THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 7

JANUARY 2009
LAW ENFORCEMENT

Contact: CIPP02@gmu.edu
703.993.4840

This month, *The CIP Report* focuses on law enforcement, a vital area of homeland security that presents a variety of issues. Law enforcement agencies at the Federal, State, and local levels are key in the protection of our Nation. There are new threats and concerns everyday that compel law enforcement to the forefront of security.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION

The Commission on Accreditation for Law Enforcement Agencies, Inc.(CALEA) provides an overview of their work to establish a set of law enforcement standards for the many different law enforcement agencies that exist. CALEA provides accreditation programs that focus on management criteria as well as public safety communications. The next article, a contribution from the Federal Law Enforcement Training Center (FLETC), discusses some of the challenges law enforcement agencies face regarding homeland security. It also describes two training courses offered by the FLETC, aimed at integrating law enforcement and critical infrastructure protection.

We also present an article about the International Civilian Police (CIVPOL) program. This program focuses on post-conflict societies and the development of effective criminal justice systems. The National Institute of Justice (NIJ) provides an article on the research they have done and technology being developed to assist law enforcement in detecting concealed weapons. Lastly, *Legal Insights* looks at law enforcement in the world of cyber.

We hope this month's issue of *The CIP Report* is informative and we look forward to your feedback. We owe a great deal to these brave men and women who form our first line of defense for this Nation and we will continue to bring updates from time to time. We thank you for your continued support.

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

Mick Kicklighter

CALEA
Law Enforcement Accreditation

by Sylvester Daughtry, Jr., Executive Director
Commission on Accreditation for Law Enforcement Agencies, Inc.

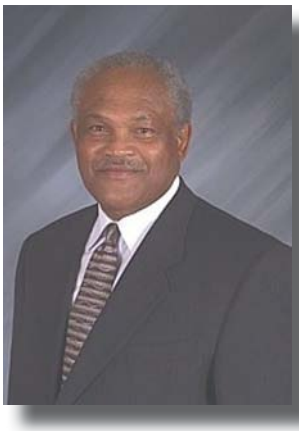
The Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA®), located in Fairfax, Virginia, is an independent, non-profit corporation established in 1979 under a grant initiative provided by the United States Department of Justice. Under the direction of the four leading law enforcement executive associations: the International Association of Chiefs of Police (IACP); the National Organization of Black Law Enforcement Executives (NOBLE); the National Sheriffs' Association (NSA); and the Police Executive Research Forum (PERF), CALEA's original purpose was to develop a set of law enforcement standards and to establish and administer an accreditation process through which agencies could demonstrate that they meet professionally-recognized criteria for excellence in management and service delivery. In response, the Law Enforcement Accreditation Program and its distinctive CALEA Accreditation Process was created.

Over the years, the scope of CALEA's mission has broadened to include additional public safety functions. The Public Safety Communications Accreditation Program and the Public Safety Training Academy Accreditation Program were developed, as well as an additional stepping-stone program for law enforcement called CALEA Recognition. CALEA's reputation as a leading credentialing authority in the United States has also expanded, as has its acceptance internationally. Today there are also agencies in Canada, Mexico, and the Caribbean accredited or enrolled in the process. CALEA's authority is derived solely from the voluntary participation of public safety agencies in its credentialing programs.

The CALEA Accreditation Process is a proven modern management model; once implemented, it presents the CEO, on a continuing basis, with a blueprint that promotes the efficient use of resources and improves service delivery — regardless of the size, geographic location, or functional responsibilities of the agency.

The standards upon which the Law Enforcement Accreditation Program is based reflect the current thinking and experience of law enforcement practitioners and researchers. Major law enforcement associations, leading educational and training institutions, governmental agencies, as well as law enforcement executives internationally, acknowledge CALEA's *Standards for Law Enforcement Agencies*© and its accreditation program as benchmarks for today's law enforcement agencies.

What outcomes can an agency expect to derive from its



Executive Director

achievement of accreditation?

- CALEA Accreditation requires an agency to develop a comprehensive, well thought out, uniform set of written directives. This is one of the most successful methods for reaching administrative and operational goals, while also providing direction to personnel.
- CALEA Accreditation standards provide the necessary reports and analyses a CEO needs to make fact-based, informed management decisions.
- CALEA Accreditation requires a preparedness program be put in place — so an agency is ready to address natural or man-made critical incidents.
- CALEA Accreditation is a means for developing or improving upon an agency's relationship with the community.
- CALEA Accreditation strengthens an agency's accountability, both within the

(Continued on Page 3)

CALEA *(Cont. from 2)*

agency and the community, through a continuum of standards that clearly define authority, performance, and responsibilities.

- Being CALEA Accredited can limit an agency's liability and risk exposure because it demonstrates that internationally recognized standards for law enforcement have been met, as verified by a team of independent outside CALEA-trained assessors.
- CALEA Accreditation facilitates an agency's pursuit of professional excellence.

There are currently 462 standards in the latest edition of the law enforcement standards manual, which are organized into 38 chapters and address nine major law enforcement subject areas:

- role, responsibilities, and relationships;
- organization, management, and administration;
- personnel structure;
- personnel process;
- operations;
- operations support;
- traffic operations;
- detainee and court-related activities; and
- auxiliary and technical services.

