

Tuesday, March 29, 2010 - Conference					
8:00 am – 8:45 am	Registration and Breakfast				
8:45 am – 9:45 am	KN-1: Keynote Address: Randy Vickers, Director, US-CERT (Computer Emergency Readiness Team)				
	Track CI – Critical Infrastructure Protection	Track TC – Cyberterrorism and Cybercrime	Track DI – Domestic and International Terrorism		Track LE: Law Enforcement Case Studies, Tactics and Technologies
10:00 am – 11:15 am	CI-1: Threats to Critical Infrastructure – Understanding, Prioritizing, Defending	TC-1: Cyber Security Issues in the Field	DI-1: Counter-Surveillance in Anti-Terrorism Operations	DI-2: An Update on Homegrown Terrorists& Lone Wolves	
11:25 am – 12:25 pm	CI-2: F/ICAM: Next Steps for Federal ICAM Architecture	TC-2: Preparing Senior Leadership for Cyberspace Operations	DI-3: Avoid, Deny, Defend (ADD): Civilian Response to Active Shooter Events	DI-4: The Human Factor in Catastrophic, Unexpected Events – Attack on the Pentagon	
12:30 pm – 1:50 pm	KN-2: Luncheon and Keynote Address: Janice K. Fedarcyk, Assistant Director in Charge, New York Field Office, FBI				
2:00 pm – 3:05 pm	CI-3: It's Easy to Smuggle Illegal, Threatening and Deadly Items into So Called Secure Environments	TC-3: Sharing and Layering in Cyber Investigations	DI-5: Mumbai & Beyond: Lessons for American Law Enforcement	DI-6: Improvised Explosive Devices	
3:15 pm – 4:30 pm	CI-4: Waterside Security & Maritime Terrorism: Protection of Ports, Harbors and Vital National Waterside Infrastructure	TC-4: Geek Squads: Maintaining a Cyber Savvy Law Enforcement Cadre	DI-7: Times Square VBIED Case Study	DI-8: Connecting the War on Drugs with the War on Terror (P)	
4:30 pm – 5:30 pm	Conference Reception				

Wednesday, March 30, 2010 - Conference				
9:00 am – 10:00 am	KN-3: Keynote Address: Admiral Thad Allen, USCG (Retired), Commander, Deepwater Horizon Oil Spill			
	Track 1 – Critical Infrastructure Protection	Track 2 – Cyberterrorism and Cybercrime	Track 3 – Domestic and International Terrorism	Track 4: Law Enforcement Case Studies, Tactics and Technologies
10:15 am – 11:20 am	CI-5: Protecting Critical Infrastructure from Cyber Attack	TC-5: Advanced Persistent Threats – Current Trends in Cyber Crime	DI-9: Terrorist Ideologies and Pre-Attack Indicators	
10:30 am – 11:30 am				LE-1: Identifying and Responding to Suspicious Behavior
11:30 am – 12:30 pm	CI-6: Threats to Critical Infrastructure by Transnational, Hostile Non-State Actors	TC-6: Being Proactive and Less Reactive in Security Operations and Cyber Attack Response	DI-10: Suicide Bombings – When it Happens Here	
11:45 am – 12:45 pm				LE-2: Social Networking Investigations for Threat Assessment
1:00 pm – 1:50 pm				LE-3 - 4th Generation (4G) Mobile Broadband Applications for Public Safety

Thursday, March 31, 2010 - Conference					
	Track 1 – Critical Infrastructure Protection	Track 2 – Cyberterrorism and Cybercrime	Track 3 – Domestic and International Terrorism		Track 4: Law Enforcement Case Studies, Tactics and Technologies
10:30 am – 11:30 am					LE-4: From Intelligence Led Policing to Predictive Policing: How Technology and Information Fuse a New Paradigm
11:45 pm – 12:45 pm					LE-5: Law Enforcement Response to Mentally Disturbed Persons or “MOs”
1:00 pm – 2:00 pm	KN-5: Keynote Address: Nicholas Stein, Executive Producer, Border Wars				
2:15 pm – 3:15 pm					LE-6: Active Shooter Response Capabilities and Training Standards: Learning from Those who Have Gone Before Us

TRACK CI: Critical Infrastructure Protection

Critical infrastructure and key resources, in public and private sectors, must develop resiliency to various risks in order to continue operating safely and uninterrupted. This track examines the threats facing our nation's critical infrastructure and how to best protect and secure these resources.

