THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND HOMELAND SECURITY

VOLUME 11 NUMBER 10

APRIL 2013
PARTNERSHIPS & INFORMATION SHARING

EDITORIAL STAFF

EDITOR
Kendal Smith

JMU COORDINATORS
Ben Delp
Ken Newbold

PUBLISHER
Melanie Gutmann

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

In this month's issue of *The CIP Report* we highlight advancements and future challenges in public and private partnerships and information sharing.

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

First, we look at recent policy developments and efforts on the government side, with articles from the U.S. Department of Homeland Security, National Protection and Programs Directorate, and the White House, National Security Staff. We follow this with an article introducing the Cyber Security Information Analysis Center from Taz Daughtrey, Senior Scientist at Quanterion Solutions, Inc. Next, Ross Johnson shows how information sharing helps prevent terrorism, and Dr. Amit Kumar explains how it assists in countering the financing of terrorism in India. Then, Andy Jabbour, Managing Director of the Real Estate Information Sharing Analyis Center, describes partnerships and initiatives in the private sector. Finally, we take a look at InfraGard, a public-private partnership led by the Federal Bureau of Investigation.

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

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

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

Strengthening the Security and Resilience of the Nation's Critical Infrastructure

by Bruce McConnell, Senior Counselor for Cybersecurity, National Protection and Programs Directorate, U.S. Department of Homeland Security

The U.S. Department of Homeland Security (DHS) actively collaborates with public and private sector partners every day to help prevent and respond to attempted disruptions to the Nation's critical cyber and communications networks. Recent actions taken by the President are a key step towards improved security and resilience as we continue to work with Congress to keep our Nation safe and secure for generations to come.

Critical infrastructure is the backbone of our Nation's economy, security, and health and it provides the essential services we need—the power we use in our homes, the water we drink, the transportation that moves us, the bridges that connect us, and the technology we rely on to communicate.

Ensuring the security and resilience of the Nation's critical infrastructure is a shared responsibility among multiple stakeholders that takes a "whole community" approach—neither government nor the private sector alone has the knowledge, authority, or resources to do it alone. By taking a whole community approach we are strengthening security systems, better sharing risk and threat information, collaborating on incident response, and maintaining confidence among the American public that critical infrastructure—our Nation's backbone—is secure, functioning and resilient.

In February 2013, the President signed Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience. The policies set forth in these directives take steps towards strengthening the security and resilience of our Nation's critical infrastructure against evolving threats and hazards. These documents call for an updated and overarching national framework that reflects the increasing role of cybersecurity in securing physical assets and the importance of building resilient systems in the face of a wide range of hazards.

These orders represent an integrated approach that strengthens the security and resilience of critical infrastructure against all hazards through an updated national framework that acknowledges the evolving risk environment and increased role of cybersecurity in securing physical assets.

Implementation of the Executive Order on Cybersecurity took a major step forward on April 3, 2013. The National Institute of Standards and Technology (NIST) conducted an all-day workshop to involve industry in developing a Cybersecurity Framework for critical infrastructure by voluntary adoption. DHS and the Department of Commerce participated in dialogue and information sharing with members of the private sector to begin to identify and collect best practices and standards that can be used across all sectors.

Several themes emerged from the NIST Workshop, including the importance of taking a risk-based (rather than absolute) approach to cybersecurity, the need for particular focus on control systems security, and of working collaboratively—across the government and with critical infrastructure owners and operators—in any effort to strengthen the security and resilience of the Nation's critical infrastructure.

Partnerships and information sharing are paramount for effective critical infrastructure protection and resilience strategies, and timely, trusted information sharing among stakeholders is essential to the security of the Nation's critical infrastructure.

Physical and cyber infrastructure have become inextricably linked. We rely on cyber systems to run everything from power plants to pipelines and hospitals to highways. This connection means that both cyber and physical security measures are required to holistically address the varying nature of potential attacks. Physical security

(Continued on Page 3)

(Continued from Page 2)

measures prevent unauthorized access to servers and other sensitive information technology equipment, protecting against insider threats, which leverage close proximity to networks, systems, or facilities in order to modify, gather, or deny access to information.

Conversely, cybersecurity measures can prevent an attack that could result in physical consequences. A successful cyber attack on a control system, such as those used in water treatment plants and energy facilities, could have devastating impacts on the health and safety of human lives and cause serious damage to the environment and the economy. These events frequently steal data, could disable systems, potentially disrupt business operations, and have the potential to destroy infrastructure. Individually, or in combination, these attacks could negatively affect the quality of life and well-being of all Americans.

Together, the Executive Order and Presidential Policy Directive create an opportunity to reinforce the need for holistic thinking about security and risk management and drive action toward a whole of community approach to security and resilience. These actions also create leverage to dramatically enhance the efficiency and effectiveness of the U.S. government's work to protect critical infrastructure.