The standard states what must be accomplished, but allows each agency to determine how to achieve compliance with the standard. Several standards relate to critical infrastructure-related topics. Standard 42.1.6 specifically addresses criminal intelligence, and others such as those in Chapter 46 (Critical Incidents, Special Operations, and Homeland Security), deal with an "All Hazard" plan and homeland security.

The purpose of Standard 42.1.6 is to underscore an agency's responsibility to focus on criminal activities that may have a terrorist link:

42.1.6 *A written directive addresses the collection, processing, and sharing of suspicious incidents and criminal intelligence relating to criminal and homeland security activities (including information detailed in 43.1.1 and 46.3.2) with appropriate entities, to include:*
a. a description of the function;
b. the responsibilities of all agency personnel;
c. training of personnel;
d. procedures for safeguarding, securing, and storing information;
e. procedures for ensuring that information collected is limited to criminal conduct or relates to activities that present a potential threat to the jurisdiction;
f. legal and privacy requirements;
g. documentation, reporting, and dissemination of information;
h. procedures for purging out-of-date or incorrect information; and
i. an annual review of procedures and processes.[1]

While the "commentary" sections support the standard statements, they are advisory in nature and not binding. The commentary for 42.1.6 serves as a guide to clarify the intent of the standard:

Commentary: The intent of this standard is to document agency accountability for the collection and sharing of suspicious incidents and criminal intelligence information.

It is recommended that agencies utilize file procedures (i.e., Law Enforcement Intelligence Unit [LEIU] Criminal Intelligence File Guidelines) as a check and balance against inappropriate activities. The collection/submission, access, storage, and dissemination of criminal intelligence information must respect the privacy and constitutional rights of individuals, groups, and organizations.

… The National Criminal Intelligence Sharing Plan (NCISP) identifies a wide array of suggested accountability mechanisms…

Agencies should leverage a number of resources, including existing information sharing initiatives — such as INTERPOL, the Homeland Security Information Network (HSIN), the Regional Information Sharing Systems (RISS), and Law Enforcement Online (LEO) — and reference materials such as Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector, LEIU Criminal Intelligence File Guidelines, the Justice Information Privacy Guideline document, and the NCISP.[2]

Although the link between suspicious and criminal activity to terrorism may not always be obvious, law enforcement personnel trained in these areas are "encouraged to document information gleaned from a

(Continued on Page 9)

[1] Standards for Law Enforcement Agencies, 5th Edition, CALEA, 2006: p. 42-3.
[2] Ibid.

Vital Connection, Bridging the Gap: Law Enforcement and Critical Infrastructure/Key Resources Protection Training

by Scott I. Flax, Senior Instructor
Federal Law Enforcement Training Center

Critical infrastructure protection has become a phrase that is very familiar across law enforcement in recent years; however, less than a decade ago it was a foreign language for many public safety agencies. Since 9/11 our country has undergone a dramatic realignment of priorities and concerns to the protection of our communities and our nation as a whole. In 2002, the Department of Homeland Security was established and with it was born a new set of requirements and priorities. A major one was the protection of critical infrastructure. Still today, seven years after the founding of Homeland Security, many law enforcement agencies are trying to establish and align their assets and resources to accomplish this important mission. Federal, State, and local law enforcement are battling with how to protect something that they do not own. An additional difficulty is that the facility may be essential to their public safety mission, their community, or the nation, yet they have no direct control over its operation and protection. Law enforcement personnel are often left with more questions than answers such as: Who is responsible for protecting critical infrastructure facilities? How do we develop partnerships with private sector owners and operators for the protection of the facilities? And where do we turn to train our officers to accomplish this new and evolving mission?

Homeland Security Presidential Directive/HSPD-7 clearly defines the overall mission and areas of responsibility for Federal Executive agencies but it is merely an outline for the overall mission plan. The purpose of the directive is "to establish a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[1] It also outlines the roles and responsibilities for the Federal Sector-Specific Agencies (SSAs) as well as other departments, agencies, and offices. The Secretary of Homeland Security recognized "that each infrastructure sector possesses its own unique characteristics and operating models,"[2] therefore they would be best suited to identify what areas needed protection. This seems like a simple task. Each Sector can take care of their areas of responsibility, right?

HSPD-7 clearly defines who is responsible, but how they are to protect it is a totally different issue. Sectors have direction and the Federal agencies have direction, but where is the guidance for the State and local law enforcement? At a majority of the critical infrastructure facilities around the country, State and local law enforcement will be the first responders to the scene.

Often there can be a disconnect or a gap between the Federal agencies, the State and local law enforcement, and the private sector owner and operators. Sectors and agencies need to grasp the complexities involved in the cross-sector interdependencies and dependencies. Sectors cannot operate independently of each other. They have to rely on each other and take a pro-active posture in order to make the protection of the infrastructure critical to our Nation to make it safer, more redundant, and more resilient.

(Continued on Page 10)

[1] Homeland Security Presidential Directive/HSDP-7, available at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.
[2] Ibid.

