including the ACU–1000, an audio gateway system that ties together incompatible radio systems. The ACU–1000 provided coverage at the inauguration of President George W. Bush, linking the U.S. Secret Service, the U.S. Capitol Police, the Federal Bureau of Investigation, and other agencies. Alexandria will soon test two new systems: Lyric, a Motorola product to link Motorola technology, and Incident Command Radio Interface (ICRI), a Communications Applied Technology product. Although similar to the ACU–1000, the portable ICRI system can run its briefcase-sized unit on AA batteries for up to 24 hours.
- **CAPRAD.** In the Balanced Budget Act of 1997, Congress directed the FCC to reallocate 24 MHz of spectrum in the 700 MHz band for public safety use. Now used by UHF television channels 60 to 69, this spectrum will become available within the next several years. In anticipation of the release of this spectrum, the National Public Safety Telecommunications Council (NPSTC) and the Public Safety Communications Council requested the development of a Computer-Assisted Precoordination Resource and Database (CAPRAD) to facilitate interregional coordination in the allotment of frequencies. NLECTC–Rocky Mountain recently completed this database, which will

have secure Internet access, and is now working on database distribution and orientation.

- **CAPWIN.** Several years ago, a man threatened to commit suicide by jumping from the Capital Beltway's Woodrow Wilson Bridge. Agencies from Maryland, Virginia, and the District of Columbia ran into numerous interoperability problems while trying to coordinate rescue efforts and untangle a rush-hour traffic jam. This incident, among others, triggered the request to create the Capital Wireless Integrated Network (CAPWIN). CAPWIN will integrate existing data and voice communication systems into the Nation's first multistate integrated wireless data network devoted to transportation and public safety. Research and development are now under way at the University of Maryland, the University of Virginia, and George Mason University. The goal is to make this network a model that can be replicated in other regions of the country.
- **COPLINK.** Developed through a joint effort between the University of Arizona and the Tucson Police Department, COPLINK Knowledge Management System software uses the Internet to link member databases. The COPLINK Connect module allows real-time information sharing across a network of records management systems that use different software and parameters. The COPLINK Detect module provides advanced data analysis. For example, one can search for information on white two-door cars and information on sex offenders known to frequent school playgrounds, then search for matches between the two.
- **INFOTECH.** INFOTECH, an NIJ research and development project completed in FY 2001, developed tools and technologies to tie together disparate legacy systems to permit information sharing with appropriate security/privacy. Software and data models from this project are freely available. INFOTECH uses Java™software and encryption to allow searching with a simple Internet browser and offers real-time access to criminal history information, motor vehicle registration information, driver's license information, and local agency data. Participating agencies decide what information to make available to other members. Sheriff's departments in Monroe, Broward, and Brevard Counties in Florida provided an early demonstration of this system. Virginia's Tidewater region; the Charleston, South Carolina, region; the State of Oregon; and the cities of San Diego and Los Angeles all have deployed INFOTECH based solutions for their information-sharing needs.
- **Software-Defined Radios.** AGILE staff are helping to develop and evaluate a new generation of communications devices known as Software Defined Radios (SDRs). SDRs, which can be quickly reprogrammed to transmit and receive on multiple frequencies in different transmission formats, could change the way users communicate across wireless services and promote more efficient use of the radio spectrum. In SDRs, functions that were formerly carried out solely by hardware, such as the generation of the transmitted radio signal and the tuning of the received radio signal, are performed by software. Because these functions are carried out by software, the radio is programmable, allowing it to transmit and receive over a wide range of frequencies and to emulate virtually any desired transmission format.

Interoperability Standards

Just as the research and development portion of AGILE includes many components, its Standards Project reviews and analyzes standards related to all of the many facets of interoperability. The project's goal is to identify and create comprehensive interoperability standards for NIJ adoption. Coty says that although some new standards may need to be developed, most interoperability standards already have been created by such organizations as the Telecommunications Industry Association (TIA) through the development work of the Association of Public Safety Communications Officers (APCO) and the Institute of Electrical and Electronics Engineers. AGILE is supporting several standards development projects, including—

- **Project 25**, an APCO effort that developed an interface standard for digital radios with backwards compatibility to analog and manufacturers' legacy systems.

- **Project MESA**, is a TIA/European Telecommunications Standards Institute initiative to create specific requirements for broadband transmission. Increased use of broadband transmission could allow rapid streaming of videos and images to law enforcement personnel in the field.
- **XML-Based Standards for Integrated Justice,** jointly supported by the Bureau of Justice Assistance and AGILE, is a project of the Infrastructure and Standards Working Group of the Global Advisory Committee to facilitate the sharing of justice information and integration of justice information systems among Federal, State, and regional jurisdictions; establish ground floor information standards; guide and assist justice and public safety information systems developers; and further other efforts to share justice information.

Interoperability Outreach and Assistance

AGILE outreach, like research and development and standards development, encompasses many elements. Outreach components include the website, conference presentations, and telephone assistance. Additionally, in response to requests from public safety agencies, AGILE dispatches experts to assess agencies' capabilities and propose solutions, Coty says. "Often, a lot of the solutions are fairly simple. For example, the agency may be dealing with vendors who sell new equipment. We send out an engineer who will sit at the table with them during vendor discussions. This expert has only their interests in mind."

Technical experts also visit sites once the equipment is in place, Coty says. After the equipment is set up, it is important that the agency work out agreements with other nearby units, develop a policy on use of the new equipment, and practice and train for its use. Outreach and assistance projects include—

- **National Task Force on Interoperability.** In an effort to improve public safety radio communications, NIJ, supported by 17 national associations, cosponsored the 2001 National Public Safety Wireless Interoperability Forum in October 2001. Forum participants were predominantly State and local elected and appointed officials and representatives from the public safety community. Its goals were to raise public safety wireless interoperability issues to the national level and to give participants the opportunity to develop a list of actions that could be taken to overcome the policy barriers to improving public safety wireless communications.

  The forum received such a positive response that NIJ continued the effort by funding the creation of a National Task Force on Interoperability (NTFI). NTFI's vision is to foster cooperation among Federal, State, regional, and local public safety agencies through the development and use of interoperable communications systems. Its mission is to help public safety agencies achieve communications interoperability. NTFI serves as a conduit between State and local officials, their representative associations, Federal officials, and public safety and industry representatives to create a unified policy front and facilitate resulting actions. To accomplish this, NTFI will educate State and local officials and their representative associations about the benefits of interoperability, assist them in addressing the policies needed to overcome current barriers, and provide a forum for policymakers to work with the public safety community to address interoperability issues.
- **NPSTC Support Office.** AGILE also funded the creation of the NPSTC Support Office (NSO) in FY 2000. NSO fills the role of secretariat for NPSTC, a federation of 17 associations that represents the national public safety community in wireless communications.
- **Interoperability Assessment for the State of Texas.** In conjunction with the Sheriffs' Association of Texas and the State of Texas, AGILE is surveying the existing infrastructure and proposing solutions to interoperability issues. In addition to building partnerships among associations throughout the State, this project will develop a how-to guide for interoperability projects statewide.

Technology, standards, and outreach and assistance add up to AGILE's mission to solve the problems related to interoperability, problems that also include a lack of available spectrum and funding for new equipment. "Technology isn't the stumbling block," Coty says. "You can overcome

technology issues. The really hard task is working out the policies and their day-to-day execution."

For more information on AGILE, visit the AGILE website at www.agileprogram.org.

The National Law Enforcement and Corrections Technology Center System Your Technology Partner, www.justnet.org, 800–248–2742 ❖

This article was reprinted from the Fall 2002 edition of TechBeat, the award-winning quarterly news magazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.✠

Forensic Epidemiology

Francis D. Schmitz
First Assistant United States Attorney
Eastern District of Wisconsin

I. Introduction

The anthrax attacks and other biological threats and hoaxes that occurred throughout the United States in the fall of 2001 required unprecedented cooperation between law enforcement, first responders, public safety officials, and public health agencies. The responses to such threats affirmed many similarities in the investigative methods used by both law enforcement and public health officials, but the events also highlighted significant differences in the ways that each responder approaches a problem. In order to increase the effectiveness of responses to possible future biological threats, the United States Centers for Disease Control Prevention (CDC) thought it necessary to foster improved understanding of the investigative goals and methods used by each discipline and strengthen interdisciplinary collaboration. In the spring of 2002, the Public Health Law Program of the CDC, in partnership with the Department of Justice (Department) and other agencies, undertook to develop a course for the joint training of law enforcement and public health officials. (Further information on the Public Health Law Program can be found at www.phppo.cdc.gov/od/phlp). This course has often been referred to as the "Forensic Epidemiology" course.

II. How the course works

Once the course was developed, it piloted successfully in Chapel Hill, North Carolina; Jacksonville, Florida; Baltimore, Maryland; and Los Angeles, California.

Frank Whitney, the United States Attorney for the Eastern District of North Carolina, participated in the first trial and is a strong supporter of the course. He states, "by spending a day and a half working through bioterrorism scenarios with the North Carolina state epidemiologist, I learned how critical it was that we team up the investigative resources of law enforcement and public health. In the case of a

real bioterrorism incident, time is too precious to be meeting and coordinating with your public health colleagues for the first time." E-mail from Frank Whitney to Francis Schmitz (April 17, 2003).

In April 2003 the Department's Office of Legal Education sponsored a "Train-the-Course Managers" program in Atlanta, Georgia. Each U.S. Attorney's Office was invited to send a representative, along with a public health official from the state and a weapons of mass destruction (WMD) coordinator from each FBI Division.

The first training session used presentations about criminal and public health laboratories and FBI investigations of WMD to establish a common understanding of the goals, methods, and vocabulary used by both law enforcement and public health officials. Afterwards, the participants broke into small groups consisting of an equal mix of public health and law enforcement officials and facilitators. The groups were then presented with three scenarios based upon actual incidents. One scenario involved finding a suspicious letter containing white powder in DeKalb County, Georgia; another dealt with the anthrax scare in Florida; and the third recreated an Oregon cult's salmonella poisoning incident. In small groups, the participants addressed key objectives on a variety of issues that included:

- conducting an epidemiological investigation;
- responding to public health concerns at a crime scene;
- meshing criminal investigative procedures with epidemiological, laboratory, and other scientific procedures; and
- combining law enforcement and public health operations and communications.

Finally, the attendees reconvened in the third session to combine their new skills and develop a possible after-action plan.

During the course, each attendee received a training package that included: a Course Manager's Guide in both cd-rom and paper format, and an instructional template that can be used in any jurisdiction in the United States. The Guide provides:

- detailed information on course planning and design;
- template presentations and case studies;
- supplemental reference material; and
- logistical information.

Additionally, sample agendas, suggestions on which participants to include, and discussions on how to modify the course to meet particular jurisdictional needs are provided. In the past, AUSAs gave the law enforcement for public health presentation, but the course is flexible enough to have a local law enforcement officer make the presentation.

III. Impact

As of April 2004, sixty-five courses have been conducted throughout the nation in twenty-six states. Over 5,000 individuals have been trained, and many other courses are being planned and scheduled. The CDC has contracted with Science Applications International Corporation (SAIC) to provide assistance to public health and law enforcement officials involved in the planning of future training. The SAIC representative is Ms. Carey Mitchell, who can be reached at 770-936-3620 or by e-mail at Elizabeth.C.Mitchell@saic.com. Ms. Mitchell is willing and able to assist in any course planning, and she keeps agendas and training materials on file. She can also provide a Forensic Epidemiology Course Manager's Guide if needed. Ms. Mitchell has designed a one-day course that is available to districts. The instructional template made it easy to design the course in conjunction with state and local public health officials. In Wisconsin, the materials were tailored to include a brief introductory presentation on terrorism threats. This presentation benefitted public health attendees who normally do not receive such information. Dr. Richard A. Goodman, Co-Director of the CDC Public Health Law Program can also be contacted for assistance at 770-488-2624 or Rag4@cdc.gov.