A key tenet of the Presidential Policy Directive is to synthesize how the Federal government interacts with critical infrastructure partners on both physical and cyber security efforts. It presents an opportunity to refine the existing public-private partnership model for critical infrastructure to address cyber security risk, enhance risk management approaches, and improve multi-directional information flow.

To implement the policy directives, the Federal government has formed an interagency Integrated Task Force, facilitated by DHS. The task force consists of working groups designed to address the specific issue areas called out in the Presidential orders. These working groups are undertaking collaborative activities to develop: a voluntary cybersecurity framework; incentives to adopt such a framework; enhanced cyber threat information sharing among cybersecurity and critical infrastructure partners; a list of cyber-dependent critical infrastructures for which a cyber event could produce catastrophic impacts to public safety or national and economic security; and, efforts to ensure that privacy, civil rights, and civil liberties are addressed throughout the implementation of these activities.

Additionally, the Task Force is implementing the directives' call to evaluate the existing public-private critical infrastructure partnership model and mechanisms, and to revise or otherwise evolve any relevant national-level plans related to critical infrastructure security and resilience.

All efforts to implement the Executive Order and Presidential Policy Directive are being conducted in full collaboration and consultation with private sector, State, local, tribal and territorial (SLTT) governments, non-profit entities, and international partners.

To that end, the task force is using existing partnership structures and relationships across the Federal interagency, public and private sector, and SLTT arenas to identify and reach out to necessary stakeholders. The task force is also working with Sector Specific Agencies (SSAs), Federal field staff, and regional organizations and consortia to identify other opportunities to broaden its engagement to appropriate stakeholders that may currently partner in ways that are not as easily identified through current national engagements.

The policies treat partnership and consultation as both ends and means of activities they direct. The consultative process to be employed by the task force is intended to serve as a lasting framework for collaboration and information sharing that can be leveraged across all security, resilience, and risk-management activities moving forward.

The nature of threats and risks to critical infrastructure and cyber networks continue to evolve as the interdependence between the two increases. As such, our collaborative activities must also continue to evolve and expand. Participation in these efforts will form the model for future collaboration. Participation by all partners at this stage will ensure that our collective actions build on each other over time and represent an iterative approach to our shared security, resilience, and risk-management imperatives.

(Continued on Page 4)

(Continued from Page 3)

For more information about the Executive Order and Presidential Policy Directive as well as DHS's efforts in cybersecurity and critical infrastructure security please visit:

- Executive Order on Improving Critical Infrastructure Cybersecurity
- Presidential Policy Directive on Critical Infrastructure Security and Resilience
- Enhanced Cybersecurity Services
- DHS's efforts in cybersecurity
- DHS's efforts in critical infrastructure security ❖

16th Annual Emergency Management Higher Education Symposium
June 3-6, 2013
Emmitsburg, Maryland

From Theory to Doctrine to Practice
Background, Goals, and Objectives
Federal Emergency Management Agency, U.S. Department of Homeland Security

For representatives of colleges and universities which (1) have an existing hazard, disaster, or emergency management program, or (2) are attempting to develop and implement a program on their campus (e.g., a degree, certificate, minor, or concentration)

For more information click here.

Partnerships and Information Sharing: The Administration's Efforts to Enhance Critical Infrastructure Security and Resilience

by Nitin Natarajan, Director, Critical Infrastructure Policy
National Security Staff, The White House

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical and cyber spaces, and governance constructs that involve varied authorities, responsibilities, and regulations.

Within the critical infrastructure security and resilience mission space, partnerships and information sharing are perhaps two of the most important concepts, yet are often complicated to implement effectively.

To help enhance public-private partnerships and information sharing, the President signed Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience (CISR) on February 12, 2013. PPD-21 aims to strengthen the effectiveness of existing and new public-private partnerships and significantly expand current information sharing efforts. This directive allows the Nation to build upon the successes of the past while establishing a mechanism to closely integrate physical and cyber security efforts across the critical infrastructure sectors in an all-hazards manner in the future.

Partnerships can be interpreted to mean a wide variety of relationships including contractual, one-directional, or consensus based relationships. Within each of these models, the outcomes are traditionally set by one party and accepted or acquiesced to by the other. In a true partnership, we need to ensure all key stakeholders are at the table to develop and frame the "picture of success" that reflects the shared interests of all parties. Only through a true collaborative effort can we ensure the goals that are developed and the method in which those goals will be met are truly mutually beneficial.

The Department of Homeland Security began the work of developing a public-private partnership whereby government (Federal, State, local, tribal and territorial) and critical infrastructure owners and operators can work together to enhance the security and resilience of our Nation via the 2009 National Infrastructure Protection Plan (NIPP). This partnership takes place under the umbrella of the Critical Infrastructure Partnership Advisory Council (CIPAC) and engages on a variety of topics including risk assessment, information sharing, research and development, and the development of standardized metrics.