International Civilian Police Program

by Richard C. Cashon, Vice President
Law Enforcement Programs, DynCorp International

"A cornerstone of stable and democratic nations is a criminal justice system in which citizens broadly accept and voluntarily comply with the law."

That is the introduction to a factsheet published by the U.S. Department of State Bureau of International Narcotics and Law Enforcement Affairs, describing the International Civilian Police (CIVPOL) and Rule of Law programs. As part of the U.S. government's mission to support the creation or establishment of stable democracies, especially in areas that have suffered from years of civil strife, abusive dictatorships, or repressive regimes, the Bureau of International Narcotics and Law Enforcement Affairs (INL) creates programs to help institutionalize sustainable growth in the criminal justice sector, instill public trust in the Rule of Law and protect human rights. This support, often in cooperation with other nations or international bodies, is designed to promote security sector stability by the establishment of professionalized, democratic-style civilian police and full law enforcement services, public prosecutors, district attorneys, courts and tribunal systems, and prisons or correctional facilities. CIVPOL missions from the United States and more than 50 other countries are deployed around the globe in support of international post-conflict stabilization and redevelopment operations. Their presence promotes peace and stability in areas recovering from conflict, and their efforts to reform and/or develop indigenous police forces into modern, democratically-oriented law enforcement services helps to ensure that peace and stability can be sustained even after international peacekeepers depart.

CIVPOL has become a vital tool of U.S. foreign policy, and reflects the U.S. government's recognition of the importance of a functioning, credible criminal justice system to restoring stability in post-conflict situations. CIVPOL missions funded by the State Department INL Bureau not only assist international military forces in the short term by addressing and resolving civilian law enforcement issues, but also help develop local policing institutions founded on democratic style law enforcement that ultimately will be responsible for integrating with the host country's criminal justice system and provide law and order functions.

DynCorp International (DI), a provider of specialized mission-critical services to civilian and military government agencies worldwide, is a major implementer of U.S. government programs to build civilian police institutions in post-conflict environments. DI, under contract with the State Department INL Bureau, was part of the first U.S. CIVPOL operation in 1994 with the United Nations in Haiti to assist in restoring the elected government, provide public security, maintain the rule of law, and establish a new Haitian National Police Service. Since that time, more than 6,000 law enforcement personnel have participated in international police missions through DI, advising, training and mentoring their counterparts. Currently, DI is involved in CIVPOL missions in Iraq, Afghanistan, Haiti, Liberia, Sudan, and the Palestinian Authority. Other CIVPOL missions have been in Sierra Leone, East Timor, Bosnia and Herzegovina, Kosovo, Serbia and Montenegro, the Eastern Slavonia region of Croatia, and Macedonia.

CIVPOL missions supported by INL vary considerably in size and in

(Continued on Page 6)

CIVPOL *(Cont. from 5)*

objective. In some missions, officers perform typical law enforcement functions (patrol, investigation, etc.) in the absence of effective and fair indigenous police forces. In other cases, CIVPOL may be responsible for rebuilding, monitoring, and/or advising local police as they make the transition to democratic policing. In this capacity, CIVPOL may be directly involved in the entry-level, supervisory and managerial training and organizational development activities for a host country's police force.

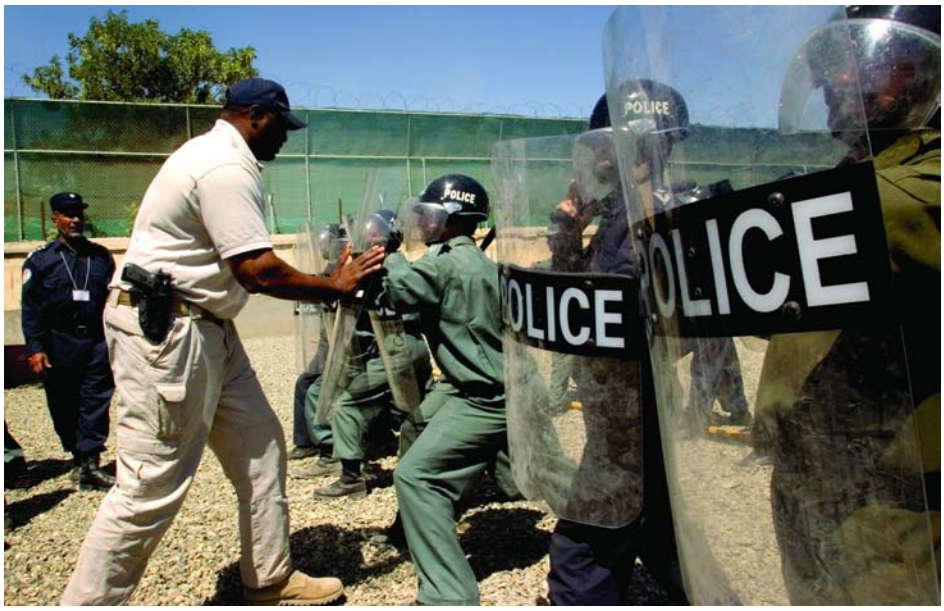
What does not vary is that all candidates for international police missions are experienced law enforcement professionals who apply the lessons they learned in years of employment to their international law enforcement duties. The police personnel provided by DynCorp have an average of 15 years of law enforcement experience prior to their CIVPOL engagement.