At a recent ATAC Coordinator's conference, many said that the lack of funds hampered the districts' ability to conduct the training. The CDC, however, has graciously provided funding through a bioterrorism cooperative agreement with each state health department that will assist in planning and implementing this training. State officials are advised to check award number U90/CCU116972-040 for funds.

IV. Conclusion

Most prosecutors, law enforcement officers, and public health officials have never had an opportunity to work with one another. This course will not only expose these disciplines to each other, but it will also build relationships necessary to successfully work together in the event of a bioterrorist threat. Given the interest that terrorist organizations have shown in biological and chemical weapons, it is therefore important that forensic epidemiology training be conducted in every district, with the support of the ATAC.❖

ABOUT THE AUTHOR

❑**Francis D. Schmitz** is the First Assistant United States Attorney and ATAC Coordinator for the Eastern District of Wisconsin where he has been employed for over twenty years. Prior to his tenure as a federal prosecutor he served as a law clerk for a Seventh Circuit Court of Appeals judge.✠

PATRIOT–Counterterrorism Training Program

Jim Greenlee
United States Attorney
Northern District of Mississippi

David Crews
LECC/Anti-Terrorism Advisory Council Chief-Information Officer
United States Attorney's Office
Northern District of Mississippi

Tom Bartlett
Anti-Terrorism Coordinator for the Southern Regional Public Safety Institute

Max Fenn
Intelligence Research Specialist
United States Attorney's Office
Southern District of Mississippi

I. Introduction

In a terrorism training seminar shortly after 9/11, an officer posed a question that shivered the spines of those from the United States Attorney Offices (USAOs) who were teaching. The question drove home the need for a top-notch, practical approach to strengthening law enforcement's ability to understand, prevent, and interdict terrorist plans and attacks. The officer asked, "This is good information, but I really don't need to be here. I'm a patrolman. What does prevention and intel have to do with me?" Based on this simple misunderstanding, Mississippi's USAO Anti-Terrorism Advisory Councils (ATACs) and Law Enforcement Coordinating Committees (LECCs) developed a coordinated, content-driven, practical seminar giving patrolmen and other first responders the tools needed to identify, report, and prevent possible terrorist activities.

II. Course overview

The prevention-oriented anti-terrorism training was aptly named "PATRIOT," an acronym standing for Preventive, Anti-Terrorism Recognition and Interdiction Operational Techniques. The training was conducted from January through September 2003, and over 3,000 personnel attended, including officers from law enforcement, fire, hazardous materials (haz-mat) teams, emergency management, emergency medical services, and school resource officers.

Training for first responders traditionally has concentrated on how to respond to an event or crisis. PATRIOT's core goal was to give officers, agents, and first responders the tools and intelligence information to help prevent and interdict terrorism.

PATRIOT training focuses on the following three tiers of prevention:

- preventing an attack from occurring;

- if an attack occurs, preventing first responders and civilians from becoming additional victims; and
- learning evidence recognition and preservation skills so that rescue efforts also can preserve evidence as much as possible.

With proper evidence, perpetrators can be brought to justice quickly, thereby preventing further terrorism through successful prosecution.

Training the first responders in Mississippi strengthened their ability to work together in a common effort to recognize and prevent terrorism. The two-day PATRIOT seminar was taught across the state of Mississippi. The training was a joint effort sponsored by the ATACs of the U.S. Attorneys' Offices for the Northern and Southern Districts of Mississippi, and co-sponsored by the following agencies:

- the Federal Bureau of Investigation;
- the Mississippi State Department of Health; and
- the State Fire Academy and the Mississippi Emergency Management Agency.

The Mississippi Department of Public Safety, the Southern Regional Public Safety Institute, the Mississippi National Guard, the Mississippi Department of Environmental Quality, the U.S. Marshals Service, and the Mississippi Board of Standards and Training also were involved in PATRIOT's development and presentation. The combined efforts of all of these agencies made the PATRIOT seminar not only successful, but also cost effective.

The training was held in fifteen locations statewide so that first responders were not required to travel over forty-five minutes to attend the training. The training was made as accessible as possible in order to maximize participation among agencies.

PATRIOT was designed to train first responders "in concert" so that each discipline might appreciate the other's significant role in preventing and responding to terrorism. The key difference between PATRIOT training and other training is that the core focus of the seminars was on threat recognition and interdiction in order to foster prevention. The sixteen-hour course included topics such as terrorist cell structure, terrorist financing, intelligence considerations, databases, information-sharing systems and the intelligence cycle, evidence preservation, haz-mat issues, and public health threats when a terrorist uses chemical, biological, radiological, and explosive agents, as well as a wide variety of other topics.

From the inception of PATRIOT, the importance of having quality instruction and materials was paramount. The finished product encompassed twelve modules including content-rich materials coordinated with the instructors' presentations. Each module was prepared and taught by certified instructors and subject-matter experts, so that appropriate credit was received upon completion. Each participant received the instructional manual, which can be used as a reference guide.

Fundamental to the curriculum integrity and premium quality of PATRIOT was intensive review and critique by an expert team of multi-discipline evaluators. From the beginning, developers sought input from the Center for Domestic Preparedness (CDP) in structuring the course. CDP helped advise PATRIOT developers how the PATRIOT multi-agency team could build its own prevention-based curriculum. It was at CDP's suggestion that developers opted for the two-day curriculum, as this time frame represented the best balance between content and the ability of most first responders to attend.

Tom Bartlett served as primary course developer. In addition to his present service as Antiterrorism Coordinator for the Southern Regional Public Safety Institute, Tom is a long-time law enforcement officer who has also served as a fireman, emergency medical technician, and a haz-mat team leader. He served on the adjunct staff of the Center for Domestic Preparedness and also taught for the Department of Defense and other agencies. Tom worked directly with agency personnel in preparing the curriculum.

A two-day dress rehearsal of the program was held with a "blue ribbon" team of approximately fifty multi-discipline evaluators from Mississippi. Originally, PATRIOT was to be taught with separate break-out sessions for different first responder disciplines. However, at the conclusion of the dress rehearsal, evaluators unanimously agreed that they wanted to train together throughout the entire course.

National evaluators from the following agencies were invited to attend:

- State and Local Anti-Terrorism Training (SLATT);
- the Regional Information Sharing System (RISS);
- the Office of Domestic Preparedness in Washington, D.C.;
- the Center for Domestic Preparedness in Anniston, Alabama; and
- the Executive Office for U.S. Attorneys (EOUSA).

Additionally, course developers stayed in contact and consultation with coordinators at EOUSA and the Department of Justice (Department) Counterterrorism Section (CTS) throughout the process. In February 2004 the program's progress and success was briefed to CTS, EOUSA and ODP. At each step, developers have looked for ways to "hone and refine."

III. Remarks and concurrent training

United States Attorney Jim Greenlee (N.D. Miss.) said, "PATRIOT Training being first responder training makes our law enforcement, fire, and EMS personnel much more effective in combating terrorism—the President's, the Attorney General's and the Nation's top priority. It has the additional benefit of fostering cooperation and of strengthening skills that will help us in many other areas as well." State Fire Academy, Pearl, Miss. (Sept. 30, 2003). United States Attorney (S.D. Miss.) Dunn Lampton noted that "It is imperative that our focus be on the prevention of terrorist acts, and this training makes all of us more vigilant and skilled in prevention efforts. Combined field training among fire, law enforcement, and EMS to *prevent* terrorism was unprecedented before PATRIOT, and should become a model for future teamwork and training in our state and across the Nation." State Fire Academy, Pearl, Miss. (Jan. 27, 2003).

Both District Offices in Mississippi have held a variety of antiterrorism training sessions that have delved into specialized topics such as intelligence, suicide bombings, complex investigations, and Weapons of Mass Destruction (WMD). Among the instructors at these seminars have been David Harel of the Israeli Security Agency, Kim Durham of Scotland Yard, Bill Lowry of the Intelligence Special Branch of Northern Ireland, Dick Marquise of the FBI (who headed the Lockerbie/Pan Am 103 investigation), Dr. Ahmed Hashim of the U.S. Naval War College and Central Command (CentCom), Detective Sergeant Bob Fromme who launched the Hezbollah investigation in North Carolina, Chief Detective John Short of Crime Operations Northern Ireland, FINCEN instructors, and many others.

IV. PATRIOT training modules and special materials

Module 0 Registration

Module 1 Introduction, Information Sharing & OPSEC

Includes special articles as follows:

- Overview of Information Sharing
- Regional Information Sharing Systems
- 9/11 Exposed Flaws in Rescue Plan
- Do Fire Departments Need OPSEC?

Module 2 Agency Coordination & Incident Command/NIIMS

Includes special articles as follows:

- Techniques for Dealing with Media Regarding Security Issues

Module 3 Terrorist Recognition, Interdiction & Prevention

Includes special articles as follows:

- Guidance for Terrorist Surveillance Detection
- FBI Bulletin–Indicators of Al-Qaeda Surveillance
- Clues to Al-Qaeda Cells Operating in U.S.
- Bold Tracks of Terrorism's Mastermind
- FBI Bulletin–Lone Extremists
- FBI Bulletin–Using Women to Facilitate Al-Qaeda Operations
- FBI Bulletin–Increasing Potential in Hate Crimes Against Arabs, Muslims & Sikh Americans

Module 4 Target Recognition, Interdiction & Prevention

Module 5 Haz-mat Targets & Prevention

Module 6 Bomb/Burn Injury Recognition & Prevention

Module 7 Weapon Recognition, Interdiction & Prevention

Includes special articles as follows:

- Homeland Security Information Bulletin—Potential Indicators of Threats Involving Vehicle Borne Improvised Explosive Devices

Module 8 Immigration Documents & Interactive Panel Scenarios

Module 9A Public Health Update

Module 9B Evidence Recognition & Preservation

Module 10 Bio/Chem Recognition, Preparedness & Prevention

Includes special articles as follows:

- Countering Bioterrorism and Other Threats to Food Supply
- Hazardous Chemical Web sites

Module 11 Personal Protective Equipment & Decontamination Planning

Module 12 Introduction to Terrorist Operations, Counterterrorism Strategies & Tactical Options

Includes special articles as follows:

- Biological and Chemical Agents- Quick Reference Guide
- Al Qaeda Training Tape Assessment
- FBI Bulletin—Refinement in Al-Qaeda Operational Capabilities
- Suspicious Inquiries about Chemical Agents
- Al-Qaeda Bio-Chem, Radiological, Nuclear Threat and Basic Countermeasures
- FBI Bulletin—Improvised Chemical and Biological Agents
- FBI Bulletin—Potential Improvised Chemical Weapons Threat

Module 13 Interactive Panel Interdiction Scenarios

Appendices

Tab 14 War on Terrorism Accomplishments—Establishing the Priority of Prevention

Tab 15 Federal Statutes RE: Counterterrorism

Includes special articles as follows:

- U.S. Code Provisions Applicable to Terrorism
- Current Counterterrorism Legislation and Information Resources

Tab 16 National Strategy for Combating Terrorism

Tab 17 Emergency Responder Guidelines

Tab 18 Terrorist Financing, Organizations, Operations

Tab 19 Anti-Radiation Public Safety Primer

Tab 20 Training and Technical Assistance

Tab 21 Antiterrorism Funding and Equipment

Includes special articles as follows:

- Training and Technical Assistance Resources
- MEMA Training Section and Application

Tab 22 Homeland Security

Tab 23 Citizen Preparedness & Web sites

Includes special articles as follows:

- Department of Homeland Security
- Advisory System Color Code Chart
- Mississippi Homeland Security
- DHS Citizen Preparedness
- FBI War on Terrorism
- Mississippi Dept. of Public Safety
- American Red Cross
- Individual Preparedness for Orange Alert
- FEMA Preparedness Website
- Security Related Consideration for Managers
- Emergency Procedures for Disabled Persons
- CJCS "Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism"

V. Program learning objectives

The sixteen-hour PATRIOT program is presented at the awareness level for first responders who may be in a position to detect pre-incident indicators of a terrorist threat, and prevent initial or additional threats and acts of terrorism. At the conclusion of this training program, the participant should be able to:

A. Understand the need for a local anti-terrorism prevention initiative, understand the general characteristics of terrorist threats, and identify terrorist recognition parameters.