CI-1: Threats to Critical Infrastructure – Understanding, Prioritizing, Defending

Tuesday, March 29, 2010 – 10:00 am – 11:15 am

Mischel Kwon, President, Mischel Kwon and Associates, LLC
Mark Weatherford, Vice President and Chief Security Officer, North American Electric Reliability Corporation (NERC)
Karl Gumtow, President, Cyber Point International
Patrick Beggs, Director, NPPD Critical Infrastructure Protection, Department of Homeland Security

It is clear, whether physical or cyber, defending ones country's Critical Infrastructure is a priority. What is the threat to Critical Infrastructure? Is this strictly a US phenomenon? Understanding the level of vulnerability is critical to understanding the level of protection needed to defend. Understanding the highest target values, defining the defensive priorities and understanding the responsible parties are critical in developing a defense. In this talk. discussion will center around what makes Critical Infrastructure critical, what the current threats are, what makes it vulnerable, and what areas are the highest targets, identifying hierarchy of risk, intelligence availability, and where responsibility lies in protecting Critical infrastructure.

Learning Point 1 – Understand Critical Infrastructure – what is Critical Infrastructure and what is the maturation of IT systems that support Critical Infrastructure.

Learning Point 2 – Understanding the threat to Critical Infrastructure.

Learning Point 3 – What Critical Infrastructure organizations are the highest priority to protect.

Learning Point 4 – What intelligence is available to help Critical Infrastructure organizations develop defenses.

Learning Point 5 – How to develop a defensive security posture to protect Critical Infrastructure

CI-2: F/ICAM: Next Steps for Federal ICAM Architecture

Tuesday, March 29, 2010 – 11:25 am – 12:25 pm

Deborah Gallagher, Chair, Roadmap Development Team, GSA

Federal Identity Credential and Access Management (F/ICAM) is one of the cornerstones for protecting our people, information, facilities and systems from attack. It is a methodology whereby we can recognize who is asking for access to any of those resources and giving us a means to make the determination of who will be granted that access. Protecting our people and information is an integral part of all our security efforts - whether it's cybersecurity or physical security. The Identity Credential and Access Control Sub-Committee (ICAMSC) Roadmap Development Team is developing the second phase of the (F/ICAM) roadmap and i

CI-3: Its Easy To Smuggle Illegal, Threatening And Deadly Items Into So Called Secure Environments

Tuesday, March 29, 2010 – 2:00 pm – 3:05 pm

Glenn Bartholomew, CEO, Security Knowledge Solutions
Cynthia White, Training Specialist, Diplomatic Security (Retired) US Department of State
Art Rosati, Department of Defense

During authorized checkpoint security intrusion testing of secured government facilities, undercover operators breached multiple facility check points, on multiple occasions with simulated IED's and Weapons. THERE WAS NOT A SINGLE occasion operator(s) were prevented from entering a secured area WITH an IED or weapon. Yes; our "secure government facilities" had a 100% failure rate. This session explains why this happens and how to prevent it happening

Learning Point 1 - How easy it is to avoid detection of illegal items at a secure checkpoint

Learning Point 2 - Specific examples of intrusions

Learning Point 3 - How to stop the intrusions

CI-4: Waterside Security & Maritime Terrorism: Protection of Ports, Harbors, and Vital National Waterside Infrastructure

Tuesday, March 29, 2010 – 3:15 pm – 4:30 pm

Ronald Carmichael, Program Manager, Staff, Chief of Naval Operations

Captain Brian Kelley, Deputy Commander, U.S. Coast Guard

Since 9/11 there has been an increase in the awareness that maritime terrorism against both military and commercial infrastructure is a real threat and present possibility. Protecting the nation's borders along the waterways has become a major challenge and focus. An example of possible waterside targets might include critical government and commercial infrastructure along the Chesapeake Bay. Even the nation's capital has both private and government facilities adjacent and accessible from the Chesapeake Bay waterways. With over 361 ports, like the Port of Baltimore and 95,000 miles of coastline, the United States is extremely vulnerable to a terrorist attack. More than 95% of the nation's overseas cargo move through ports. World-wide over 80% of the world's trade by volume is moved through ports.