While the existing public-private partnership has created a foundational structure upon which much work has been done to enhance the resilience and security of the Nation, we are now in a position to evaluate the successes of the last few years and identify areas that require further development. How do we access areas of our critical infrastructure that may not be participating in the partnership? What is the current value proposition for owners and operators to participate in the process? How do we learn from non-CISR related public-private partnerships such as those established overseas in developing nations? These questions and others will be discussed and addressed as all levels of government, academia, private sector partners, and critical infrastructure owners and operators work collaboratively to frame the critical infrastructure public-private partnership of the future.

(Continued on Page 6)

[1]The White House. (2013, Feb 12). *Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience,* 2. Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

(Continued from Page 5)

The term information sharing can have many different connotations, each with its own complex challenges. Sharing machine readable data that is able to be ingested by various recipients poses a myriad of challenges. The sharing of finished analytic products may be too technical or not technical enough, depending on the audience. Sharing sensitive information across the Nation may not be accomplished in a timely manner. At each turning point, one party may be able to claim success while another claims failure. Identifying the information requirements, expectations and true capabilities (and gaps) early is critical to a successful information sharing program. PPD-21 brings together these diverse communities to address this challenge and build upon the progress made over the last decade.

Information sharing among critical infrastructure partners has taken a wide variety of paths and methods since the inception of the NIPP. Some critical infrastructure sectors have created robust Information Sharing and Analysis Centers, yet others have utilized secure web portals to share information with their partners. Some have closely integrated owners and operators in their response operations, while others have focused on cybersecurity efforts. Although extensive strides have taken place in progressing information sharing initiatives, there is much more that must be done. While there are mechanisms to share, one of the key challenges is defining what specific information requirements exist. With the understanding that neither partner is holding on to the proverbial silver bullet to solve each other's information gaps and that sharing everything is as effective as sharing nothing, more must be done to collect and share actionable information that leads to more informed decision making among all partners.

The Administration is committed to a transparent, inclusive, and collaborative process as we enhance our public-private partnerships and information sharing initiatives. Only through a truly collaborative effort with partners throughout the Nation can we truly enhance the security and resilience of our critical infrastructure. ❖

On-Site Registration!

THE 2013 CRITICAL INFRASTRUCTURE SYMPOSIUM

CELEBRATING 10 YEARS!
THE INFRASTRUCTURE SECURITY PARTNERSHIP™

"Advancing Full Spectrum Resilience"

April 15-16 • Thayer Hotel, West Point, New York

Hosted By: The Infrastructure Security Partnership, Society of American Military Engineers, the U.S. Army Corps of Engineers Engineer Research and Development Center, and the U.S. Military Academy at West Point

Please Click Here for Additional Information.

Introducing a New Partner: The Cyber Security Information Analysis Center

by Taz Daughtrey, James Madison University
Senior Scientist, Quanterion Solutions, Inc.

All critical infrastructure and key resource sectors depend in large measure on the successful operation of software. Yet the complexity of that software, and of its interactions with hardware and with human users, is quite daunting. The understanding and control of software-intensive critical systems is beyond the capabilities of any one entity, philosophy, or technique. It does indeed take a community … a community of practitioners and researchers from across a range of disciplines and organizations.

The critical infrastructure protection community now has a new and dedicated partner: the Cyber Security and Information Systems Information Analysis Center, or CSIAC. Established in 2012 through the consolidation and expansion of existing operations, the CSIAC (www.thecsiac.com) is fashioning itself as a "community of practice" within its scope of operations. The CSIAC supports the development, testing, validation, and transitioning of software engineering technology to the defense community, industry, and academia. Its subject areas encompass the entire software life cycle and includes software engineering methods, practices, tools, standards, and acquisition management.

The CSIAC brings together the resources of three predecessor entities: the Data and Analysis Center for Software (DACS), the Information Assurance Technology IAC (IATAC) and the Modeling & Simulation IAC (MSIAC), with the addition of Knowledge Management and Information Sharing technical areas. Information Analysis Centers (IACs) are research and analysis organizations established by the Department of Defense to support researchers, scientists, engineers, and program managers with expertise in all areas of Defense research and engineering. The CSIAC is one of eight such centers sponsored by the Defense Technical Information Center, the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today.

The Information Analysis Center Program is a resource to provide analysis, synthesis, and dissemination of relevant, timely, scientific, and technical information. Products such as State-of-the-Art Reports provide a detailed analysis of immediate critical challenges, while technical inquiry services offer a direct connection to a network of Subject Matter Experts from across government, industry, and academia. IACs maintain involvement in technical communities, collect research data, and conduct analysis to identify long term trends and provide recommendations to the acquisition community.