- Identify the objectives of the United States Attorney's Office in preventing future terrorist attacks through the Anti-Terrorism Advisory Council (ATAC) concept.
- Understand the significance of local first responders functioning as partners in the prevention of terrorist threats or acts.
- Identify past terrorist events and understand how both foreign and domestic terrorism poses a potential threat to the United States.
- Understand suicide bomber motives and identify potential terrorist recognition factors.

B. Recognize hazardous materials incidents.

- Understand what hazardous materials are, as well as the risks associated with these materials in a terrorist or emergency incident.
- Identify if hazardous materials are present in a terrorist emergency incident.
- Know how to use the *North American Emergency Response Guidebook* (NAERG*)* published by the U.S. Department of Transportation to recognize potential terrorist haz-mat targets.
- Use the NAERG, or other available resources, to identify the hazardous material that might be targeted by terrorists.
- Understand the potential outcomes or consequences of the terrorist event or emergency due to the presence of hazardous materials.

C. Know the protocols used to detect the potential presence of Weapons of Mass Destruction (WMD) agents or materials.

- Understand what WMD agents or materials are and the risks associated with these materials in an emergency incident.
- Know the indicators and effects of WMD on individuals and property. Be able to recognize signs and symptoms common to initial victims of a WMD-related incident.
- Know the physical characteristics or properties of WMD agents or materials that could be reported by victims or other persons at the scene.
- Be familiar with the potential uses and means of delivery of WMD agents or materials.
- Know locations or properties that could become targets for persons using WMD agents or materials.
- Recognize unusual trends or characteristics which might be pre-incident indicators or an actual event involving WMD agents, destructive devices or materials.

D. Know and follow self-protection measures for WMD events and hazardous materials events.

- Understand the hazards and risks to individuals and property associated with WMD agents and hazardous materials. Recognize the signs and symptoms of exposure to WMD agents and hazardous materials.
- Understand the requirements and proper use of personal protective equipment (PPE) which may be issued to the responder. Understand the limitations of this equipment in protecting someone exposed to WMD agents or hazardous materials.
- Understand the purpose and types of decontamination, the importance of isolating contaminated persons from those who are not contaminated, and tactical considerations during the decontamination process.
- Understand the roles of different types of first responders, as well as other levels of response in preventing and preparing for an emergency as well as emergency responses.

- Be familiar with his agency's emergency plan and procedures, the individual officer's role in those procedures, the Incident Command System (ICS), and integration of the FBI into the event.
- Know what defensive measures to take during a WMD or hazardous materials incident to help ensure personal and community safety through the ATAC and Joint Terrorism Task Force (JTTF) concepts.

E. Know procedures for protecting a potential crime scene.

- Understand and implement procedures for protecting evidence and minimizing disturbance of the potential crime scene while protecting others. Understand the roles, responsibilities, and jurisdictions, of federal agencies related to a WMD event.
- Protect physical evidence such as bomb fragments, contaminated clothing, relevant containers, and other potential evidence items.
- Recognize witnesses and bystanders and document for later interviewing.

F. Know and follow agency/organization's scene security and control procedures for WMD and hazardous material events.

- Understand the agency/organization's site security and scene control procedures for awareness level trained personnel. Follow these procedures for ensuring scene security and for keeping unauthorized persons away from the scene and adjacent hazardous areas. Such procedures include cordoning off the area to prevent anyone from inadvertently entering the scene. Maintain scene security and control until a higher authority arrives at the scene.
- Be familiar with the agency's incident command procedures.
- Know and follow the agency's procedures for isolating the danger area. Know how to deal with contaminated victims until a higher authority arrives.
- Recognize that the incident or event scene may be a crime scene and that evidence must be protected and undisturbed until a higher authority arrives and takes control.

G. Possess and know how to properly use equipment to contact a dispatcher or higher authorities to report information collected at the scene and to request additional assistance or emergency personnel.

- Understand the need to contact the dispatcher or higher authorities to apprise them of a situation, at the scene, and to request additional assistance and personnel to properly deal with the event.
- Understand how to accurately describe a WMD event.
- Have an awareness of the available emergency assets within the affected jurisdiction(s) nearest the event location.
- Know when to request additional help and follow the agency's emergency plan procedures for establishing incident command
- Know how to notify the communications center or dispatcher and to assess the degree of hazard to obtain appropriate additional resources.

VI. Course delivery with budget constraints

PATRIOT was developed and delivered utilizing the Fiscal Year 2003 funding allotted to each U.S. Attorney's Office. Acknowledging that additional ATAC monies will be unavailable in the foreseeable future, districts need to utilize innovative strategies to deliver the training. Given that the PATRIOT curriculum templates are already developed, only specific geographic content tailoring and future updates are needed to adapt the program to any federal judicial district. Of course, partnership with other key federal, state, and local agencies is both a key to cost efficiency, as well as a significant program goal in itself.

The incentive for partner agencies to provide instructors free-of-charge is a relatively easy and highly credible venue to educate first responders about particular capabilities and services. With many agencies working together, no one agency has to do too much, and instructors need only attend the sessions for which they are responsible. PATRIOT is also a way for partner agencies to satisfy any outside training requirements their agencies may have.

Teamwork and closer relationships are also built through pro bono use of public facilities for classrooms and other training space. For example,

when a local government allows free use of its community civic center, everyone is seen as contributing to the global war on terrorism in a team effort.

Printing course book materials typically is the most significant cost concern. In Mississippi, this issue was satisfied by one of the primary training partners, the Mississippi State Department of Health. Since the course included significant Health Department training, conducted by Health Department personnel, the Department allowed use of its in-house printing shop, and the only expense for other partners was the cost of paper. This example of partnership provided a dramatic cost savings while also helping create closer relationships between the partner agencies.

Distributing the course book appendices on a computer compact disc can also reduce printing costs. While the entire course book could be reduced to compact disc, it is highly recommended that at least the PowerPoint classroom handout sheets be printed, so students may refer to prior slides in class. Of course, if the class size is small enough, a district might opt to photocopy the materials on its own in-house equipment. However, it is strongly recommended to use an agency partner's in-house printer if the above arrangement is possible in your jurisdiction.

ATACs should consult LECC managers, budget/procurement specialists, and ethics advisors to determine an appropriate process for funding remaining expenses. A local agency or agency association may be willing to cover course materials and refreshments for a nominal fee. Depending on the expected size of the class and local government constraints, it may be possible for a local agency or agency association to serve as a sponsor and supply basic light refreshments. The program agenda for each training session should then credit these agencies for their service and commitment.

VII. Program completion and availability

Work presently is underway to develop a "train-the-trainer" package for PATRIOT. Included in the complete course package will be an electronic copy of each template needed to successfully tailor and deliver PATRIOT to audiences in any federal judicial district. Included will be the following materials:

A. Overview/production notes

- Organizing Partnerships
- Recruiting Tips
- Site Location
- Working on a "Shoe String" or on a "Next-to-Nothing" Budget
- Choosing Sites
- Publicizing

B. Promotional products

- Brochure/Registration Form
- E-mail/FAX Promo Flyer

C. Registration

- Sign-in Sheet
- "ID Required" Table Tent
- Name Tags

D. Press packet

- Program "Kick-Off" Sample Release
- Training On-Site Sample Release
- Tips on Working with Media
- Sample Video Clips
- Sample Press Clippings

E. Classroom posters

- JTTF/ATAC Comparison
- Sponsoring Agencies
- Title Poster
- State Map of Training Sites

F. Handouts and information table

- ROCIC Publications (The Regional Organized Crime Information Center is a component of RISS, the Regional Information Sharing System)
- Information Table Tent
- Tips on Potential Agency Publications, etc.

G. Textbook inserts

- Color Cover & Spine
- Color Front page
- Front Text Sample Materials (Agenda, Contents, Key Contacts, etc)
- Supporting Articles
- Appendices

H. PowerPoint slides

- CD-ROM in numeric module order
- Instructor notes for PowerPoint slides

I. DVD set with videos of seasoned instructors teaching each module

J. Completion Certificate

Instructor notes for PowerPoint slides are being generated as of this writing, and will be available in the near future. Additionally, the course will be submitted to the Office of Domestic Preparedness for ODP certification. It is the opinion of course developers that a partnership between the key players of the ATACs, the professional education infrastructure of the ODP, and the Department's Office of Legal Education, is the best way to give IMPACT maximum availability and ease of accessibility.

Should an organization be interested in the PATRIOT curriculum, this sixteen-hour course is easily adapted for training sponsors, such as ATACs, State Departments of Homeland Security, or other organizations interested in cohesive and joint training geared toward prevention, interdiction, and coordination of first responders. The course's template can be tailored and adapted to the needs and realities of any jurisdiction. For further information, contact David Crews or Paul Rowlett in the Northern District of Mississippi at (662) 234-3351, or Stan Harris or Max Fenn in the Southern District of Mississippi at (601) 965-4480.❖

ABOUT THE AUTHORS

❑**Jim Greenlee** serves as the US Attorney for the Northern District of Mississippi. Prior to his appointment, he served as an AUSA in the district for fourteen years.

❑**David Crews** serves as the LECC Coordinator and ATAC Chief Information Officer for the Northern District of Mississippi. Prior to assuming that position, he was a U.S. Marshal.

❑**Tom Bartlett** serves as the Anti-Terrorism coordinator for the Southern Regional Public Safety Institute in Long Beach, MS. He is a certified DOD/DOJ HAZMAT instructor.

❑**Max Fenn** serves as the Intelligence Research Specialist for the Southern District of Mississippi. Prior to his assignment in 2002, he served seventeen years in the military, with tours in U.S. Marine Force Reconnaissance and U.S. Army Special Forces.✠

IMPACT—Intensive Marine Port Area Counter-Terrorism Program

Stan Harris
First Assistant United States Attorney
United States Attorney's Office
Southern District of Mississippi

Max Fenn
Intelligence Research Specialist
United States Attorney's Office
Southern District of Mississippi

Robert J. Arndt
Port Security Specialist
U.S. Coast Guard Marine Safety Office
Mobile, Alabama

Tom Bartlett
Anti-Terrorism Coordinator
Southern Regional Public Safety Institute (SRPSI)
Long Beach, Mississippi
(SRPSI is a division of the University of Southern Mississippi and the Harrison County Sheriff's Department.)

I. Introduction

The attacks on the *U.S.S. Cole* and those of 9/11 illustrate the susceptibility of maritime ports to direct attack, and to the illegal movement of people and material supporting terrorist and criminal activity. Additionally, the use of lawful materials (e.g., fertilizer bombs) in domestic terrorism, frequent attempts to steal anhydrous ammonia, and other increasing risks to port area infrastructure, have made safeguarding our ports one of the top national priorities.