DI has been a major part of the CIVPOL mission in Iraq since 2003, and we are responsible for providing more than 800 civilian police advisors to help advise, train and mentor the Iraqi Police Service, Ministry of Interior, and Department of Border Enforcement. These police mentors are assigned to the Civilian Police Advisory Training Team (CPATT), the component of the U.S. military Multinational Security Transition Command (MNSTC). MNSTC is responsible for the U.S.-led effort to train and equip the Iraq police service, and they work with military police teams under the command of Multi-National Corps-Iraq (MNC-I). This effort is complemented by a recent contract award from the Department of Defense to provide up to 128 senior level positions which will be directly engaged with the Iraqi Ministries of Defense and Interior, with the overall role of assisting MNSTC to transition security responsibilities from Multi-National Forces to the Iraqi government.

Afghanistan is another major focus, with close to 600 civilian police advisors for similar duties in support of the Afghanistan National Police and the Ministry of Interior. A key part of this effort is the organizing of the Focused District Development (FDD) program, an eight-week training course where Afghan police units train together in the relative safety of U.S. military bases. A fundamental part of the FDD program is the embedding of DI employed police-mentors with U.S. military Police Mentor Teams. Mentor Teams are comprised of 16-member groups of senior officers and noncommissioned officers who have attended a special two-month training course at Fort Riley, Kansas, which prepares them for participation in the FDD program.

Some on-the-ground examples of effectiveness include teaching first responders in the Kurdish region in northern Iraq to secure and clear crime scenes, canvass witnesses, prepare crime scene diagrams and gather relevant evidence. DI personnel were instrumental in the creation of an independent full-service Forensics Crime Lab in Sulaymaniyah Province in Iraq. In Afghanistan, we helped create a vetted and computerized police personnel database for Afghan National Police, including issuance of an identification card used for payroll disbursement, effectively addressing instances of fraud and overpayment in distribution of police salaries. A DI police mentor set up a Family Response Unit in

(Continued on Page 12)



Detecting Concealed Weapons: Directions for the Future

by Chris Tillery, Associate Deputy Director for Science and Technology
National Institute of Justice

On July 24, 1998, a man entered the U.S. Capitol building in Washington, DC, with a .38-caliber handgun concealed under his clothing. A security check point with a portal weapons-detection system had been established at the entrance of the building. Knowing that his gun would be detected if he walked through the portal, the man stepped around it. Immediately, he was confronted by Jacob Chestnut, one of the Capitol Police officers operating the portal. The man drew his gun and killed Chestnut. He then shot and killed a second officer, John Gibson, before he was stopped.[1]

Seven years later, on December 5, 2005, a man with a bomb vest under his clothing approached a shopping mall in Netanya, Israel. His behavior alerted police and mall security. When he was confronted outside the mall, the suicide bomber detonated his bomb, killing 5 people and injuring 50.[2]

Although there has yet to be a suicide bombing in this country, such an attack could happen anywhere — on a bus, at a mall, at the Super Bowl, or at the Academy Awards. It is vital for law enforcement to be able to detect and respond to weapons at a sufficient distance to allow officers to make decisions and take actions that deal safely with the situation. For over a decade, the National Institute of Justice (NIJ) has been working to address this need.

Limitations of Current Weapons-Detection Systems

The incident at the U.S. Capitol showed the limitations of current security-detection portal systems — they must be near an individual to work. They generally provide sufficient warning when it comes to detecting a knife, but they cannot detect weapons that can kill beyond arm's reach. By the time a handgun or a bomb vest is detected, it generally is too close to be dealt with safely.

But there are ways to provide more warning. One is to move the portal farther from the operator. It can be incorporated into a building's entrance and operated from a control room at another location. A person who wants to enter the building is then required to first go through the portal before an interior door opens to allow admittance to the building. If the portal detects a weapon, the operator does not open the interior door or the door locks automatically, without the operator's intervention. To further protect the public, exterior doors open only after a second interior door is closed behind the person who has entered. In this way, only one person at a time can enter the building, preventing innocent bystanders from being trapped in an entryway with an armed person. Despite their advantages, remote portal weapons-detection systems have significant limitations. They require more space for the remote location, which is not always available, and they impede traffic flow. Using a remote exterior door with screening equipment and a second interior door in a crowded venue, such as a sporting event or an airport, would impede the flow of pedestrian traffic and cause people to collect in a relatively small area, creating a prime target for a suicide bombing or other attack.

Another approach to detecting concealed weapons is through the use of back-scatter x-ray weapons-detection systems, which use low-dose x-rays to develop images of objects under clothing. The x-rays pass through clothing and are reflected — or "scattered back" — by the skin. These systems have the same limitation as existing portal weapons-detection systems: They require close proximity to detect a weapon. They can, however, reduce the nuisance alarms that occur when metal objects other than weapons are detected and thus move

(Continued on Page 13)

[1] "Shooting at the Capitol, Special Report: From the Shootings to the Investigation," Washington Post, www.washingtonpost.com.
[2] Myre, G. "Bomber Kills 5 Outside Shopping Mall in Israel," New York Times, December 5, 2005, available at www.nytimes.com.