(Continued on Page 8)

*Image courtesy of sixninepixels/FreeDigitalPhotos.net

(Continued from Page 7)

Quanterion Solutions Incorporated operates the Cyber Security and Information Systems Information Analysis Center to serve as a Center of Excellence for the DoD in Cyber Security, Modeling and Simulation, Knowledge Management, and Software Engineering. The Center will be focused on leveraging knowledge bases, best practices, and expertise from industry, government, and academia in each of the technology domain areas. Quanterion also operates similar activities of the Reliability Information Analysis Center (RIAC).

The CSIAC operation is based at the State University of New York (SUNY) Institute of Technology in Utica, New York and at the Griffiss Institute in Rome, New York. Key members of the Quanterion team include Assured Information Security, SRC, AEgis Technologies, Syracuse University, the University of Southern California, and George Mason University.

The CSIAC has begun publishing a new quarterly print and digital *Journal of Cyber Security and Information Systems* available on its website, as are a number of other resources including:

- Software and Systems Cost and Performance Analysis Toolkit (S^2CPAT), a repository of size, cost, and schedule data reported on major weapon systems acquisitions at each acquisition milestone, with the goal of capturing and analyzing system and software engineering data.

- Software Development Tools and Technology Information Clearinghouse (SDTATIC), a searchable database that allows users to find, browse, and compare information on software development tools best for a specified development environment.

- ROI Dashboard, providing information on the costs and benefits of various improvements to software technology, based on historical data obtained from open source literature.

- Software Models Repository (SWMR), a centralized web-based repository to collect, analyze, and verify the existence and characteristics (including assumptions, limitations, and maturity) of software models for estimation, behavior, data, and object modeling.

- A large collection of previously produced reports, journal articles, "gold practices," a software engineering bibliographical database, and links to web resources.

The online Community of Practice will be used to gauge, through discussions and polls, interest and use of products including webinars, training, reports, and tools. The first major CSIAC publication was a June 2012 State of the Art Report, *Handbook of Software Reliability and Security Testing*. Similar reports are planned to be released as both topical updates and comprehensive reference volumes.

Interested professionals are invited to join the community at www.thecsiac.com/user/register. ❖

The Role of Communication in the Prevention of Terrorist Attacks

by Ross Johnson, CPP*

In the broadest sense, terrorism is an act of violence where the victim is not the intended target. In their selection of a victim (or victims), terrorists seek to send a message to someone else. For example, al Qaeda's 12 October 2000 attack against the U.S. guided-missile destroyer *U.S.S. Cole* was not just a raid against a warship—it was a message to the architects of United States policy in the Middle East. A similar message was sent with the 11 September 2001 destruction of the iconic World Trade Center.

The most common message that governments send back to terrorists is their refusal to negotiate. They use this tactic for two reasons: to reduce the threat of terrorist attacks by publically tying themselves to a position that would create political jeopardy later if they were to relent, and to deny the terrorists the status carried with the illusion of equality.

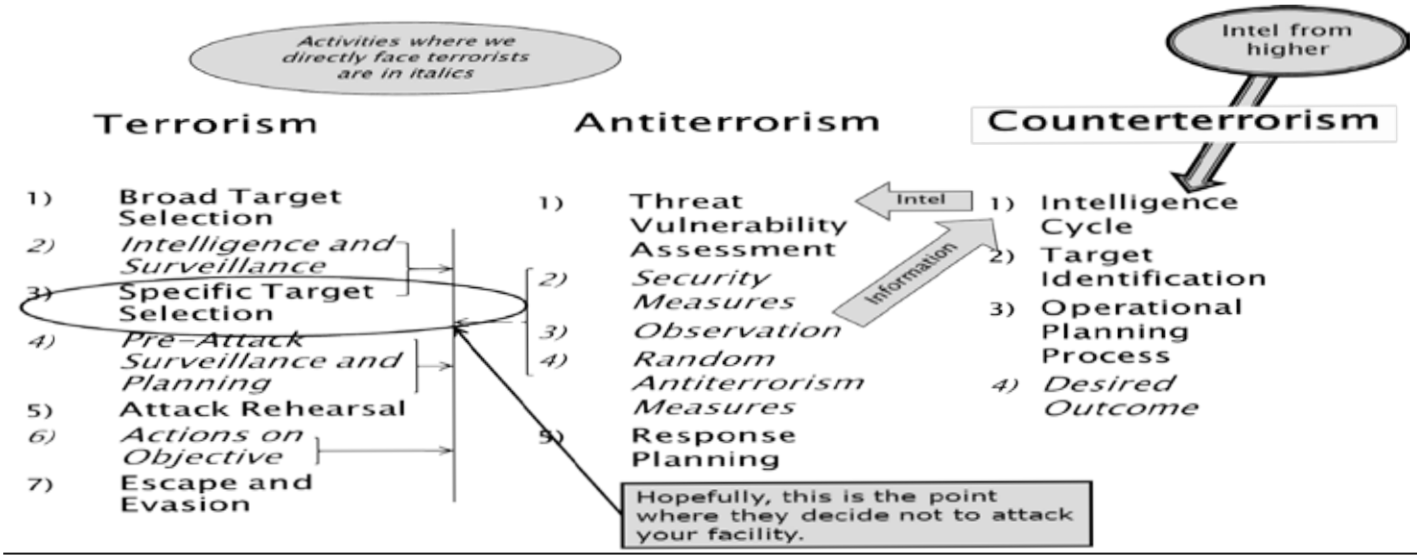
The Global War on Terrorism was based on a strategic message. In his 20 September, 2001 speech to Congress, President George W. Bush said, "Every nation, in every region, now has a decision to make. Either you are with us, or you are with the terrorists. From this day forward, any nation that continues to harbor or support terrorism will be regarded by the United States as a hostile regime."[1] By saying this, President Bush elevated the stakes, warning that terrorism would invite military attack against those nations that supported terrorists, with the hope that governments overseas that had remained passive about (or tacitly supported) the existence of terrorist groups in their midst would see it in their own best interests to become more active in their pursuit and more selective in their friends.