The specialized issue and limited resource challenges facing maritime ports show a critical need for teamwork among health, safety, and security professionals. If these entities work together to share pertinent information, ports will be better equipped to prevent terrorist threats.

The Intensive Marine Port Area Counter-Terrorism Program (IMPACT) is a field-delivery training program focused on pre-incident indicators and prevention. The course was developed through a cooperative effort between the Coast Guard Marine Safety Office (MSO) in Mobile, Alabama, and the Anti-Terrorism Advisory Councils (ATACs) of the Southern District of Alabama, the Northern District of Florida, and the Northern and Southern Districts of Mississippi. Mobile's MSO Northeast Gulf of Mexico Regional Maritime Security Committee includes representatives from each of the ATACs, and has subcommittees which represent each of the major port areas in these federal judicial districts.

After the success of the Preventive Anti-Terrorism Recognition and Interdiction Operational Techniques (PATRIOT) Program in Mississippi, the ATACs decided to use remaining Fiscal Year 2003 funds to implement IMPACT. The course was designed for:

- port health, safety, and security professionals;
- security guards;
- dispatchers, and managers of public and private facilities;
- fire, health, haz-mat, and emergency managers; and
- law enforcement officers.

IMPACT was intended to meet specific needs of both coastal and inland maritime ports. The course may be taught alone or in conjunction with PATRIOT training. IMPACT trains port area professionals to work together to implement key prevention principles. They are taught what to look for, whom to contact, and how to report suspicious activity. The training is cooperatively sponsored by federal, state, and local governments, and is offered free of charge. While the program also enjoys strong private sector cooperation, it has not accepted private financial support.

IMPACT's team of multi-disciplinary federal, state, and local officials provide an overview of new regulations under the Maritime Transportation Security Act, Pub. L. No. 107-295, 116 Stat. 2064, and they teach others how to recognize terrorist conduct, potential local targets,

terrorist weapons, and pre-incident indicators. They also teach basic prevention and interdiction steps to help avoid or minimize a successful terrorist attack against targets in a local port area.

Participants who complete both days of instruction receive a multi-agency certificate of completion. In addition, continuing education (CE) credit may be available from participating state certification agencies.

II. Development and delivery

The IMPACT program was designed to promote information sharing, one of the vital keys in preventing terrorism. It was developed as a result of extensive research into existing government training programs and national standards, and the program became the first counterterrorism course of its kind specifically tailored to educate first responders and private security professionals. Previously, no government field training counterterrorism program existed in which all first responders and private security professionals could train together with an emphasis on prevention. With broad use of partnerships and funding from the ATACs, IMPACT was able to overcome the initial challenges of finding funding, gaining agency support, preparing instructors, producing course materials, and arranging training schedules and locations.

In September 2003 a two-day format was designed in order to conform to agency funding constraints and personnel logistics. Typically, two days is the most training time a first responder agency can devote for significant numbers of its personnel. The IMPACT curriculum was designed to compliment PATRIOT and a student can profitably attend both programs. PATRIOT is a general counterterrorism training program; IMPACT focuses on the issues unique to maritime port areas.

Tom Bartlett, the Antiterrorism Coordinator for the Southern Regional Public Safety Institute, served as the IMPACT professional course developer. Tom is a longtime law enforcement officer who has also served as a fireman, an emergency medical technician, and a haz-mat team leader. He served on the adjunct staff of the Center for Domestic Preparedness and taught for the Department of Defense before serving as a developer and instructor for the PATRIOT Program. His wealth of knowledge and experience has contributed to the success of IMPACT.

In November 2003 the full sixteen-hour IMPACT program was presented to a thirty member review panel comprised of federal, state, and local agencies, as well as private sector security professionals, who critiqued a "dress rehearsal" of the entire two-day curriculum. After incorporating the panel's changes into the curriculum, the course was presented from November 2003 to January 2004 in:

- Mobile, Alabama;
- Panama City, Florida;
- Pensacola, Florida;
- Gulfport, Mississippi;
- Pascagoula, Mississippi; and
- Vicksburg, Mississippi.

Sixty-seven percent of the 400 participants were federal, state, and local government employees. The participants included:

- law enforcement officers;
- fire fighters;
- emergency medical service personnel;
- haz-mat teams;
- 911 operators;
- military security and force protection professionals; and
- emergency management officials.

Approximately 33 percent of the students were security professionals from private industry. Since the course did not include members of the general public, IMPACT highlights existing Coast Guard instructional programs, such as the "Community Coastal Watch Program" in Mobile, which are specifically designed to reach out to community groups and individual members of the public.

The sixteen-hour original version of IMPACT accomplishes the goal of creating flexible, scalable, exportable, field-level training, directed toward first responders, security managers, and industry personnel. In subsequent versions, the program can be useful to other specific audiences.

In February 2004 the Coast Guard's Northeast Gulf Coast Regional Committee put together an IMPACT Task Force to review and refine IMPACT's curriculum in order to continue and expand the program. The task force is also

looking into the possibility of releasing a specifically tailored eight-hour version of the course for port line security officers.

A team of IMPACT developers traveled to Washington, D.C., and provided special briefings to the CTS, the Office of Domestic Preparedness (ODP), and the Training Committee of the U.S. Maritime Administration (MARAD). Some of the key developmental issues that made IMPACT a success include:

- comprehensive information collection;
- intensive curriculum development involving real-world officials;
- full dress rehearsal and workshop;
- evaluator presentations; and
- ongoing refinements.

Furthermore, the program accomplished its goals by successfully recruiting local agents as instructors, creating a flexible and adaptable program, and making the course proactive rather than reactive. IMPACT proved to be cost effective, and it encouraged government and private industry interaction, as well as interagency cooperation. Despite initial challenges, the hard work of team members and ATAC funding made IMPACT surpass the expectations of the students, faculty, and reviewers.

III. The development/evaluation/sponsorship team

The quality of the course was made possible due to diligent support and feedback from the many agencies listed below. Representatives from the following agencies and departments participated in the development of IMPACT by helping to serve as contributors, evaluators, sponsors, and/or instructors:

- the U.S. Air Force;
- the Amtrak Police;
- the U.S. Army Corps of Engineers;
- the U.S. Attorneys' Offices;
- Anti-Terrorism Advisory Councils and Law Enforcement Coordinating Committees of the Southern District of Alabama;
- the Northern District of Florida;
- the Northern and Southern Districts of Mississippi;
- the District of Vermont;
- the U.S. Coast Guard;
- the U.S. Coast Guard Haz-Mat Strike Team;
- U.S. Customs and Border Protection;
- the Office of Domestic Preparedness (including the Center for Domestic Preparedness);
- the Federal Bureau of Investigation;
- U.S. Immigration and Customs Enforcement;
- the U.S. Maritime Administration (MARAD);
- the U.S. Marshals Service;
- the Naval Criminal Investigative Service;
- the Regional Information Sharing System (RISS) and its Regional Organized Crime Information Center (ROCIC);
- State and Local Anti-Terrorism Training (SLATT) (a division of the Institute of Intergovernmental Research and funded by the Bureau of Justice Assistance);
- the Transportation Security Administration;
- the Alabama Peace Officers Standards and Training Commission;
- the Alabama Department of Transportation;
- the Alabama Marine Police; the Alabama Department of Public Health;
- the Alabama State Port Authority;
- the Mobile County Emergency Management Agency;
- the City of Mobile;
- the Mobile Fire and Rescue Department;
- the Mobile Police Department;
- the Florida Department of Law Enforcement;
- the Florida Emergency Management Agency;
- the Florida Department of Health;
- the Florida Department of Transportation;
- the Florida Fish and Wildlife Commission;
- the International Port School of the University of Southern Mississippi;
- the Mississippi Attorney General's Office;

- the Mississippi Emergency Management Agency;
- the Mississippi Department of Environmental Quality;
- the Mississippi Department of Health;
- the Mississippi National Guard;
- the Mississippi State Fire Academy;
- the Mississippi Gaming Commission;
- the Mississippi Department of Marine Resources;
- the Mississippi Department of Public Safety (including the Mississippi Highway Patrol and Peace Officer Standards & Training);
- the Mississippi Department of Transportation;
- the Mississippi Department of Wildlife, Fisheries & Parks;
- the Mississippi Water Resources Commission;
- the State Port at Gulfport;
- the Port of Pascagoula;
- P & O Ports;
- the Tennessee-Tombigbee Waterway Authority;
- the Southern Regional Public Safety Institute;
- the Harrison County Sheriff's Department;
- Signal International;
- the Kansas City Southern Railroad Police;
- the Mississippi Security Police; and
- Swetman Security.

IV. Course overview

This sixteen-hour training program is presented for members of a port area's health, safety, and security community; for security guards, dispatchers, and managers of public and private facilities; for fire, health, haz-mat, and emergency managers; and for law enforcement officers. By training these professionals together, IMPACT helps build not only a sense of community, but it also enhances the knowledge and understanding necessary in counterterrorism networks.

A. Primary objective

IMPACT's primary objective is to prevent terrorism by enhancing awareness and reducing vulnerabilities in coastal and river port area security. In particular, IMPACT focuses on security requirements of the Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064. The course is designed to jointly train members of the port area security community, and it should receive substantial support from port area professionals.

B. Documents

During the course, instructors distribute a course manual and/or compact disc containing instructional material. Additionally, a variety of handouts and supplementary materials are made available.

C. Proceedings

IMPACT consists of fifteen training modules. The course material is presented by agencies such as the U.S. Coast Guard, U.S. Immigration & Customs Enforcement, the Federal Bureau of Investigation, State Marine Law Enforcement, and others. The course includes exercises at the close of each day, with a two-hour port area tour conducted prior to an Incident Management Session.

D. Course justification

Foreign and domestic terrorist groups and other criminals pose significant threats to political and economic systems in the United States and its Marine Transportation System (MTS). With the integration and worldwide interdependence of national economies, improvements in commercial transportation infrastructure, and modalities to facilitate international trade, terrorist and criminal organizations can operate on an international scale and increase the volume, speed, and efficiency of illegal transactions. Any terrorist group can easily exploit intelligence failures by selecting a port that does not have the intelligence network, technology, and interdiction capabilities, of other ports.

A security failure could result in direct threats to the economic and trade interests of the United States. Therefore, it is essential for the United States, and her maritime trading partners, to reduce criminal and terrorist exploitation of commerce in the international maritime trade corridors by improving port and cargo security.

Continued training each year is necessary to implement new regulations and training requirements. Acquiring funding can be a difficult prospect for both government and private industry. The cost-effective success of the IMPACT training initiative depends on the cooperative engagement of area ports and government agencies, as well as private sector stakeholders with interests in port and transportation systems.

E. Terrorist threats

This module is current, can be regularly updated, and is applicable to both cargo and cruise port operations. Details are provided on how to analyze a terrorist threat, and how to identify the terrorist mind-set, methods of operation, motivations of terrorists, and characteristics of transnational terrorist organizations. Additionally, money laundering, cigarette smuggling, and other crimes that support terrorist financing are discussed.

F. Terrorist weapon recognition

This segment helps participants recognize terrorist instruments such as weapons of mass destruction (WMD) and conventional explosives. The characteristics of explosive materials such as bomb components, precursor chemicals, reagents, and dissemination devices are presented. Additionally, trainees are taught to detect, as well as to self-protect against three types of WMD, radiation dispersal devices (RDD), biological weapons, and chemical weapons.