Legal Insights

Is Law Enforcement Falling Further Behind in Cyber Fight?

by Timothy P. Clancy, JD, Principal Research Associate for Law

In the cyber world, national boundaries are blurred and so too are the lines between the criminal, organized criminal groups, transnational terrorists, and the state actor. On the opposite side, lines have been blurred as well. Private companies — internet service providers (ISPs), banks, money transfer agents — are usually the first line of defense against malicious cyber incidents. In short, the ISPs "control the field". Government, in particular law enforcement agencies, are almost completely dependent on these private organizations to combat cyber crime.

Recently, there has been much discussion about military cyber forces and the need for greater counter-intelligence against cyber-espionage. Clearly the cyber threat has risen to threaten U.S. national security in a way that transcends law enforcement, meaning use of all tools at the disposal of the government to better secure the nation's critical infrastructures.

However, when it comes to major cyber incidents, law enforcement is government's primary response mechanism. In most U.S. domestic cases, it is the only mechanism allowed under federal law and the Constitution.

Use of law enforcement to combat bad behavior has numerous practical advantages including: relative transparency, methodical gathering of evidence, proving malicious conduct in open court, and the corresponding deterrent effect of prosecution and conviction. Nevertheless, law enforcement agencies everywhere have one major weakness — a serious lack of speed and agility to combat a threat that moves at Moore's Law speed.

Sadly, law enforcement agencies' cyber capabilities remain woefully inadequate worldwide, despite years of studies, reports, testimony, and media stories about ever-increasing cyber threats and vulnerabilities. The security software vendor McAfee recently released another such report — the annual "Virtual Criminology Report" (PDF) that cast the fight against transnational cyber crime in stark terms. Data collected in the report suggest that more and more organizations and individuals turn to cyber crime capitalizing on public fears amidst the global economic downturn. The scale of the cyber crime activity cited by the report is astounding. The volume of malware and PUPs (potentially unwanted programs such as spyware and adware) has increased dramatically in some cases by a factor of seven in less than two years. New fraud scams aimed at economically vulnerable consumers have proliferated.

The report by an international panel of cybercrime experts concludes that law enforcement agencies are losing the battle against cyber crime. Specifically, the report concluded:

Cybercrime is not yet enough of a priority for governments to allow the fight against it to make real headway. Added to that, the physical threats of terrorism and economic collapse are diverting political attention elsewhere.

Cross border law enforcement remains a long-standing hurdle to fighting cybercrime. Local issues mean laws are difficult to enforce transnationally. Cybercriminals will therefore always retain an edge unless serious resources are allocated to international efforts.

Law enforcement at every level remains ad hoc and ill-equipped to cope. While there has been progress, there is still a significant lack of training and understanding in digital forensics and evidence collection as well as in the law courts. The cyber-kingpins remain at large while the minor mules are caught and brought to rights. Some governments are guilty of protecting offenders in their own

(Continued on Page 14)

CALEA *(Cont. from 3)*

variety of sources."[3] As a result, they more readily recognize circumstances where criminal activity can be attributed to a means to financing terrorism. These proactive investigative concepts are emphasized by agencies operating on the CALEA management model, which results in safer and more secure communities.

The 20 standards in Chapter 46 relate to critical incidents encountered, and special operations conducted, by a law enforcement agency. "Critical incidents connote situations, generally of an emergency nature, that result from disasters, both natural and man-made, and civil disturbances. Disasters include floods, hurricanes, earthquakes, explosions, and tornadoes. Civil disturbances include riots, disorders, and violence arising from dissident gatherings and marches, rock concerts, political conventions, and labor disputes. The critical incident section (46.1) follows the structure of the National Incident Management System (NIMS). The incident command system is a component of the National Incident Management System."[4]

Of particular interest are standards such as:

46.1.2 *The agency has a written "All Hazard" plan for responding to critical incidents such as natural and man-made disasters, civil disturbances, mass arrests, bomb threats, hostage/barricaded person situations, acts of terrorism, and other unusual incidents. The plan will follow standard Incident Command System (ICS) protocols, which include functional provisions for: command (46.1.3), operations (46.1.4), planning (46.1.5), logistics (46.1.6), and finance/administration (46.1.7).*

Commentary: *The Incident Command System (ICS) has proven very effective in federal and fire services emergencies over the past two decades. This system permits a clear point of control and can be expanded or contracted with ease to escalating or diminishing situations. The Federal Emergency Management Agency's (FEMA) ICS is comprehensive, available on the Internet, and widely used. The Incident Command System (ICS) establishes standardized incident management processes, protocols, and procedures that all responders — federal, state, tribal, and local — will use to coordinate and conduct response actions. With responders using a common language and standardized procedures, they will all share a common focus, and will be able to place full emphasis on incident management when a critical incident occurs—whether terrorism or natural disaster.*[5]

Together, the eight mandatory standards in this section comprise a comprehensive set of guidelines for a law enforcement agency to follow. There is example after example of how an accredited agency was able to document positive-outcome aspects to an incident because it was prepared to respond.