Additionally, many of the nation's nuclear power plants are located on major waterways for easy access to cooling waters. The protection of ports, harbors, nuclear power plants and other waterside vital national infrastructure from terrorists using scuba divers, underwater vehicles or small-manned submersibles is a daunting task. This session addresses the waterborne threat, including swimmer/diver, unmanned small vessels or surface threats.

Learning Point 1 - Define waterside security threats

Learning Point 2 - Review Port and Harbor Maritime Terrorism

Learning Point 3 - Swimmer/Diver Defense Technology's

CI-5: Protecting Critical Infrastructure from Cyber Attack

Wednesday, March 30, 2010 – 10:15 am – 11:20 am

Curtis Papke, Strategic Development, Idaho National Laboratory

Rob Hoffman, National Homeland Security Strategist, Idaho National Laboratory

This presentation will discuss the multiple interactions and coordinations necessary between local, tribal, state, federal,

government, private sector, and international partnerships for an effective response to emerging cyber security threats. It will discuss the DHS National Cyber Incident Response Plan and its implications for National Security.

Learning Point 1 – Appreciate the multiple facets of an effective cyber security strategy including, technical, legal, and moral implications

Learning Point 2 - Understand current federal government approach to cyber security strategy

Learning Point 3 – Develop a framework for linking cyber security strategy to protection of critical infrastructure

CI-6: Threats to Critical Infrastructure by Transnational, Hostile Non-State Actors

Wednesday, March 30, 2010 – 11:30 am – 12:30 pm

Maria Velez de Berliner, President, Latin Intelligence Corporation

Transnational, hostile non-state actors are utilizing friendly countries, such as Canada, the UK, and Mexico, as a springboard to cross into and operate inside the USA. While focus on countering them rests on a law enforcement approach, few are paying attention to the readily available technologies and industrial materials available to those actors to cross the US Southern Border to cause grave damage to the critical infrastructure of the USA. Attendees will be give actionable intelligence that can be applied to counter hostile non-state actors from Africa, China, the Middle East, and Russia who exploit the friendly relations between most of Latin America and the USA to use the US Southern Border as a breachable point of entry.

Learning Point 1 – Identification of Transnational, Hostile Non-State Actors in the USA

Learning Point 2 - Which technologies they might use

Learning Point 3 – How available are these technologies, how they might use them, and where

TRACK TC: Protecting from Cyberterrorism and Cybercrime

Cyberterrorism and cybercrime are a growing national security threat. Whether coming from foreign governments, organized crime or terrorist organizations, these cyber attacks are only going to increase in intensity. No single process will stop these attacks; new approaches and increased vigilance are required. These

sessions will provide the an understanding of the nature and source of these attacks and how to protect against them.

TC-1: Cyber Security Issues in the Field

Tuesday, March 29, 2010 – 10:00 am – 11:15 am

Darnell Washington, CISSP, President/CEO, SecureXperts, Incorporated
Ron Martin, Program Manager, Identity and Access Management, Office of Security and Strategic Information, HHS

Cyber security was once relegated to secure infrastructures within walls. Today's paradigm shift to mobile computing environments has redefined the level of protecting edge devices (mobile phones, mobile computers, and PDA's used in government for public safety, law enforcement environments and interoperable government communications. Additional cyber security issues are presented as the Federal Government moves to web based and cloud computing architectures, which are extended to provide access to email, social networks, and off the shelf technologies. This presentation will focus of today's emerging threats to mobile computing devices (i.e. malicious wireless sniffing and password capture software), and tools used by cyber criminals to capture sensitive data from systems that are not protected by physical infrastructures. The lessons learned from this presentation will create awareness of the requirements of protecting information such as anti-skimming from ATM machines, cyber intrusion, and identity of not only the user, but family, associates, and federal agencies from computer theft while engaging in personal or business interactions on the internet.