G. Security challenges

Importation of terrorists, WMD, and other contraband are the most pervasive threats facing ports. The economic importance of ports and the MTS cannot be overlooked, and systems for continuously monitoring and challenging personnel working in the port are the basic tools to counter internal conspiracies. Access control, physical security measures, and the involvement of multiple agencies contribute to this task. The Department of Homeland Security (DHS) is having a positive impact on these issues and IMPACT highlights key DHS changes.

H. Vulnerability assessment

IMPACT instruction centers on the examination of threats, and weighing those threats against port security and MTS vulnerabilities. Techniques of categorizing and prioritizing security threats are presented, and a risk assessment matrix is demonstrated and discussed. Further, contingency planning for the development of prevention and response operations is explained.

I. Physical security

Port security guidelines are important to the development of physical security and access controls. By addressing such services as port signage, local law enforcement agency supports, badge systems, port gate operations, cruise ship terminal operations, and the inbound and outbound escort of tanker trucks, the system allows certain matters in the port to be documented and routed to the appropriate department for response.

J. Personnel protective equipment and decontamination

Personal Protective Equipment (PPE) and Decontamination (DECON) is necessary during port security interdiction operations that involve a potential or actual haz-mat issue or WMD. This module provides introduction to the proper understanding, selection, and use of PPE and, more importantly, it advises what not to do in threatening situations. Tactical planning for implementation of emergency decontamination in the event of a terrorist weapon interdiction is a key component of this module.

K. Port protective operations

Port security operations conducted by government authorities or private sector firms present significantly different limitations, and security depends on adherence to documented policies and procedures.

L. Cargo security

Various situations involving contraband, concealment techniques, unregistered containers, precursor chemicals, cargo discrepancies, diversion techniques, fraudulent documentation, and cargo theft are addressed in this module. Profiling characteristics and related issues are also examined.

M. Container interdiction

Computerized identification systems, x-ray scanners, random vessel inspections, seal tampering detection, and other types of detectors installed in surface traffic lanes have the potential for detection of WMD and terrorist smuggling.

X-ray, gamma-ray, scanning, random vessel inspections, dangerous cargo manifests, VICAS, GPS, E-Seals, RFID tags/stickers, seal tampering detection, and other prevention techniques are discussed.

N. Immigration fraud

Stowaways and illegal immigration present grave threats to port security. These threats can be mitigated by improving monitoring procedures for freight carriers, cruise liners, and cargo ships. Prevention of illegal immigration, illegal export of currency, and abuse of controlled goods, can be better improved by methods similar to those used against drug smuggling.

O. Document fraud

The manufacturing, obtaining, and possession of fraudulent documents are similar threats to port security, which can be mitigated by superior monitoring procedures. This crime can be countered with systems and measures that range from detecting forged/false personal documentation in the port area, to helping prevent the hijacking of shipments in road/rail transit after goods leave the port.

P. Port tour field trip

The two-hour port tour is made possible by the combined effort of senior management officials from the host port, the Coast Guard, representatives of port area industries, and other agency officials. The tour is an ideal opportunity to highlight the unique aspects of particular ports. During the tour, key agency officials and industry representatives sit near the front of the bus, and use the public address system to speak to the group when the bus nears areas of their expertise. Even professionals who have spent many years working in one facility of a port area may have little knowledge of other areas of the port.

The tour is another excellent opportunity to discuss local information-sharing network opportunities. Technical insight is often gained from observation of participants. Most students agree that the port tour is one of the best parts of the field training program.

Q. Incident management

The National Incident Management System (NIMS), the Unified Command System used during a terrorist or weapon interdiction operation or emergency response, Crisis Management response, and Coast Guard and National Response Team integration are discussed during this module. The module may be taught by a representative of the State Emergency Management Agency.

R. Prevention and incident scenarios/interactive panel-led exercises

During this session a fictional terrorist incident is presented to foster interactive discussion regarding strategies and tactical considerations during the response. Total time allotted for these exercises should be one hour at the end of each day.

S. Certificates and closing comments

It is important to gather course evaluations from students prior to issuing certificates. Evaluations should always be reviewed in an "after action" process.

T. Handouts and resource material

Materials can be obtained from the Regional Information Sharing System (RISS) and from sponsoring agencies. An effective way to emphasize key information is to have tables set up for material distribution, and visible posters displayed throughout the training area.

U. Scheduled media opportunity

Press releases are an effective way to distribute information regarding the schedule and location of training sessions. Media opportunities may be used to promote public awareness of the Coast Guard and its programs.

V. Train-the-trainer products

A complete "train-the-trainer" package is currently being developed. The training package will include information sets and templates for the following:

- color promotional brochure;
- registration kit with name tags;
- classroom posters;
- PowerPoint slides with instructor notes;
- media kit;
- completion certificates;
- digital video disc set with video of seasoned instructors teaching each module;
- student course book; and
- RISS and other suggested handouts.

VI. Contacts

Roy Sawyer (SD AL): (251) 415-7166
John Peaden (ND FL): (850) 444-4000
Ginger Golden-Bouk (ND FL): (850) 444-4008
Dave Crews (ND Miss): (662) 238-7671
Max Fenn (SD Miss): (601) 973-2841

VII. Conclusion

As noted, the Coast Guard's Northeast Gulf of Mexico Regional Maritime Security Committee presently has a task force reviewing IMPACT and working with ATACs to create a train-the-trainer package and other templates targeted at specific audiences. These will include up-to-date and improved, "user friendly" curriculum modules. The task force is also making recommendations regarding IMPACT's potential to serve as a template for port security partnership training in other jurisdictions.

The program is thought to be flexible enough to adapt to all local areas, and has proven effective in creating bonds between federal, state and local agencies, industry, and private-sector communities. IMPACT will soon be presented to the (ODP) for official ODP course certification.

IMPACT's goal of partnering communities for prevention and sharing information can be achieved with great benefit to those who participate. It is necessary to use every available and appropriate tool to prevent future terrorist acts. In so doing, many agencies are finding that closer relationships and better information sharing are already having a tremendous impact on their daily activities in the real world of maritime ports.❖

ABOUT THE AUTHORS

❑**Stan Harris** began service as First Assistant United States Attorney for the Southern District of Mississippi on October 23, 2001. Harris serves as Chief-of-Staff for U.S. Attorney Dunn Lampton, and serves as the Southern District's Anti-Terrorism Coordinator.

Mr. Harris formerly served as Chief Counsel and Deputy Chief-of-Staff for Senator Trent Lott, Minority Leader of the U.S. Senate.

Mr. Harris has handled cases and projects involving virtually every federal department and agency, and has received numerous commendations for work on behalf of local, county, state and federal government.

❑**Max Fenn** serves as the Intelligence Research Specialist for the Southern District of Mississippi. Prior to his assignment in 2002, he served seventeen years in the military, with tours in U.S. Marine Force Reconnaissance and U.S. Army Special Forces.

❑**Robert J. Arndt** serves as the Port Security Specialist for the U.S. Coast Guard Marine Safety Office in Mobile, Alabama.

❑**Tom Bartlett** serves as the Anti-Terrorism Coordinator for the Southern Regional Public Safety Institute (SRPSI) in Long Beach, Mississippi (SRPSI is a division of the University of Southern Mississippi and the Harrison County Sheriff's Department). He is a certified DOD/DOJ HAZMAT instructor. ✠

State and Local Anti-Terrorism Training (SLATT) Program

Domingo S. Herraiz
Director, Bureau of Justice Assistance
Office of Justice Programs
Department of Justice

The State and Local Anti-Terrorism Training (SLATT) Program is funded by the United States Department of Justice, Bureau of Justice Assistance (BJA), through a grant to the Institute for Intergovernmental Research (IIR) in cooperation with the Federal Bureau of Investigation. It is a training and research program providing pre-incident awareness, preparation, investigation, prevention, and interdiction training

and information to state and local law enforcement in the areas of terrorist and criminal extremist activity. This focus distinguishes SLATT from "first responder" and other related weapons of mass destruction/nuclear, biological, chemical, and radiological response training provided to emergency service personnel.

The SLATT Program was implemented in 1996 in response to the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, and the rising militia movement in the United States. At the time of its introduction, responding to pressing concerns, SLATT focused primarily on domestic terrorism and special-interest/single-issue extremist groups. However, as the new millennium approached, officials recognized the need to broaden the program's scope. Research and training topics were added, including the threat of foreign-inspired terrorism on American soil. Unfortunately, the need to share this expertise was called on within the span of a few short years.

On September 11, 2001, America entered a new phase in the fight against terrorism. The SLATT Program was poised and ready to address most current, critical counterterrorism issues, such as detection, intervention, investigation, and prevention. SLATT quickly increased training offerings in foreign-inspired terrorism, encompassing specific groups and organizations believed to be involved in the attacks. In addition to the increased training emphasis on foreign-inspired terrorism, SLATT research also identified an increase in violent acts linked to certain special-interest groups. Once again, SLATT course offerings were increased to address this emerging area as well.

A key challenge in addressing counterterrorism efforts was the realization that America's law enforcement was facing a new enemy. Unlike traditional criminals that are often driven either by greed or emotion, terrorists are driven by ideology. This necessitates a different approach in investigation, infiltration, and intervention, as well as an increased need to share information and intelligence. It also requires different skills than those needed to battle more traditional criminals. When state and local law enforcement became the front line in protecting the homeland, the skill sets and training necessary for success became even more imperative.

Because SLATT is an investigation and prevention-oriented counterterrorism training program, the demand for SLATT workshops increased dramatically following the 9/11 attacks. With over 20,000 law enforcement agencies employing in excess of 650,000 officers, the task of responding to all training requests and providing counterterrorism training to every officer became a daunting challenge.

In an effort to get critical counterterrorism training information to the field in a timely fashion, specialized SLATT workshops were developed for, and delivered through, the United States Attorneys' Offices (USAOs), the Regional Information Sharing Systems (RISS) Intelligence Centers, state police chief and sheriffs' associations, and other law enforcement organizations. Over 40,000 law enforcement professionals have been trained across the country, with more than 3,400 individuals trained during specialized workshops conducted for the USAOs, and over 3,000 trained through the RISS centers during annual conferences.

In addition, BJA requested that a SLATT Train-the-Trainer program be developed to enhance the multiplying effect of delivering basic terrorism orientation and awareness training. A focus group of subject-matter experts, experienced police trainers, and some of the nation's leading criminal justice academics, was convened to assist in identifying the basic elements necessary for a successful terrorism Train-the-Trainer program. As a result of this feedback, a complete Train-the-Trainer package was assembled consisting of over 350 PowerPoint slides, lesson plans, learning objectives, and four CDs of video clips, to offer a complete program necessary for the success of this critical effort. Delivery of these workshops began in late 2002.

As of March 2004, fifteen Train-the-Trainer workshops have been delivered to almost 700 experienced law enforcement trainers from the Federal Bureau of Investigation, Regional Community Policing Institutes, criminal justice training academies, and state and local law enforcement agencies. These trainers have, in turn, trained over 73,000 officers nationwide. The multiplying effect of this training effort is staggering. The SLATT Train-the-Trainer program has been very successful in delivering a valuable and constantly changing training tool for law enforcement. Successful participants of this program are given access to a secure Web site

where updated presentation materials are available in order to assist the trainer in presenting the most up-to-date material, and to leverage the research capabilities of the SLATT research unit.

Because the needs vary in relation to threat, groups, resources, and geography, SLATT offers various training formats in order to effectively respond to state and local law enforcement needs. These include, but are not limited to:

Investigative/Intelligence Workshops

Designed for state and local law enforcement investigators, intelligence officers, and analytical personnel, this workshop includes topics related to the unique aspects inherent in the investigation and prosecution of terrorist and criminal extremist activity. This workshop is four days and includes topics such as:

- Terrorism Overview;
- Investigating Religious Terrorism;
- International Terrorism and Extremism Groups;
- Domestic Terrorism;
- Understanding the Terrorist Mindset;
- Terrorist Financing;
- Interview Techniques;
- Special-Interest/Single-Issue Terrorism;
- Explosives and Explosive Devices; and
- Role of Intelligence.