Security managers charged with the protection of critical infrastructure can send a message as well. First, though, a couple of useful definitions:

- Antiterrorism: passive measures designed to reduce the likelihood of terrorist attack. Activities related to antiterrorism are undertaken by the private sector, or government facilities not directly involved in the counterterrorism fight.

- Counterterrorism: those active measures undertaken by law enforcement, the intelligence community, militaries, and diplomats which are designed to hunt down and neutralize terrorist groups. This is almost always within the jurisdiction of governments.

The interaction between terrorist groups, antiterrorism planners, and counterterrorism forces is described in Figure 1, and explained below.



[1] Available at http://yc2.net/speech.htm.

(Continued on Page 10)

(Continued from Page 9)

Terrorist attacks are characterized by: very short duration; routine activities of authorities; little warning; and a quickly developing threat. These characteristics compensate for the overwhelming weakness of most terrorist groups—their inability to fight a sustained battle with government forces—which drives their absolute need to achieve surprise at their objective.

The best way for a terrorist group to achieve surprise is by thorough knowledge of the objective. What security measures are in place? What is the routine? Where are the weak spots in the perimeter? Are there any gaps in security? How do they handle visitors? Couriers? Deliveries? VIPs? Are they actively watching outside the perimeter? Where is the closest law enforcement or military post? How long would it take for an organized force to arrive at the objective? What is the routine of local police? The more information that a terrorist group can collect the more certain they will be of success.

To enhance the likelihood of success, terrorist groups follow their own routine:

- Broad Target Selection: a list of potential targets based on the intended target of the message

- Intelligence and Surveillance: information collected from all sources, including cursory surveillance

- Specific Target Selection: a comparison of the choices from the broad target list resulting in a decision of which one to attack

- Pre-Attack Surveillance and Planning: the collection of detailed information needed to successfully attack the objective

- Attack Rehearsal: usually conducted in a remote location free of unwanted observers

- Escape and Evasion: often necessary even in the case of suicide bombers, as there may be other terrorists nearby the bomber acting as spotters, photographers, or handlers

The message that security managers need to send terrorists is simple: *You will not be successful here*. To do this, we need to engage terrorists during their two information collection phases (Intelligence and Surveillance and Pre-Attack Surveillance and Planning).

Antiterrorism planning follows a routine as well. There are five distinct elements:

- Threat Vulnerability Assessment: an honest and thorough evaluation of the likely terrorist threats to a facility or organization. This assessment is usually site-specific, so a site in an area that has a past history of terrorist groups who possess both the capability and the intentions of attacking targets similar to your own facility will have a higher threat than a facility in an area with no known history of terrorist activity. An accurate threat vulnerability assessment depends on good relations with local counterterrorism forces, as their intelligence input is often crucial.

- Security Measures: a collection of measures that allow security managers to increase or decrease the application of security measures in consonance with the perceived threat level. These measures usually include static and mobile armed or unarmed security guards, closed-circuit television cameras, fences or walls, barbed or concertina wire, gates or other vehicle barriers, and procedures for access control of employees, visitors, and deliveries.

- Observation: a systemic process, called surveillance detection, that involves watching the most likely locations that terrorists will collect information on the target, including a mechanism for collecting useful information on unusual or suspicious activities and reporting it to someone in a position to act on it—usually security management and local counterterrorism forces. This supply of information is very important to counterterrorism, as often the first hard indicator of terrorist interest is in the targets they choose to watch. Inclusion of counterterrorism forces at this stage allows them to begin their operational cycle through countersurveillance (identifying, investigating and following surveillants)—hopefully disrupting the terrorist group long before they get to the attack itself.