TC-2: Preparing Senior Leadership for Cyberspace Operations

Tuesday, March 29, 2010 – 11:25 pm – 12:25 pm

William Waddell, Director, Command, Control and Cyberspace Operations Group, US Army War College

Cyber security across the breadth of government has become an issue that needs to be addressed by senior leadership, as it has implications that cross all other domains. In most cases senior leaders are not thoroughly prepared to face the decision making challenges in this environment. Issues such as national and international laws and charters, national strategies, government to

private commerce relationships, threat and vulnerabilities, and catastrophic consequences are all pertinent to this issue. This session will discuss leadership requirements for effective operation in cyberspace, and recommend some methodologies for preparing the next generation of leaders.

Learning Point 1 – What senior leadership needs to know in cyberspace

Learning Point 2 - What are the effects of a vacuum of leadership in cyberspace

Learning Point 3 – What educational methods are most effective in preparing senior leaders

TC-3: Sharing and Layering in Cyber Investigations

Tuesday, March 29, 2010 – 2:00 pm – 3:05 pm

Dr. Kathleen L. Kiernan, President, InfraGard National Members Alliance
Ronald E. Plesco, CEO, National Cyber Forensics and Training Alliance
Rob Schmidt, CEO, InfraGard National Members Alliance
Dr. Gregory J. Rattray, Partner, DeltaRisk

Attacks on information infrastructure pose the most serious economic and national security threat of the 21st century. Gone are the days of individual hackers as the primary threat to cyber security; today's cyber warriors are members of organized crime rings and hostile nation states, and their targets are government and financial networks; communications, utilities and critical infrastructure control, and sensitive defense and military information. Learn from these veterans of policy and technology development about how to implement best practices that can ensure your organizations investigative, defensive and offensive capabilities are always one step ahead of cyber enemies.

TC-4: Geek Squads - Maintaining A Cyber Savvy Law Enforcement Cadre

Tuesday, March 29, 2010 – 3:15 pm – 4:30 pm

David Daniels, Special Agent, U.S. Department of State, Bureau of Diplomatic Security

Moving into the 21 century with the increasing reliance of the U.S. government and private sector on computer networks and computer technology to store critical and sensitive data, the nature of crime and criminal methods has evolved almost as quickly as the cyber realm itself. Through computer networks, crime has become international at the touch of a button, as well as multi-lingual, with dealings occurring within seconds. Criminals have become more "cyber savvy" and educated in the use of computers to further their pursuits, often times resulting in real-world destruction of property, sensitive information loss, terrorist activity, and some cases, loss of life. Law enforcement officials have been forced to re-focus its recruiting efforts towards the multi lingual, computer scientists, IT professionals, and other "cyber savvy" sources to maintain its edge against criminals, terrorist, and spies. The profile and educational background of the law enforcement official is evolving, and the building of "geek squads" has become critical to keeping the nation safe from the current threats.

Learning Point 1 – Problems in the past in recruiting "geeks" for law enforcement work

Learning Point 2 - How to recruit law enforcement officers with "non traditional" backgrounds

Learning Point 3 – Motivations for "geeks" to look forward to a career in government or law enforcement

TC-5: Advanced Persistent Threats - Current Trends in Cyber Crime

Wednesday, March 30, 2010 – 10:15 am – 11:20 pm

*David Morgan, Cyber Intrusion Analyst, Booz Allen Hamilton
Jon Stevenson, Chief, Counterintelligence Cyber Analysis Branch,
Defense Security Service*

Advanced Persistent Threats are highly organized, sophisticated, and targeted hacking campaigns. In comparison to kiddie-script hacking attempts, the goal of which is usually just for bragging rights, state-sponsored groups and criminal enterprises attempt to

steal proprietary information and intelligence from corporations and governments to use in the development of their own technology. Law enforcement at every level must be knowledgeable of the threat and be prepared to respond. This presentation will give attendees an appreciation of this serious and growing threat and some tools and techniques to protect computers and networks. Most of the content of this session will not be technical in nature, and any advanced computer terminology and concepts will be fully explained.