Also in this chapter are four standards directed toward homeland security, including one that requires the agency to maintain liaisons with other organizations for the exchange of information relating to terrorism. This directly relates to contemporary crime fighting initiatives, such as the one recently launched by the Federal Bureau of Investigation which allows local law enforcement to share tips about possible terror threats with other agencies. Called eGuardian, the program was designed to get law enforcement at all levels (federal, state, local, tribal, and campus public safety) sharing data quickly about suspicious activity and people. The new system provides a format for letting police report their suspicions to the FBI and also search the system for similar patterns in other jurisdictions.[6]

These are but a few examples of how CALEA's Law Enforcement Accreditation Program prompts agencies to create policies and procedures in accordance with best practices as prescribed by internationally accepted standards. Please visit the CALEA website for information and to purchase copies of its publications: www.calea.org. ❖

[3] Ibid., p. 42-4.
[4] Ibid., p. 46-1.
[5] Ibid., p. 46-2.
[6] FBI Website, http://www.fbi.gov/page2/sept08/eguardian_091908.html.

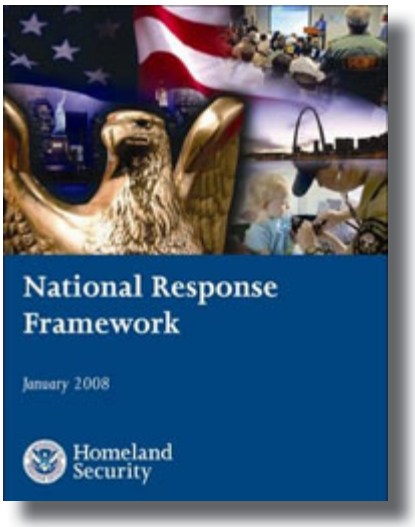
FLETC *(Cont. from 4)*

Sectors put together Sector-Specific Plans (SSPs) as guidelines to assist sectors in forging a path and partnership between agencies and State, local, and private sector entities. Agencies therefore set forth policies based on HSPD-7 and endeavored to secure the assets under their jurisdiction. These partnerships are the cornerstones of a good CI/KR program.

Law Enforcement Responsibility

On the regional level local law enforcement has the responsibility of protecting or augmenting the protection of the infrastructure within their jurisdiction. Traditionally they are the first responders to all kinds of situations, to include parking violations, lost children, vehicle accidents, terrorist attacks, and natural disasters. Therefore, law enforcement must be well versed in preparedness, response, mitigation, and recovery. First responders are our first line of defense. They are the ones who are the boots on the ground. Law enforcement is responsible for understanding a diverse amount of information. Not only understanding the information they receive, but disseminating the proper information to the proper recipients. This can be challenging because there may be a powerful cultural disincentive to sharing information. This has gradually changed over the years and has increased as efforts have been made to share information between entities. Information is not concentrated on just one sector. It may cross some or all of the sectors. Law enforcement is not only responsible for the Emergency Services sector, but they cross over, respond to, and/or need to have an understanding of all, depending on what sectors they have within their jurisdiction.

Having an understanding of CI/KR protection can assist law enforcement in ensuring better communication, teamwork, utilization of resources during a crisis incident, awareness training for employees, and information sharing between stakeholders within a CI/KR community. Better communication between law enforcement and private sector stakeholders will leverage the objectives set forth in the



National Incident Management System (NIMS) and the National Response Framework (NRF). Communication is the key that will open the doors to many opportunities. These are opportunities to train and practice skills in multiple venues in which you will one day respond. Utilizing partnerships within the community can increase your coverage ten to one hundred fold by awareness training and buy-in from your CI/KR community. Law enforcement must take a pro-active posture in addressing CI/KR protection. You cannot just wait until a natural disaster, a terrorist attack, or a critical incident happens to start planning. You must have plans in place so that when it does happen you will be ready. The plans must be written, tested (through tabletop exercises and then actual scenario-based exercises), and trained so it is not just some nice looking book sitting on someone's shelf that no one has read. It must be read, tested, and trained to be retained and become second nature.

Bridging the Gap

The Federal Law Enforcement Training Center (FLETC) serves as an interagency law enforcement training organization for more than 85 Federal agencies. The Center also provides services to State, local, tribal, and international law enforcement agencies. The FLETC offers many courses covering a wide variety of basic and advanced law enforcement topics.

In the area of CI/KR, the FLETC offers two courses that aid in bridging the gap between law enforcement and CI/KR protection. The main objective and goal in creating these courses was to

(Continued on Page 11)

FLETC *(Cont. from 10)*

standardize and set baseline training within the realm of the CI/KR world.

Standardized, baseline training is what is needed across the board so that everyone is on the same page and speaking the same language. The FLETC is filling the gap and meeting that vital need. Most CI/KR programs offer portions of CI/KR training such as vulnerability assessment methodologies or CI/KR laws. The FLETC is the only standardized CI/KR program based upon the National Infrastructure Protection Plan (NIPP), offering a complete overview of CI/KR protection from the national level down to the State and local level.