Specialized Training Events

This training is designed to provide an effective, flexible response to state and local law enforcement training needs. Training topics, locale, and course length are tailored to the specific requirements of the requesting agency. Course length typically varies from four hours to two days.

Train-the-Trainer Workshops

Designed for qualified law enforcement trainers, this workshop is intended to assist agencies in developing in-house counterterrorism training capabilities, and provides law enforcement trainers with the ability and information (i.e., lesson plans, sample notebooks, presentation materials, reference materials, etc.) to train other law enforcement personnel. This workshop is two days and includes topics such as:

- Terrorism Overview;
- Law Enforcement Roles;
- Domestic Terrorism;
- International Terrorism;
- Terrorism Indicators;
- Officer Safety Issues; and
- Community Partnerships.

Narcotics Task Force Antiterrorism Briefings

Designed for multijurisdictional narcotics task force personnel, this briefing combines terrorism awareness and investigative training with the expertise, experience, and contacts of narcotics task force groups to aid in the investigation, interdiction, and prevention of terrorist- and extremist-related crimes. This briefing is eight hours and includes topics such as:

- Introduction—Why Narcotics Officers;
- Terrorism: What Is the Threat;
- Recognizing Terrorist Indicators and Warning Signs;
- Explosives and Explosive Devices;
- Officer Safety Issues;
- Who Is Responsible for Follow-Up?; and
- The Future.

Discovering, monitoring, and delivering the most current terrorism-related information is integral to the mission of the SLATT Program. To that end, the SLATT research component is critical, providing ongoing research on terrorist groups and ideologies; criminal extremist movements, strategies, alliances, goals, trends, and threat potential; and other related areas. SLATT researchers rely upon public databases and media scans. SLATT research supports the information and training needs of the program. It makes analyzed information obtained from the public domain available through its products, which include:

- Specialized publications;
- Chronologies of terrorist events;
- Resource CDs (over 18,000 distributed since January 2002); and

- Other multimedia applications presented via training classes, the RISS secure intranet, and other appropriate means.

Due to the continued high demand for SLATT training since 9/11, requests for assistance are sometimes met most expeditiously and efficiently through the dissemination of these resource materials.

The key to the success of the SLATT Program is a cadre of instructors who possess extensive terrorism-related law enforcement experience at the local, state, and federal levels, many of whom are nationally recognized experts from the academic community. This combination of terrorism-related experience at all levels allows SLATT to combine real-world experience with the continual research necessary in the dynamic area of anti-terrorism training in the 21st century.

SLATT staff also provides specialized support to the Counter-Terrorism Training Coordination Working Group (CTTWG). The CTTWG was established in November 2002 by the Office of Justice Programs' (OJP) Assistant Attorney General to aid law enforcement in meeting the challenges of terrorism in furtherance of the mission of OJP to develop the nation's capacity to prevent and control crime. The Working Group was tasked with analyzing counterterrorism training offered or contemplated by any component of the U.S. Department of Justice (Department), minimizing duplication, identifying training to recommend to the field, and determining the most effective method of delivery. Since its inception, many other agencies have joined the Working Group, and the Group has expanded its focus to include training beyond the offerings of the Department.

A major initiative of the Working Group is the implementation and facilitation of the Criminal Intelligence Training Coordination Strategy (CITCS) Working Group. The mission of the CITCS is to coordinate intelligence training initiatives to avoid conflicting messages, to establish and promote mutually agreed-upon intelligence training objectives, and to further the training goals as outlined in the Global Justice Information Sharing Initiative's *National Criminal Intelligence Sharing Plan*. The CITCS, which functions in cooperation with Global Intelligence Working Group (GIWG) membership, is in the process of coordinating an effort to bring together the various organizations developing or offering intelligence training, in an atmosphere of cooperation, goal identification, and resource sharing, to address federal, state, local, and tribal criminal intelligence training coordination issues. The final product of the CITCS will be a set of intelligence training standards for varying levels of law enforcement that will be presented to the CTTWG, vetted through the GIWG, and presented to the Global Justice Information Sharing Initiative for adoption. These intelligence standards will provide an invaluable tool for law enforcement across the country.

In addition to providing support to the CTTWG and the CITCS Working Group meetings, SLATT staff researches, develops, and provides content management for the CTTWG's Counter-Terrorism Training and Resources for Law Enforcement Web site, http://www.counterterrorismtraining.gov, which provides information on promising couterterrorism initiatives and programs, available technical assistance and training, and other related information.

For additional information about the SLATT Program and related services, please contact Eileen M. Garry at Eileen.Garry@usdoj.gov or slatt@iir.com.❖

ABOUT THE AUTHOR

❑ **Domingo S. Harraiz** was unanimously confirmed by the United States Senate as BJA's new Director on March 8, 2004. President Bush signed his commission on March 9, and he was officially sworn in on March 15. Before joining BJA, he was the Director of the Ohio Office of Criminal Justice Services, the state criminal justice planning agency. From 1986 to 2000, Mr. Herraiz was the Executive Director of the Ohio Crime Prevention Association. While in that position, he served as Executive Committee Chair of the Crime Prevention Coalition of America, where he designed a national crime prevention model and the McGruff the Crime Dog campaign for the Department and the National Crime Prevention Council.✠

First Responders at the Cocoanut Grove Night Club Fire in 1942

Beverly Ann Jones
Employee Assistance Program
Executive Office for United States Attorneys (EOUSA)
Department of Justice

September 11, 2001, gave the world an in-depth look at the heroic but harrowing work that is done by "first responders" every day in this country and around the world. Not a day went by during the first month after 9/11 without millions of people witnessing the brave police officers, firefighters, emergency services workers, excavation teams, medical teams, and mental health teams doing their jobs at Ground Zero or the Pentagon. First responders, and their very critical role, were indelibly engraved into our consciousness after the terrorists' acts. Yet, from time immemorial, there have always been people willing to put their lives on the line to respond to mass tragedies. In the past they were known as rescuers. Their jobs were no less dangerous and no less traumatizing than the brave people who were called to duty almost three years ago. The following is an account of the roles that rescuers or "first responders" played in the Cocoanut Grove Nightclub fire in November 1942.

On November 28, 1942, Holy Cross College played an afternoon football game against Boston College and won. Boston was alive with excitement and with fans celebrating the victory. Many fans from the game were among the 1,000 people reveling at the popular Cocoanut Grove Nightclub in the midtown theater district of Boston. On that night, the club admitted 400 people over its occupancy limit.

The country was in the midst of World War II. Together at the nightclub with the revelers from the football game were Marines, soldiers, sailors, and Coast Guard personnel. There were young men getting ready to join the army for training, military personnel getting ready to be shipped abroad to fight in the war, and military personnel on leave from their units just having fun. There was a wedding party in the club that night, as well as a large number of local hospital personnel.

Shortly after 10:00 p.m., a fire started in the dimly lit basement of the nightclub. A busboy, replacing a light bulb that had been removed as a prank by one of the celebrating patrons, struck a match in order to see the outlet. The match touched one of the artificial palm trees in the bar and flames began to spread throughout the building. Because of the large number of flammable decorations and silk draperies in the club, the fire spread rapidly, engulfing the nightclub.

The nightclub did not have clearly marked emergency exits. The two revolving doors at the front of the building opened inwardly rather than outwardly. In a panic, people attempted to leave the nightclub the same way they had entered. As the hordes moved through the roaring fire in complete darkness, they jammed against the revolving doors. Just about one half of the club patrons escaped the Cocoanut Grove fire. Approximately 492 patrons were killed during the fire. Many others were injured. Near the front entrance of the club, where the doors jammed, witnesses said that bodies were stacked six feet high.

The nightclub had several other exit doors, but the patrons had no knowledge of them. One exit door's panic bar had been welded shut. There were no clear directions to another exit door, which was well-hidden behind decorations and drapes.

A full battalion of rescue workers ("first responders") was called into duty that night. There was a mobilization of police and firefighters. Civil defense personnel (medical personnel) and air raid wardens were asked to maintain order and/or to give first aid to people suffering from smoke inhalation and burns. Soldiers who escaped the fire went to work trying to help with the recovery efforts. Priests participated in the rescue and recovery operation by administering last rites to the dying.

In 1942 rescuers did not have the luxury of modern technology. Fire apparatus and rescue vehicles were parked adjacent to patrons' cars. This slowed down the rescue operation. The

rescue was carried out without cell phones, which had not yet been invented. Much of the communication was done by people willing to go on foot or by car to deliver messages.

Firefighters eventually entered the revolving doors, and found the front area of the night club piled high with bodies. It took firefighters just over an hour to put the fire out completely. Thereafter, they began to remove people from the nightclub. Many of the firefighters were traumatized by the conditions of the bodies they found and by the contorted positions in which they found them. In one account, a firefighter stood screaming hysterically at the sight that unfolded before him.

An article by Roger C. Evans and Rupert Evans, *Accident and Emergency Medicine*, 68 POSTGRADUATE MEDICINE J, 714-34 (1992), describes how deaths from trauma usually happen in one of three distinguishable periods. The "first peak" occurs within seconds/minutes of the injury, where only prevention of the accident could have avoided deaths. The "second peak" happens in the second to fourth hours post injury, ("golden hour") which results in 35% of deaths from trauma in countries with advanced trauma services. The "third peak" occurs several days/weeks after the initial injury where death results from sepsis or multiple organ failure.

Rescuers in 1942 did not have the knowledge about mass traumatic injuries that "first responders" in the study above had. By 1942 Boston, like other cities in the country, had been preparing for war and for soldiers returning home from battle. Boston Massachusetts General and Boston City Hospital had established burn units in preparation for an enemy attack with massive fire and war casualties. The two hospitals had already established wartime protocols. As a result, Massachusetts General Hospital was able to save thirty-nine people who had been in the fire. Boston City Hospital saved 131. Advances in the treatment of fire-related injury and trauma were made because of the treatments administered to survivors of the Cocoanut Grove fire. Some of the procedures and techniques were used in the treatment of injured soldiers returning from the war.

Charles C. Kenney is a retired firefighter who has studied the Cocoanut Grove Nightclub fire. He was a seventeen-year-old sailor in the U.S. Navy on his way to London on that night. His father was a firefighter who helped with rescue on the night of the fire. This writer spoke to Mr. Kenney, who now lives in Harwich, Massachusetts. He recalled talking at length to physicians, firefighters, police officers, and patrons who survived that night. Mr. Kenney recounted how it took firefighters only two to three minutes to respond to the fire because they were just around the corner answering another alarm. He believes that his father, like other rescuers, put everything on "automatic" and went to work doing their jobs "clinically" and "dispassionately." It was only later that he believes they experienced "depression" and other traumatic symptoms.

While Boston City Hospital and Massachusetts General Hospital saw most of the patients, other patients were being transported by ambulances and taxis to emergency facilities. Emergency facilities and hospitals were forced to design makeshift morgues to accommodate the dead. Because of the sheer number of dead, some medical staff refused to begin counting them until the next morning. Garages were used as temporary morgues. Witnesses reported that the huge concrete bays were emptied of vehicles and filled with the deceased.