Learning Point 1 - Current Advanced Persistent Threats

Learning Point 2 - Who is responsible for most US cyber crime

Learning Point 3 - Ways your computer users can protect themselves better

TC-6: Being Proactive and Less Reactive in Security Operations and Cyber Attack Response

Wednesday, March 30, 2010 – 11:30 am – 12:30 pm

Don Goff, Ph.D., CEO, CSTAR Systems

Christina Raftery, Information Systems Security Officer, FBI Los Angeles Field Office

Douglas Himberger, Ph.D., Sr. Vice President and Director, Security, Energy, and the Environment, NORC at the University of Chicago

Creating and maintaining a baseline of security preparedness in order to provide a proactive approach to security operations. Cyber threat awareness within the security operations center is a key to creating a workforce able to respond to malicious attacks.

Preventing a cyber attack has become almost impossible with the amount of malicious software and viruses so being able to respond and quarantine is a important in a proactive operation. Keep politics out of security operations, create a streamline of communication to only include those figures that will assist in the operation keep upper management apprised of situations but limit the amount of information so a reactive response is not triggered based on ignorance. Overall structure and education is the key to a proactive security operations center.

Learning Point 1 – Creating and Maintaining a Security Policy Baseline

Learning Point 2 - The Importance of Security Preparedness and Response Techniques

Learning Point 3 – Overall Structure and Education of the Security Operations Center

TRACK DI: Domestic and International Terrorism

The terrorist threat to our nation's physical and economic security is always with us. Preparing, preventing and responding to attacks is more critical than ever before given the increasing sophistication and creativity of those who wish to do us harm. Agencies and individuals at all levels of government as well as the private sector must remain knowledgeable, vigilant and prepared. These sessions will increase your understanding of these threats and how to protect our nation.

DI-1: Counter-Surveillance in Anti-Terrorism Operations

Tuesday, March 29, 2010 – 10:00 am – 11:15 pm

Michael Burke, Investigator/Security Specialist, US Department of Commerce

A non-classified primer in how to incorporate Counter-Surveillance (CS) techniques in day-to-day LE and Security operations. Active CS techniques are a cost effective way to supplement existing countermeasures and physical security plans in your jurisdiction or in supporting specific high-value assets in your area of operations. Used as a force-multiplier, CS can reduce your risk, detect classic terrorist pre-attack surveillance, and deter criminal attacks.

Learning Point 1 - How terrorists and criminals use surveillance to "case" targets.

Learning Point 2 - How to effectively use Counter-Surveillance techniques to detect active surveillance on your site or in your jurisdiction.

Learning Point 3 - How to incorporate CS techniques into your day-by-day LE or force protection routines and reduce the likelihood of a criminal/terrorist attack

DI-2: An Update on Homegrown Terrorists & Lone Wolves

Tuesday, March 29, 2010 – 10:00 am – 11:15 am

Colonel Jennifer Hesterman, U.S. Air Force (retired); Vice President of Academic Research and Development, 5th Generation Warfare

Institute; Full Professor, Counter Terrorism Studies, American Military University

Daveed Gartenstein-Ross, Director, Center for the Study of Terrorist Radicalization, Foundation for Defense of Democracies
Rich Sanoske, Founder and Chairman of the Board, 5th Generation Warfare Institute

Matt Branigan, CPP, CHS-III, Retired US Air Force Colonel and President, Watermark Risk Management International, LLC

Efforts by terrorists abroad to radicalize and recruit U.S. residents present new security threats. The threat posed by homegrown extremists shows that the battle against terrorism has become more complex in the past year, underscoring the challenges of pinpointing and blocking plots. Since 2009, at least 63 American citizens have been charged or convicted for terrorism or related crimes, "an astoundingly high number of American citizens who have attacked -- or intended to attack -- their own country. This session will explore this increasingly important threat

DI-3: Avoid, Deny, Defend (ADD): Civilian Response to Active Shooter Events

Tuesday, March 29, 2010 – 11:25 am – 12:25 pm

Pete Blair, Ph.D., Researcher, Advanced Law Enforcement Rapid Response Training (ALERRT) Program, Texas State University

The goal of this presentation is to provide civilians and administrators with a basic, but effective response strategy that can be utilized should an active shooter event occur at their location. The presentation will discuss how to identify that an active shooter event is occurring, the avoid, deny, defend response strategy, and how to behave when law enforcement arrives. Real world examples of the avoid, deny, and defend strategy in action will be presented. The importance of preparation will also be discussed.