With this in mind, the FLETC offers courses for the Federal, State, local, tribal, territorial, and international agencies with CI/KR protection responsibilities and private sector owners and operators of CI/KR. The Critical Infrastructure Protection Training Program (CIPTP) is a one-week manager's level course, and the Critical Infrastructure Key Resource Training Program (CIKRTP) is a two-week practitioner's level course.

CIPTP

This course, which is intended for the CI/KR manager, assists the students in understanding how infrastructure impacts their mission and the importance of building resiliency and redundancy into their security plan. The goal of the course is to equip them to better understand how to protect the infrastructure critical to their mission. The CIPTP course will enhance their current CI/KR program or can facilitate the creation of a new one. The CIPTP course covers the guiding documents set forth by our national policy, the commonalities found in vulnerability assessment methodologies, physical and computer security, interdependencies and dependencies, and the importance of partnership models and information sharing.

CIKRTP

This course is intended for CI/KR practitioners and those that are fully immersed in CI/KR duties. It is designed to establish a reference point and standard of performance for federal employees by providing common references, processes, and tools to facilitate consistency within the federal community charged with CI/KR protection. The target audience for this course is the security specialists, program managers, inspectors, investigators, and officers charged with NIPP implementation, compliance, and information sharing.

In accordance with HSPD-7 paragraph 14, the Secretary of Homeland Security will establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities. This course will walk the student step-by-step through the NIPP's Risk Management framework (RMF); define consequence, vulnerability, and threat; and discuss the importance of each. It will also look at different assessment methodologies, review the laws and policies that guide CI/KR policy, discuss the SSPs' interdependencies and dependencies, and the importance of partnership models and information sharing. This course includes a written test and a practical exercise reiterating the principles that were taught during the course of the program. ❖

For additional information concerning these courses, please contact:

Scott Flax
FLETC
Counterterrorism Division (CTD)
Senior Instructor/Program Coordinator
Critical Infrastructure Protection
scott.flax@dhs.gov
912-267-2716
www.fletc.gov/ciptp

Kevin McCarthy
FLETC
Counterterrorism Division (CTD)
Program Specialist/Program Coordinator
Critical Infrastructure/Key Resource Program
kmccarthy@dhs.gov
912-267-3587
www.fletc.gov/cikrtp

CIVPOL *(Cont. from 6)*

Afghanistan to provide help and assistance for women who have been abused.

These Iraq and Afghanistan programs coordinate and work directly with the lead U.S. military agency and the security transition commands to implement U.S. Foreign Policy objectives related to nation building and sustainable development. In contrast, our work in Liberia, Sudan, and Haiti is coordinated through senior officials at the U.S. Embassy responsible for rule-of-law programs, the INL Bureau of the State Department, and/or United Nations missions in each country. In Haiti, we are providing specialized training for up to 444 Haitian National Police to prepare them for assumption of law enforcement responsibilities in Haiti's highest crime area. The program includes procurement of basic and specialized non-lethal equipment, vehicles and communications equipment, and refurbishment of the main police station in Cite Soleil. In Liberia, DI is training and equipping up to 500 Liberian National Police members who will establish an Emergency Response Unit (ERU) with the United Nations Police and the United Nations Mission in Liberia (UNMIL). Our secondary function is to construct a new ERU headquarters building where the unit can operate more professionally.

Coordination

It is important to emphasize that policy direction and decision-making on the CIVPOL program remains, quite appropriately, within the U.S. government and international organizations such as the United Nations. The role of the private sector is to essentially provide the experienced law enforcement talent to these institutions, using our developed contacts and our experience engaging professionals within the law enforcement community across the United States. In every CIVPOL program, DI program managers in-country coordinate closely with authorized U.S. government and international interlocutors. In Washington, DC, there is a steady flow of communication to, and program guidance and direction from, the International Narcotics and Law Enforcement Affairs Bureau of the U.S. Department of State.

The second important role of the private sector is logistics and organization. In most cases, the local infrastructure has been severely damaged, neglected, or does not exist in a form that would be suitable even for expeditionary requirements. DI is contractually obligated to provide all life support systems, including construction of living facilities, food and catering, IT and other communications, medical care and treatment, utilities and transportation. The costs and quality of such support is closely monitored by government contract officials and will be the subject of much negotiation and coordination during contract implementation.

Benefits for Participants

As in every international program, the benefits are not only to the foreign police or security officials receiving advice, mentoring, equipment or supplies. American police officers who take part in international police missions gain tremendous insights and new perspectives into their work as well as new skills in cross-cultural problem solving and communication. Service with an international police mission allows officers to apply their considerable professional skills in dynamic environments that are experiencing intense cultural and political change. It provides valuable experience that cannot be replicated in a lifetime of police work at home, not to mention the networking and professional contact with international colleagues. CIVPOL programs offer one-year contracts, sometimes with extensions, but do not replace a domestic law enforcement career. Based on our 14+ years of direct involvement with international law enforcement missions, we believe it is a career enhancing experience. Many officers are placed in leadership roles on their CIVPOL missions that then pay off in improved leadership skills in their promotion process at home. Beyond career development, DI maintains contact with former police advisors and actively supports a smooth re-integration into their domestic workplace, with ground-breaking programs in PTSD monitoring, available psychological counseling, and an established, recognized Alumni Association.