This is from a commentary that Bernard De Voto wrote about the Cocoanut Grove Nightclub fire for Harper's [Magazine] in "The Uneasy Chair," February 1943:

> The fire at the Cocoanut Grove was a single, limited disaster, but it exhausted Boston's capacity to deal with an emergency. Hospital facilities were strained to the limit and somewhat beyond it. If a second emergency had to be dealt with at the same time its victims would have had to wait some hours for transportation and a good many hours for treatment. If there had been three such fires at once, two-thirds of the victims would have got no treatment whatever in time to do them any good. Boston is an inflammable city and it has now had instruction in what to expect if a dozen hostile planes should come over and succeed in dropping incendiary bombs. The civilian defense agencies which were called on justified themselves and vindicated their training. The Nurses' Aid in particular did a memorable job; within a few hours there was a trained person at the bed of every victim, many other Aids worked to exhaustion helping hospital staffs do their jobs, and in

> fact more were available than could be put to use. Nevertheless it was clearly demonstrated that the civilian agencies are nowhere near large enough to take care of bombings if bombings should come. There were simply not enough ambulances: Railway Express Company trucks had to be called on to take the injured to hospitals and the dead to morgues. The dead had to be stacked like cord wood in garages because the morgues could take no more; the dying had to be laid in rows in the corridors of hospitals because the emergency wards were full. The drainage of doctors into the military service had left Boston just about enough to care for as many victims as this single fire supplied. Six months from now there will be too few to handle an equal emergency; there are far too few now for one twice as serious. One plane-load of incendiaries would start more fires than the fire department and its civilian assistants could put out. There would be more injured than there are even the most casually trained first-aids to care for. Hundreds would be abandoned to the ignorant assistance of untrained persons, in streets so blocked by rubble and so jammed with military vehicles that trained crews could not reach them even when trained crews should be free. Boston has learned that it is not prepared to take care of itself. One doubts if any community in the United States is.

Id. at 334.

Boston was in no way prepared for the tragedy that took place at the Cocoanut Grove Nightclub. The fire was unprecedented and resulted in the worst loss of life in a fire in the history of the city of Boston. The club had no fireproof fixtures. It had neither a sprinkler system nor clearly marked exits. At the time, Boston's legal occupancy laws were not applicable to nightclubs. The fire led to major fire prevention efforts and to the imposition of controls for places where large numbers of people gathered. The disaster led to modern fire code regulations as part of what was called the "Life Safety Code." Emergency lighting, exit lights, and occupant safety capacity were required by law. New fire codes were implemented which included the elimination of certain flammable decorations. There was a requirement that doors in such an establishment had to open outwardly. Laws also eliminated smoking in theaters.

Although the fire was not set intentionally, people were angry because there was a feeling that this was a disaster that was caused by negligence, and that it could have been avoided. The busboy was blamed, but a bigger blame was placed on those whose responsibility it was to take deliberate measures to save lives.

De Voto further comments:

> Deeper implications of the disaster have no direct connections with the war. An outraged city has been confronting certain matters which it ordinarily disregards. As a place of entertainment the Cocoanut Grove was garish but innocuous and on the whole useful. It had been called "'the poor man's Ritz;'" for years people had been going there to have a good time and had got what they were looking for. With the naive shock customary in such cases, the city has now discovered that these people were not receiving the minimum protection in their pleasures to which they were entitled and which they supposed they were receiving. . . . For the responsibility is the public's all along and the certain safeguard—a small amount of alertness, civic courage and willingness to lose some money—is always in the public's hands. That means not the mayor's hands, but yours and mine.

Id. at 334-35.

Natural and man-made disasters have occurred throughout history. According to the American Psychiatric Association, collective stress reactions were examined by researchers and clinicians as early as the nineteenth century, when there were massive railway accidents in England. The Association found that it was not until the 1900s that research was done on post traumatic stress reaction in rescuers. In 1914 and in 1918, Dr. Angelo Hesnard, a French psychoanalyst, examined the side effects in rescuers after two ship explosions. Angelo Hesnard, *Nervous and Psychic Disorders Following Naval Catastrophes: Contribution to the Study of Emotional Psychoneuroses*, 18 REV DE PSYCHIAT, 139-52, (1914); *Nervous and Psychic Disorders Following War at Sea*, 106 ARCH MED PHARM NAV, 241-89 (1918).

Mass trauma is defined by the Centers for Disease Control and Prevention as the injuries, death, and emotional disability caused by a catastrophic event. ("Mass Trauma Preparedness and Response," Center for Disease Control,

http://www.cdc.gov/masstrauma/default.htm.) After the Cocoanut Grove Nightclub fire, Dr. Eric Lindemann and Dr. Stanley Cobb, at Massachusetts General Hospital, studied the psychological impact of the tragedy on some of the patients who survived the fire. They assessed and treated patients with crisis intervention techniques and concluded that the survivors suffered from "acute grief." In June 1943 Dr. Cobb and Dr. Lindemann published an initial report on their findings from working with seventeen patients who were admitted to the hospital on the night of the fire. Stanley Cobb and Eric Lindemann, *Neuropsychiatric Observations During the Cocoanut Grove Fire*, 112 ANNALS OF SURGERY, 814-24 (1943). In September 1944 Dr. Lindemann wrote a more detailed account of his work with those suffering from acute grief and its management in Eric Lindemann, *The Symptomatology and Management of Acute Grief,* 101 AMERICAN JOURNAL OF PSYCHIATRY, 141-48 (1944). (Read at the Centenary Meeting of the American Psychiatric Association, Philadelphia, Pa., May 15-18, 1944).

The survivors in Dr. Lindemann's study all showed similar reactions to surviving the fire. He discovered the following patterns of trauma responses in his patients:

- somatic distress;
- preoccupation with the image of the deceased;
- guilt;
- hostile reactions;
- loss of patterns of conduct (an inability to function as competently as they did prior to the fire); and, sometimes,
- the appearance of traits of the deceased in the behavior of the bereaved, especially symptoms shown at the time of the tragedy.

Id. at 142.

Dr Lindemann also found that the duration of a grief reaction depended upon the success with which the traumatized person did "grief work" and regained a sense of equilibrium in their lives. This work was done in three stages:

- emancipation from the bondage to the deceased;
- readjustment to the environment from which the deceased is missing; and
- the formation of new relationships in the world. When a person tried to avoid the distress caused by the grief experience, he did not move through the three stages quite as easily and regain stability in daily functioning.

Id. at 143.

Dr. Alexandra Adler, at Boston City Hospital, assessed fifty-four of the survivors. She followed up with forty-six of the fifty-four over a nine-month period. Dr. Adler, like Dr. Lindemann, saw some of the same symptomatology in patients who had witnessed and survived the violent dying. She, unlike Dr. Lindemann, did not treat anyone's psychological symptoms. Dr. Adler termed the symptomatology "post traumatic mental complications". (*"Neuropsychiatric Complications in Victims of Boston's Cocoanut Grove Disaster,"* 123 AMERICAN MEDICAL ASSOCIATION, 1098-1101 (1943).

According to the findings of Dr. Adler's 1943 study at Boston City General Hospital and Dr. Cobb and Dr. Lindemann's initial study at Massachusetts General Hospital in 1943, and Dr. Lindemann's more in-depth discussion of the earlier research on the survivors in 1944, one year later, fifty percent of the survivors showed symptoms of sleep disturbance, increased nervousness, anxiety, guilt related to survival, and fears related to the Cocoanut Grove Nightclub fire. "Survivor's guilt," characterized by the survivor's confusion over having lived and the meaning of that survival, was for the first time identified by Drs. Cobb and Lindermann after this major disaster. The survivor questions why he is still alive and other people died instead. The survivor may feel total responsibility for the death of another.

What are the lessons that professionals working as first responders can learn from the Cocoanut Grove Nightclub fire in 1942? Citizen Corp, a group of volunteers who help to make their communities safer by preparing for disasters, offers the following lessons:

- Major disasters can overload the capability of "first responders," especially during the first critical twelve to seventy-two hours of an event;
- Communities can train individuals in emergency preparedness and basic response techniques in order to supplement the work of

firefighters, police, public health and safety workers; and

- It is also critically important that elected officials engage "first responders" in discussions about the vital role that they play in local disasters. They are trained professionals. Asking for and valuing their input helps to ensure that local governments address the needs of "first responders," citizens, and communities during times of mass disasters, man-made and natural.

Trauma shatters our belief systems. It snatches from us a sense of having immunity from disaster. It shatters the illusion that we will always be safe. Trauma destroys people's belief that they can always control their lives and their environment. That was true on 9/11, and that was true on November 28, 1942. When a disaster occurs, the traumatic symptoms that result are usually normal (albeit unsettling) responses to abnormal events. Dr. Lindemann, and other trauma specialists, discovered that many witnesses to mass disaster can only begin to heal when they talk about what they saw, heard, felt, and smelled. It is the recalling of the tragic incident in detail that provides catharsis and returns them to more stable functioning. If this is the case, and it certainly seems to be so, "first responders" can find relief from the gut-wrenching work they do daily. However, that relief must take place in a safe and supportive environment with supportive peers and professionals who give value and credence to the demanding job that they are called to perform.❖

ABOUT THE AUTHOR

❑**Beverly Ann Jones** is a licensed clinical social worker who began working at EOUSA's EAP in November 2002. Prior to that, she worked three years in the areas of trauma/grief/loss. During the same time, she had a private therapy practice where she worked with children, adults, and families in the areas of: substance abuse, trauma, child abuse, domestic violence, reentry back into the community from prisons, and chronic mental illness.✠

USA PATRIOT Act: Responding to Library Concerns

Stan Harris
First Assistant U.S. Attorney & ATAC Coordinator
Southern District of Mississippi

Gaines Cleveland
Assistant U.S. Attorney
Southern District of Mississippi

I. Introduction

In working with community groups, including first responders who are not routinely part of the federal law enforcement process, questions may arise about the *U*niting and *S*trengthening *A*merica by *P*roviding the *A*ppropriate *T*ools *R*equired to *I*ntercept and *O*bstruct *T*errorism (USA PATRIOT) Act. Several provisions of the Act are scheduled to terminate on December 31, 2005,

and because of this the Act has received significant media attention. Given the fact that much misinforma- tion and unfair criticism of the Act has been published, communicating accurate information to the public has become a matter of great importance. Excellent materials are available at a public Internet site maintained by the Department of Justice at http://www.lifeandliberty.gov.

The library community is one of the groups expressing concern about the Act. Their concerns mirror those of other organizations. Earlier this year, our office was invited to speak to the Friends of the Gulfport Libraries—part of one of the largest public library systems in Mississippi. We welcomed the opportunity to provide background on the Act and to answer concerns.

Prior to the library meeting, we learned that the American Library Association (ALA) had adopted a resolution raising various concerns about the Act. We found a variety of materials discussing the Act on the ALA Web site, including the ALA resolution, a Congressional Research Service (CRS) analysis, and an ALA analysis of the Act as it relates to libraries.

II. Background of the Act

The law was enacted to strengthen the effectiveness of law enforcement in the aftermath of the 9/11 terrorist attacks. The legislation received overwhelming Congressional support from both parties.

The Act:

- gives terrorism investigators the same tools that federal agents have long employed in ordinary criminal cases, but which had been unavailable in national security cases;
- helps our laws catch up with technological advances that have handicapped law enforcement because the laws were outdated; and
- promotes the sharing of important information within and among law enforcement agencies, which had previously been discouraged.

The Act also directly benefits libraries and others subject to victimization by computer hackers by allowing law enforcement to assist victims in monitoring computer trespassers. This is something that was not clearly authorized under the prior law. In addition, the Act shields remote computer service providers who volunteer information about suspected terrorist activities and other threat emergencies from civil liability.