Learning Point 1 - Participants will learn the key indicators that an active shooter event is occurring

Learning Point 2 - Participants will understand the Avoid, Deny, Defend response strategy

Learning Point 3 - Participants will be to articulate the need to plan for an active shooter event before one happens

DI-4: The Human Factor in Catastrophic, Unexpected Events – Attack on the Pentagon

Tuesday, March 29, 2010 – 11:25 am – 12:25 pm

Matthew Klimow, Executive Director, Bureau of Administration, U.S. Department of State

Colonel (Ret) Matt Klimow recounts his experience in the Pentagon on 9-11, where he served as the Executive Assistant to the Chairman of the Joint Chiefs of Staff. As the building filled with smoke, Colonel Klimow made his way to the heart of the Pentagon, the National Military Command Center, along with the Chairman of the Joint Chiefs and Secretary of Defense. In a small oxygen starved room, as a handful of senior leaders wrestled to respond to the coordinated terrorist attack, Colonel Klimow was witness to the full range of inspired leadership, tactical errors, and strategic decision making that unfolded in the immediate minutes and hours that followed the terrorist strike. Using his gripping account of events, Colonel Klimow brings out crucial and surprising lessons learned in crisis planning and emergency response.

Learning Point 1 – Decisive Leadership: Plan where you want key decision makers during a crisis, from headquarters to various field operations.

Learning Point 2 - Breaking the Mold: Prepare your responders for the unexpected with well considered branches and sequels to basic operation plans.

Learning Point 3 – Calm in the Storm: Instill a disciplined approach to decision making in the midst of a crisis

DI-5: Mumbai & Beyond: Lessons for American Law Enforcement

Tuesday, March 29, 2010 – 2:00 pm – 3:05 pm

Don Alwes, Instructor, National Tactical Officers Association

This class explores the potential threat of terrorist-sponsored Active Shooter attacks against the United States. Incidents including those in Mumbai and Fort Hood are analyzed for implications for US law enforcement. The evolution of terrorists' tactics and how patrol and tactical units should prepare to respond are discussed.

Learning Point 1 - Understand the salient lessons from Mumbai, Beslan, & similar attacks

Learning Point 2 - Understand the characteristics of Swarm and Hostage Siege-Massacre

Learning Point 3 - Understand the fundamentals of state-of-the-art law enforcement response tactics

DI-6: Improvised Explosive Devices

Tuesday, March 29, 2010 – 2:00 pm – 3:05 pm

Buddy Eanes, Director of EOD Training, Explosive Countermeasures International, Inc.

Terrorists, whether domestic or international, are by nature defined as individuals or groups whose actions cause terror. However, individuals who use improvised explosive devices to instill fear and chaos do not necessarily have to be labeled a terrorist. They can be disgruntled employees, students, ex-lovers, etc. Improvised explosive devices are common-place in today's society worldwide. All one needs to do is read a newspaper, watch the news or partake in any other media outlets to learn of its destructive capabilities. Individuals need to have an understanding of the components necessary to construct an effective device. This is necessary for individuals to gain insight into the bomber's unlimited configuration possibilities and placement potentials, to effectively develop countermeasures. Additionally, if knowledge of components is understood, then safety measures and protocols can be addressed and implemented. Through this class, participants will have the opportunity to view IEDs and receive valuable information as to what really makes an IED work in order to properly identify warning signs that demand further investigation. Learning Points:

Learning Point 1 - Develop a fundamental understanding of IED's

Learning Point 2 - Learn basic components of IED construction

Learning Point 3 - Identify hazards and potential destructive capabilities of IED's

Learning Point 4 - Learn who uses IED's and understanding why

Learning Point 5 - Understand safety concepts and procedures upon IED identification

DI-7: Times Square VBIED Case Study

Tuesday, March 29, 2010 – 3:15 pm – 4:30 pm

Lt. Timothy Carroll, FDNY Center for Terrorism and Disaster Preparedness

The presentation will examine the Times Square VBIED Attack and how it was planned, executed and successfully mitigated by inherent situational awareness. The discussion will focus on identifying indicators of why this was more than the reported car fire. Finally, the presentation will analyze the threat posed to the communities distant of the target and why this poses a threat to responders nationwide.