- Random Antiterrorism Measures: a collection of unannounced additions to security measures which, when implemented singly, will change the security posture of the facility in a way that cannot be predicted by an observer. These measures are intended to

(Continued on Page 11)

(Continued from Page 10)

introduce doubt into the terrorist planning cycle, hopefully reducing its attractiveness as a target.

- Response Planning: Predetermined actions to be taken in the event of discovered surveillance, attack, fire, explosion, etc. Prompt response to all unwanted or unforeseen events will enhance reaction time and effectiveness, minimizing consequences and reducing the perceived value of the target to terrorists.

To work effectively, antiterrorism planners and counterterrorism forces cannot operate in isolation from each other. Effective liaison is required—antiterrorism planners need to meet with their counterterrorism counterparts on a regular basis, sharing information.

Counterterrorism forces need to understand that antiterrorism planners represent the target community, and therefore have a seat at the table. Antiterrorism planners need to understand that useful intelligence is critical to their work, so they need earn the trust of counterterrorism forces, which will require security clearances, proper protection of information, and discretion.

A principle of reciprocity should be fostered by both sides. Information flow in the fight against terrorism is not a one-way street. Counterterrorism forces simply cannot expect that information will flow one way from antiterrorism planners, and must be willing to share as much as information protection policies will allow. Antiterrorism planners have to understand that intelligence related to operations will only ever be shared if they are an active target, so cannot expect that they will be given information that they do not need to know to protect their facilities.

For antiterrorism planners, industry trade groups provide an excellent opportunity to concentrate expertise and disseminate information. A good example is the Canadian Electricity Association, based in Ottawa, Canada, which maintains a Security and Infrastructure Protection Committee (SIPC) that regularly meets with representatives of Canada's federal intelligence and law enforcement agencies, as well as policy makers in both Natural Resources Canada and Public Safety Canada. Through this liaison, the SIPC has the opportunity to inform and influence regulators on how best to protect critical infrastructure, and to share threat information with counterterrorism forces.

There are excellent liaison opportunities available internationally, as well. Two examples are through the North American Electric Reliability Corporation (NERC), and ASIS International.

The mission of NERC is to "ensure the reliability of the North American bulk power system." One of the many functions of NERC is critical infrastructure protection, and to assist in this it has created the Critical Infrastructure Protection Committee. NERC reliability standards and guidelines are used in Canada, the United States, and part of Mexico. The CIPC meets quarterly, and there are regular briefings on threats to the bulk power system from governments and federal agencies.

ASIS International is the world's largest professional association for security management. It maintains security councils that represent industry sectors around the world, sharing threat information, best practices, and developing guidelines for the industries they represent.

The Canadian Province of Alberta is a leader in the cooperation between counterterrorism forces and antiterrorism planners. The Albert Sheriff's Department, a provincial law enforcement agency, has created a unit called the Alberta Security and Strategic Intelligence Support Team (known as ASSIST) that: "manages counter-terrorism security information and intelligence and develops threat assessments. This area also provides a conduit for the flow of information between law enforcement, national security agencies and the private sector as it relates to Alberta's critical infrastructure."[2] ASSIST has become a critical one-stop shop for antiterrorism planners who have information to pass to provincial or federal agencies, but may not know who to contact; or need information, but don't know where

(Continued on Page 12)

[2] Available at https://www.solgps.alberta.ca/programs_and_services/public_security/sheriffs/Pages/default.aspx.

(Continued from Page 11)

to get it. ASSIST also saves a lot of time—instead of maintaining relationships with individuals in a large number of organizations with constantly-changing staffs, security professionals in Alberta only really need to know their contact at ASSIST. They also listen closely to industry in an effort to constantly improve their services.

Through good communications, antiterrorism planners and counterterrorism forces always enjoy an enormous advantage over terrorists. We have the ability to be everywhere at once, where terrorists are isolated by geography, technology, ideology, and a public only too willing to help defeat them. Our task is to recognize the advantages that good communications provides us, and support efforts to improve wherever needed.

* *Ross Johnson, CPP is the Senior Manager of Security and Contingency Planning for Capital Power, a power generation company based in Edmonton, Alberta, with power plants in Canada and the United States. Ross is the author of the recently-published book* Antiterrorism and Threat Response: Planning and Implementation, *published by CRC Press. He is also a retired Canadian Forces intelligence officer, and is currently the Chair of the Canadian Electricity Association's Security and Infrastructure Protection Committee, the Chair of ASIS International's Petrochemical, Chemical, and Extractive Industries Security Council, and an executive committee member of the North American Reliability Corporation's Critical Infrastructure Protection Committee.* ❖

The Center for Infrastructure Protection and Homeland Security Presents:
Fatigue Risk Management in Aviation Operations

The Symposium will equip attendees with the knowledge and approaches necessary to effectively fight fatigue in the operational setting. The human physiology of fatigue and the hazards it represents in the workplace will be explored, along with the effective methods and tools to conduct fatigue risk management, mitigate fatigue's negative effects, and enhance public safety.