III. CRS: Act not aimed at libraries

According to the CRS report, *Libraries and the USA PATRIOT Act* (Feb. 26, 2003), *available at* http://www.ala.org, the Act "contains ***no*** provisions specifically directed at libraries or their patrons." (Emphasis added). However, the Act does have "several provisions...that ***might*** apply in a library context" (emphasis added) (the most often mentioned is Section 215).

The CRS Report made important observations worth bearing in mind when considering the Act:

- "Although the library community stoutly defends the importance of library-patron confidentiality, federal law has yet to recognize its privileged status...."
- "As a general rule, libraries must comply with federal grand jury subpoenas, search warrants and court orders."

Thus, information concerning library patrons has long been subject to disclosure in federal criminal cases, even before the USA PATRIOT Act was enacted.

In order to consider the ALA's specific concerns, we turned to the ALA's *Analysis of the USA Patriot Act Related to Libraries, available at* http://www.ala.org/ala/oif/ifissues/usapatriotactlibrary.htm. The document is divided into two parts examining individual provisions of the Act: "Enhanced Surveillance Provisions Affecting Library Confidentiality" and "Other Provisions That Do Not Directly Affect Libraries."

IV. ALA focus on three provisions

In addressing the impact of the surveillance provisions on libraries, the ALA singled out three provisions of the Act, in order of importance to the library community: Section 215, Section 216, and Section 214.

A. Section 215: Access to records and other items under the Foreign Intelligence Surveillance Act (FISA)

This section, which has received considerable media attention, has been largely misunderstood and, in fact, has been rarely, if ever, used. USA PATRIOT Act of 2001, Pub. L. 107-56, 115 Stat. 272, effective October 26, 2001.

Long before the USA PATRIOT Act, ordinary grand juries were able to issue subpoenas for all records relevant to criminal inquiries, including library records. An example of law enforcement's need for such records is the Unabomber case. That investigation involved a multi-year manhunt and, prior to the arrest of Ted Kaczsinski, included the FBI's obtaining records from a Utah public library regarding the circulation of books dealing with explosive devices similar to those Kaczsinksi used. At the same time, federal intelligence agents were only authorized to obtain a limited category of documents, such as car rental, travel, storage facility, and hotel accommodation records. No other documents were obtainable, even though they were needed to give the agents a complete picture of the potential threat. The USA PATRIOT Act seeks to remedy this problem.

Section 215 authorizes the FBI director or a senior FBI official to apply to the Foreign Surveillance Intelligence Court "for an order requiring the production of any tangible things (including books, records, papers, documents and other items)." USA PATRIOT Act of 2001, Pub. L. 107-56, 115 Stat. 272, effective October 26, 2001. The application must specify that the records are sought for an authorized investigation "to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." The application also must certify that it is not directed at "a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States." *Id.*

Section 215 requires that the Department regularly account to Congress regarding the use of the Act, and provides for Congressional oversight. As of September 18, 2003 (the latest date for which information has been declassified), no request under this provision had yet been issued—to libraries or anyone else.

The ALA's principal concern is that this section of the USA PATRIOT Act allows the FBI to compel the production of any tangible thing, including library circulation and Internet use records, stored in any medium. However, this is no different than what the FBI can obtain by means of a grand jury subpoena or court-authorized search warrant in ordinary criminal cases. The provision simply gives the FBI the same powers in conducting a national security investigation as in investigating fraud or drug trafficking.

A second ALA concern is that Section 215 includes no requirement to demonstrate "probable cause" (which the ALA describes as "the existence of specific facts to support the belief that a crime has been committed or that the items sought are evidence of a crime"). *Analysis of the USA Patriot Act Related to Libraries*, *supra*. What this concern disregards is that no such showing is required for grand jury subpoenas. The probable cause standard is reserved for search warrants and arrest warrants, not investigative subpoenas. What the Act does require is a certification, which is not required for grand jury subpoenas, that the records are sought to protect against international terrorism or clandestine intelligence activities.

The last concern the ALA expressed is that Section 215 prohibits recipients of FISA requests (including libraries) from disclosing the existence of the request. The USA PATRIOT Act did not invent this requirement. It was already the law for other types of investigations, particularly bank fraud and other financial fraud investigations.

The ALA's commentary fails to mention a number of safeguards in Section 215. First, the application must come from a senior FBI official. Second, the agent must apply to a federal court, which is not required for ordinary grand jury subpoenas. Third, the agent must certify the proper purpose of the investigation. Fourth, the investigation of a United States person is not to be conducted solely on the basis of activities protected by the First Amendment. Finally, the provision requires regular reporting and Congressional oversight.

B. Section 216: Expanded use of Pen Register and Trap-and-Trace Devices

Federal law long has permitted courts to issue orders for pen registers and trap-and-trace devices. A "pen register" is a device that keeps a record of the numbers dialed from a telephone. Much as a cellular telephone bill lists numbers dialed, a pen register gives this same information to law enforcement. A "trap-and-trace device" keeps a record of the telephone numbers of incoming calls. USA PATRIOT Act of 2001, Pub. L. 107-56, 115 Stat. 272, effective October 26, 2001.

Prior to the USA PATRIOT Act, orders for pen registers and trap-and-trace devices were valid only in the issuing court's jurisdiction. They

were basically limited to telephone lines, and it was unclear if they were applicable to the Internet. Thus, the law failed to address the realities of modern technology. As new means of communication became available, the law did not keep pace.

Section 216 serves to correct these deficiencies in two ways. First, courts may issue such orders and they are valid "anywhere in the United States." *Id.* Thus, law enforcement officials no longer need rely on officials in other jurisdictions, where the communications facilities may be based, to obtain these orders. Secondly, the law makes clear that these provisions apply to facilities other than telephone lines, such as the Internet. This change recognizes the reality that people now use the Internet much as they do the telephone.

The ALA is concerned that the Act extends the telephone monitoring laws to include routing and addressing information for Internet traffic. The law specifically says "that such information shall not include the contents of any communication." *Id.* That is, information in the text or subject line of an e-mail would not be disclosed.

The ALA complains that agents seeking this information need only affirm that it is relevant to a criminal investigation. That is the same requirement that exists under the present law. Under Section 215, an agent must also allege that the records requested relate to an ongoing investigation. The ALA notes that state law enforcement officials can get access to these records, but that was equally true of the old law.

The ALA also says the Act requires recipients of monitoring orders to provide cooperation to law enforcement and not disclose the order. Neither of these requirements is new. There are similar provisions in the prior law.

Finally, the ALA warns that "[l]ibraries that provide access to the Internet and e-mail...may become the targets of a court order requiring the library to cooperate in the monitoring of a user's electronic communications sent through the library's computers or networks." *Analysis of the USA Patriot Act Related to Libraries, supra.* According to the Act, however, such orders are only directed at providers of "wire or electronic communication service." USA PATRIOT Act of 2001, Pub. L. 107-56, 115 Stat. 272, effective October 26, 2001. This portion of the Act is directed at telephone and Internet service providers and the like—not libraries.

C. Section 214: Pen Register and Trap-and-Trace Device authority under FISA

This provision streamlines the process for obtaining pen registers and trap-and-trace devices by intelligence agents. It helps place terrorism investigations on the same footing as other law enforcement investigations in obtaining orders for pen registers and trap-and-trace devices.

The ALA complains that agents seeking such orders need only affirm that the information sought is relevant to terrorism or intelligence activities. This simply parallels similar provisions that apply for ordinary criminal investigations. Why should investigations into terrorism and foreign intelligence activities be treated any differently?

V. Other provisions with no direct affect on libraries

After discussing the three provisions of the Act considered most significant for libraries, the ALA addressed four other provisions that do not directly affect libraries: Section 218, Section 219, Section 220, and Section 206.

A. Section 218: Foreign intelligence information requirement for FISA authority

The sum total of this provision is to amend FISA to provide that law enforcement may obtain a surveillance order or request physical items if foreign intelligence gathering is a "significant purpose" of the investigation—rather than "the purpose" as provided under the old law. USA PATRIOT Act of 2001, Pub. L. 107-56, 115 Stat. 272, effective October 26, 2001 (emphasis added). The ALA says this provision relaxes the legal standard for FISA surveillance. In reality, the change simply serves to reduce the need to evaluate whether an investigation is for criminal or intelligence purposes, and allows greater cooperation among agencies. The former requirement that the sole purpose for court-approved surveillance was to obtain foreign intelligence information discouraged information sharing and hampered efforts to root out terrorists.

B. Section 219: Single jurisdiction warrants for terrorism

This provision allows federal courts to issue search warrants that are valid in other districts for

investigations involving terrorism. This helps expedite the process for obtaining search warrants in time-sensitive, multi-district terrorism investigations. Plus, it lets the judge who is most familiar with the case issue the warrant. Law enforcement agents still must satisfy the court that there is probable cause to justify a search.

C. Section 220: Single jurisdiction search warrants for electronic evidence

Like Section 219, this provision permits federal courts with jurisdiction over an investigation to issue search warrants for certain electronic communications (unopened e-mails that are less than six months old) stored by providers in other districts. The provision recognizes that most Internet service providers are located in California and Virginia, and allows courts in other jurisdictions to issue such warrants. As with Section 219, this section clears outdated jurisdictional roadblocks.

D. Section 206: Roving surveillance authority under FISA

The Act updates the law to provide what is called "roving" authority for electronic surveillance approved by the FISA court. The Act recognizes that in an era of disposable phones, easily available e-mail accounts, and endless communications options, it is more effective to follow a suspect, rather than a communication device. Such roving surveillance authority has long been available in drug and racketeering investigations. The Act extends this authority to FISA warrants, but only if the FISA court finds that the actions of the target may thwart the identification of the target.

VI. Safeguards in the Act

The USA PATRIOT Act is subject to a number of important safeguards, such as:

- the requirement of court approval for certain law enforcement tools authorized under the Act and the availability of judicial scrutiny for violations of the Act;
- the provision for the Department of Justice Office of the Inspector General, which reports to both the Attorney General and to Congress, to investigate and respond to claims regarding civil rights or civil liberties violations under the Act; and
- the provision that Congress is required to receive periodic reports on the implementation of the Act and Congress' exercise of oversight responsibilities, with frequent interaction with the Department of Justice about the Act's impact.

These safeguards help assure that the Act focuses on its intended targets.

We appreciate the assistance and support of Kelly Shackelford of the Executive Office for U.S. Attorneys and Barry Sabin, Linda Bizzarro, and Jerry DeMaio of the Justice Department's Counterterrorism Section in addressing USA PATRIOT issues in our district and in the preparation of this article.❖

ABOUT THE AUTHORS

❑**Stan Harris** began service as First Assistant United States Attorney for the Southern District of Mississippi on October 23, 2001. Harris serves as Chief-of-Staff for U.S. Attorney Dunn Lampton, and serves as the Southern District's Anti-Terrorism Coordinator.

Mr. Harris formerly served as Chief Counsel and Deputy Chief-of-Staff for Senator Trent Lott, Minority Leader of the U.S. Senate.

Mr. Harris has handled cases and projects involving virtually every federal department and agency, and has received numerous commendations for work on behalf of local, county, state and federal government.

❑**Gaines Cleveland** is an AUSA in the Southern District of Mississippi. He previously practiced law in Washington, D.C. and served as an Assistant U.S. Attorney in the Southern District of New York from 1990-1995.✠

NOTES

Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' BULLETIN to all **federal law enforcement personnel** who wish to receive it, we are requesting that you e-mail Nancy Bowman (nancy.bowman@usdoj.gov) with the following information: Name, title, complete address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the BULLETIN, we ask that you have one receiving contact and make distribution within your organization. If you do not have access to e-mail, please call 803-576-7659. Your cooperation is appreciated.