DI-8: Connecting the War on Drugs and the War on Terror

Tuesday, March 29, 2010 – 3:15 pm – 4:30 pm

Christy McCambell, Vice President of USIS' Global Antiterrorism Assistance Program, USIS

Dr. Paul Chabot, Chabot Strategies LLC

Mike Braun, Former DEA Chief of Operations

Jim Burch, Acting Director of the Bureau of Justice Assistance, Office of Justice Programs

Robert Clark, FBI

Gangs, guns and drug trafficking are the domestic "terrorist element," with money laundering serving as the glue that binds these criminal networks—both at home and abroad—together. State and local law enforcement must form partnerships with federal law enforcement and intelligence agencies to put an end to the cycle that ultimately funds terrorist activity. This forum seeks to bring together law enforcement experts in a panel discussion to demonstrate the connection between domestic gang issues and international terrorism and to discuss what has been done so far and where we hope to go in the future.

DI-9: Terrorist Ideologies and Pre-Attack Indicators

Wednesday, March 30, 2010 – 10:15 am – 11:20 am

Victor Vella, Director, Antiterrorism Services Branch, Dept of Defense, NAVFAC ESC

The United States faces a dynamic threat from international and domestic terrorists. The combination of open borders, internet accessible information, and the ability to easily manufacture explosives gives many terrorists and criminals the ability to strike with relative ease. Terrorists routinely use a variety of weapons of mass destruction as a means of achieving their objectives. Because of this, law enforcement personnel need to understand the who, what, where, when, and how's of terrorism. This presentation is designed to provide answers to those questions, and a lot more, as they related to terrorist threats. Attendees will develop an understanding of typical terrorist ideologies, modus operandi, tactics, and trends. Previous acts of terrorism will be used as case studies to illustrate lessons learned. Additionally, the course will describe in the phenomena associated with explosives which is a terrorist's weapon of choice. Lastly, pre-incident indicators that can be used by law enforcement personnel to detect and deter terrorists as the build up to the road to war, will be presented in an easy to understand format.

Learning Point 1 - Learn the who, what, where, when, and how's of terrorism

Learning Point 2 - How to identify indicators before an actual attack

Learning Point 3 - What we as a nation, are doing to counter terrorism

DI-10: Suicide Bombings – When it Happens Here

Wednesday, March 30, 2010 – 11:30 am – 12:30pm

John Brown, Director, Arlington County Office of Emergency Management

Glen Rudner, Project Manager, CRA-USA

During the past 10 years, the country of Israel has been under assault by their enemies. They have seen the use of suicide bombings and shootings as a very accurate tool of those enemies. This program will take the participant through how the Israeli's have dealt with and prepared for each wave. It will discuss the responsibilities of each emergency responder and their respective organization as the events unfold each and every day. It shows how their system works and how we can make some of it work for us.

TRACK LE: Law Enforcement: Case Studies, Tactics and Technologies

Law enforcement, whether federal, military, state or local, faces new and evolving challenges like never before. In addition to its traditional roles, these agencies are charged with protecting their communities from domestic and international terrorism and natural and accidental disasters. Law enforcement is also the first line of defense in homeland security and a partner in terrorism investigations. These sessions will provide the insights and tools needed to meet these challenges and ensuring the public safety.

LE-1: Identifying and Responding to Suspicious Behavior

Wednesday, March 30, 2010 – 10:30 am – 11:30 am

Doug Comfort, Criminal Intelligence Unit, Fairfax County Police Department; Detective (ret.), Vienna VA Police Department

The bread-and-butter of counter terrorism, as well as most other criminal activity, may rest with the three suspicions; persons, events, vehicles. When do you press forward and where do you go? What makes an event so suspicious as to merit further action? Common sense, a sixth sense, and thinking outside the box leads a law enforcement officer to make the appropriate decisions.