This one day session will be held May 1, 2013.
For more information on registration and agenda click here.

The Criticality of Information Sharing in Countering the Financing of Terrorism Efforts in India

by Amit Kumar, Ph.D.
Center for National Policy, Georgetown University, and George Mason University*

Introduction

Like in any other area of homeland security and counterterrorism, information sharing plays a critical role in Countering the Financing of Terrorism (CFT). This piece explores the critical role of information sharing in CFT efforts in India, and how India is benefiting and can benefit further from adopting the information sharing paradigm in its CFT efforts.

Countering the Financing of Terrorism Efforts in India

India has been a victim of terrorism and the carnage engendered by terrorists and their sympathizers for several decades. However, the CFT paradigm is relatively new for India. Even in the United States, the heightened interest in terrorist financing and CFT is mostly a post September 11, 2011 occurrence. While the United States has made great efforts nationally, bilaterally, and multilaterally to engineer a CTF effort over the last decade, India has shown remarkable progress in this area more recently, especially since the November 2008 attacks in Mumbai, and the induction of the country into the Financial Action Task Force (FATF) in 2010.

Over the last couple of years India has made notable amendments both to its primary CFT law, the Unlawful Activities Prevention Act, and its main Anti Money Laundering (AML) law, the Prevention of Money Laundering Act. These amendments concern the inclusion of the production, circulation, and distribution of counterfeit currency; and the confiscation of terrorist assets, respectively. These developments are undoubtedly heartening for a country that is developing a CFT infrastructure.

But enactment of laws alone, while necessary, is not sufficient to design and implement a robust CFT effort. A vital component of any CFT effort is the information sharing processes that make CFT implementation possible. There is thus a need to understand the role of information sharing in the CFT domain.

Information Sharing in the Context of CFT Efforts in India

Over the past year there has been a lot of talk about the establishment of a U.S.-like National Counter Terrorism Center (NCTC) in India. The immediate impetus for the idea of the NCTC came after the intelligence failures related to the Mumbai attacks in November 2008. The notion that somehow the setting up of an NCTC would serve as a panacea to the intelligence bottlenecks and the anemic information sharing processes related to terrorist threats may be

(Continued on Page 14)

(Continued from Page 13)

more utopian than many in India would concede. Sure, since law and order is a state subject, and the proposed NCTC was supposed to have law enforcement powers, there are obvious concerns relating to the principle and practice of federalism coming under direct threat from the centrally established and run NCTC. What needs to be kept in mind is that the NCTC in the United States is the primary all source intelligence collection, analysis, and dissemination (information sharing) organization when it comes to terrorist threats.

While we wait on the denouement of the debate on the NCTC in India, the country faces existential threats related to terrorist financing. These threats need to be attended to and dealt with in order to help prevent future terrorist attacks in India. Certain issues merit urgent attention in this regard.

First and foremost, the Indian law enforcement agencies need to investigate very thoroughly the means that terrorists/criminals use to source, launder, move, store, and deploy funds. This information could be obtained by open sources, credible intelligence, and through thorough investigation of arrested terrorists and their financiers/facilitators. Secondly, law enforcement agencies should share this information with the Indian Financial Intelligence Unit, FIU-India. Thirdly, FIU-India may like to share with the Indian law enforcement agencies the analysis of the information it collects from financial institutions via Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs). This two way information sharing process is of paramount importance as it serves a three-fold objective—namely, the development of typologies for terrorist financing/money laundering that can then be shared with the financial institutions to inform and educate them on what transactions should be labeled suspicious and deserve further investigation; provide crucial information for successful prosecution and conviction of terrorist financing/money laundering offenses; and reduce the defensive filing of STRs by financial institutions—a cost consuming exercise that ends up adding to their regulatory burden and wasting precious manpower and financial resources. From all accounts, the lack of convictions/prosecutions has been a serious drawback for the CFT efforts in India thus far. A couple of recent developments potentially could bring cheer to proponents of seamless information sharing. The recent approval in principle by the Cabinet Committee on Security for the setting up of a National Intelligence Grid to streamline information sharing amongst intelligence agencies, law enforcement organizations, and other Government Departments is a good step in this direction. So is the completion of the design and development of core software for the Crime and Criminal Tracking and Network System, thus bringing the system for tracking criminal records that much closer to operational status.