The creation of democratic policing institutions is fundamental to establishing long-term community stability and to laying the

(Continued on Page 14)

NIJ *(Cont. from 7)*

pedestrian traffic more quickly through security checkpoints.

Where Are We Going?

In the late 1990s, NIJ launched an aggressive program to find ways to detect concealed weapons from a safe distance. The Institute investigated a wide range of potential solutions — radar, infrared radiation (IR) cameras, acoustic devices — and determined that passive millimeter wave (MMW) cameras offered the greatest potential.

A passive MMW camera is one that does not use an artificial source of MMW radiation. It develops images from ambient MMW radiation, which, like IR radiation, is all around but cannot be seen by the human eye. Although both IR and MMW radiation can penetrate clothing to develop images of hidden objects, MMW radiation is more effective in this respect. A MMW camera can develop an image through a heavy coat, but an infrared camera cannot.

Over the past decade, NIJ has leveraged research and development on MMW technology performed by the U.S. Department of Defense (DoD) to the point that there now are commercially available MMW weapons-detection cameras.[3] These cameras represent a 10-fold decrease in size and cost from the initial prototypes, but much work remains to be done in improving resolution and range, and reducing weight and cost.

NIJ continues to work on developing MMW technology. It is also revisiting technologies, such as IR cameras, that have advanced in the last decade and which could offer new opportunities for the detection of concealed weapons. The Institute is closely following the more recent efforts in this area of DoD and the Department of Homeland Security.

New Technologies Demand New Protocols

New technology is never, in itself, the solution. Rather, the solution lies in adopting effective policies and practices for use of the technology. Emerging weapons-detection technologies pose complex questions for law enforcement agencies, particularly the development of legally defensible protocols for using them.

For instance, using a device to remotely search people walking in a public venue, without their knowledge, raises fundamental Fourth Amendment concerns with respect to lawful searches. When and under what circumstances can such a device be used? What is the public's reasonable expectation of privacy in a public venue? What constitutes probable cause for the use of these devices? What is a reasonable search?

Another issue is appropriate use-of-force protocols. Use of deadly force is governed by the totality of the situation. There are two salient points to keep in mind when developing protocols under these circumstances. The first is that no technology is perfect. A MMW camera may reveal an object that, in all likelihood, is a bomb vest, but there is still a possibility, however slim, that it may not be a bomb vest. The second point is that a suicide bomber, by definition, intends to kill or injure as many people as possible. Use-of-force protocols for dealing with a person armed with a handgun, who may or may not be suicidal, may not be appropriate for dealing with a suicide bomber, whose device might be detonated remotely by an accomplice or by the bomber himself even after being restrained.

Under the Nation's federalist system of government, the development of specific protocols for the effective use of these technologies must be done jurisdiction by jurisdiction. Jurisdictions need not work in a vacuum. Key professional public safety organizations have begun to develop guidelines, including ways for responding to suicide bombers. The International Association of Chiefs of Police (IACP), for example, includes this issue in its Training Key monographs, which provide officers with authoritative information on a broad variety of law enforcement practices and procedures. For more information on the IACP Training Key monographs, see www.iacp.org.

A New Century of Challenges

(Continued on Page 14)

[3] Two commercially available products resulting from NIJ's investment in concealed-weapons detection are the Sago ST 150 (www.trexenterprises.com/Subsidiaries/sago.html) and the Brijot BIS-WDS (www.brijot.com). These products and manufacturers are cited for informational purposes only and do not constitute product approval or endorsement by the National Institute of Justice.

CIVPOL *(Cont. from 12)*

foundation for nation-building activities. DI has been one of the more prominent implementation arms of these important goals for the U.S. Department of State. Creating a stable, secure environment where local citizens can rely on a professional, legitimate law enforcement service is a key foreign policy objective of the United States government, as well as the catalyst for true sustainable development of indigenous forces. DI has been proud to be a primary partner with the Department of State to work toward achieving these lofty objectives in 13 countries around the world for more than 14 years. ❖

NIJ *(Cont. from 13)*

The new century brings with it new challenges in detecting concealed weapons. As criminal justice professionals work on the technology and protocols to address these challenges, NIJ will continue to provide the research and development that the Federal, State, and local law enforcement communities need to help prevent attacks and ensure the safety of citizens. ❖

Legal Insights *(Cont. from 8)*

country. The findings suggest there is an ever-greater need to harmonize priorities and coordinate police forces across physical boundaries.

More troubling perhaps is that none of these recommendations are particularly novel or new. Greater investment and attention is urgently needed to bolster U.S. law enforcement cyber capabilities on a scale comparable to investments made in DNA technology in the past decade. The change must be systemic — it is not simply a question of acquiring new technology and training. Meeting the cyber threat will require profound changes to how future police officers are educated and hired as well as how law enforcement agencies organize and deploy their human capital. Further, the fight against cyber crime cannot be solely a federal effort. Cyber capacity must be boosted at every level of law enforcement, Federal, State and local. ❖

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

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