LE-2: Social Networking Investigations for Threat Assessment

Wednesday, March 30, 2010 – 11:45 am – 12:45 pm

*Johnny Lee, Peace at Work
Bruce Anderson, Digital Forensics Analyst, Reputation Defense SEO Analyst & Practitioner, REXXfield, LLC*

A growing and revealing source of information about any particular individual can be found in their online, social media activity. Threat assessment professionals can learn the intentions, violence capability and mental status of a subject through their postings and social media accounts. The workshop will review significant cases such as the Finnish man who posted videos of himself pointing a gun at the camera and stating “you die next” or a Japanese assailant who “tweeted” his plan to go on stabbing rampage minute before the event. Domestically, even the man who shot two officers at the Pentagon posted his beliefs in Craigslist and in his own blog.

In the ever growing world of social media and “online lives”, investigators need to consider the wealth of valuable information from sites such as Facebook & YouTube

Learning Point 1 - Understand the importance of investigating online activity in threat assessments.

Learning Point 2 - How to investigate social media activity of the assessment subject.

Learning Point 3 - Understand the possible legal considerations and ramifications.

LE-4: From Intelligence Led Policing to Predictive Policing: How Technology and Information Fuse a New Paradigm

Thursday, March 31, 2010 – 10:30 am – 11:30 am

Paul Joyal, Managing Director, National Strategies Inc.

The notion of intelligence-led policing is becoming more prevalent as law enforcement agencies nationwide aim to become more proactive at preventing all types of serious crime. A majority of experts believe that a nexus does exist among types of criminal activity, including illegal drug operations, money laundering, fraud, identity theft and terrorism. It is well known that some of the 9/11 terrorists were cited for traffic violations prior to the attacks. Many security experts believe there is a high probability of identifying terrorist through their involvement in precursor, or lower level criminal activity. This presentation will provide an in-depth explanation of the new all threats, all crimes, all hazards policing policy today being utilized by the NJ State Police and the role of state fusion centers in the strategy.

LE-5: Law Enforcement Response to Persons with a Mental Disorder or "MO"

Mentally Disturbed Persons or MOs

Thursday, March 31, 2010 – 11:45 am – 12:45 pm

Jeffrey Wilkins, Police Lieutenant, Department of Veterans Affairs

Roger Kelly, Chief, Threat Management Unit, CIA Police

Cathy Lanier, Chief of Police, Metropolitan Police Department - Washington DC

With over 50 different types of mental disorders, law enforcement officials are on the front lines in direct contact with the individuals. A common problem experienced in law enforcement is a lack of recognition of the type of mental disorder the individual is afflicted by. The presentation will point out disorders that appear the same as each other but have various triggers and possible approaches to handle the person with the disorder. Input has been sought from Mental Health Professionals and experiences I have been privileged to. The presentation will offer "common" disorders frequently encountered by law enforcement personnel and techniques offered to assist in dealing with these issues. I believe the importance of this presentation will allow any personnel (security, law enforcement) who may come into contact with disturbed persons to potentially recognize the disorder in an expedited manner, ensure the safety of the law enforcement personnel and disturbed persons, and yield vital information possible to the situation. It is also stressed that these are not 100% guaranteed techniques but do allow an improved ability when dealing with possibly disturbed individuals. I am also conducting further research on these topics as well as chemical dependency disorders for possible inclusion into this topic.

LE-6: Active Shooter Response Capabilities and Training Standards: Learning From Those Who Have Gone Before Us

Thursday, March 31, 2010 – 2:15 pm – 3:15 pm

Terry Nichols, Assistant Director. Advanced Law Enforcement Rapid Response Training (ALERRT) Program-Texas State University

The goal of this presentation is to update law enforcement officers, administrators, trainers and policy makers on current trends both in the United States and abroad regarding active shooter tactics. Briefly examining lessons learned from real-world events, the presentation will address training standards, methodologies and possible curriculum changes to existing active shooter training programs. The program will be presented in such a way as to not dictate a single curriculum or active shooter training program, but to identify and discuss training standards and expectations for police first responders. All jurisdictions who either have a comprehensive active shooter training program and even those that have no training or response protocols will benefit from the presentation.

Learning Point 1 - Participants will be able to discuss recent active shooter event including Virginia Tech University, Mumbai, India and Fort Hood, Texas and identify lessons learned for first responders.

Learning Point 2 - Participants will be able to identify the need for scenario-based force-on-force training in active shooter training curriculums.

Learning Point 3 - Participants will be to articulate the need to prepare first responders for the "worst case" active shooter during training exercises