Information Sharing in the CFT Realm in India and U.S.-India Collaboration

U.S.-India collaboration in information sharing relating to India's CFT efforts has proven to be remarkable and encouraging. There is much that the Indian CFT community can learn and is learning from the domain expertise of the United States as far as CFT efforts are concerned. Through ministerial level contacts, two-way official visits, and the institutional mechanism of the U.S.-India Counter Terrorism Joint Working Group, the avenues for U.S.-India information sharing relating to terrorist financing have expanded over the years. While the U.S. has signed a Mutual Legal Assistance Treaty (MLAT) with the Indian Government to facilitate exchange of information and evidence on criminal matters including banking and other financial records relating to money laundering cases, there may be an additional need for the Financial Crimes Enforcement Network and FIU-India to ink a Memorandum of Understanding (MOU) which would potentially further boost information sharing relating to best practices and operational experiences between the two FIUs. The Federal Bureau of Investigation (FBI) has provided terrorist financing instruction to participants from India. Financial supervisors from India attended the AML/CFT School run by the U.S. Treasury's Office of the Comptroller of the Currency (OCC) to increase their knowledge of money laundering and terrorist financing typologies and to improve

(Continued on Page 15)

(Continued from Page 14)

their ability to examine and enforce compliance with national AML/CFT laws. In partnership with the U.S. Department of State, the Federal Deposit Insurance Corporation (FDIC) has offered training sessions on AML/CFT issues to representatives from several countries including those from India. In addition, the FDIC met with a representative from the Insurance Regulatory and Development Authority of India to discuss issues relating to AML policies and procedures, the USA PATRIOT Act rules, SAR reporting requirements, and government information sharing mechanisms. Over the past few years, India and the United States have also engaged in a dialogue whereby India is trying to acquire U.S. technology to detect counterfeit currency—a long term crucial focus of its CFT efforts.

Despite India's recent efforts to spruce up its CFT initiatives, the lack of prosecutions/convictions/case law relating to CFT brings out an urgent and dire need for quantum improvements in investigative/prosecutorial capacity in this respect. From the U.S. perspective, this may explain the perceived inability on the Indian side to use the intelligence and investigational information provided to successfully prosecute terrorist financiers in India. Perhaps the law enforcement authorities in the U.S. and India could work together on training programs whereby the U.S. law enforcement agencies could share some of their expertise in this area, thus helping build Indian investigatory capacity.

Conclusion

This piece has offered an insight into the criticality of information sharing in building and implementing effective CFT measures in India. It is indeed heartening to discover that India is fast realizing this criticality and is working steadfastly to beef up its CFT efforts and its attendant information sharing processes. Even more productive is the ongoing collaboration through information sharing that the U.S. and India are witnessing in this realm.

** Dr. Amit Kumar is the Fellow for Homeland Security and Counterterrorism at the Center for National Policy; Adjunct Associate Professor at the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service; and Adjunct Senior Fellow at the Center for Infrastructure Protection and Homeland Security at George Mason University's School of Law.* ❖

Carpe Diem! An Opportunity to Improve Public-Private Information Sharing

by Andy N. Jabbour, Managing Director
Real Estate Information Sharing and Analysis Center (RE-ISAC)

In January 2012 the National Infrastructure Advisory Council (NIAC) completed a powerful report on Intelligence Information Sharing stating that, "Information sharing is perhaps the most important factor in the protection and resilience of critical infrastructure. Information on threats to infrastructure and their likely impact underlies nearly every security decision made by owners and operators, including which assets to protect, how to make operations more resilient, how to plan for potential disasters, when to ramp up to higher levels of security, and how to respond in the immediate aftermath of a disaster."[1]

Following the NIAC Report, President Obama released the National Strategy for Information Sharing and Safeguarding (NSISS) declaring, "As President, I have no greater responsibility than ensuring the safety and security of the United States and the American people. Meeting this responsibility requires the closest possible cooperation among our intelligence, military, diplomatic, homeland security, law enforcement, and public health communities, as well as with our partners at the State and local level and in the private sector. This cooperation, in turn, demands the timely and effective sharing of intelligence and information about threats to our Nation with those who need it…"[2] In February, the NSISS was followed by two significant documents that further elaborate on the necessary improvement in effective information exchange between government and the critical infrastructure community—Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience* and the Executive Order (EO) on Improving *Critical Infrastructure Cybersecurity*. Together, these four documents provide a backdrop and moment of tremendous opportunity to further encourage and develop current public-private information sharing initiatives and stimulate improved developments in the many existing opportunity areas with all levels of government.

PPD-21 directs that "The Federal Government shall work with critical infrastructure owners and operators… to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure."[3] To achieve the above, the Administration identified three "strategic imperatives," the second of which correctly identifies that "…a secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents. "[4]

For many years, the critical infrastructure private sector community

(Continued on Page 17)

[1]Berkeley, III A., Bush, W., Heasley, P., Nicholson, J., Reid, J., & Wallace, M. (2012, Jan 12). *National Infrastructure Advisory Council (NIAC) Intelligence Information Sharing Final Report and Recommendations*, ES-1. Retrieved from http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.
[2] NSISS, (2012, Dec.) Retrieved from http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.
[3] The White House. (2013, Feb 12). *Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience,* 2. Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[4] *Ibid.*, 6.

(Continued from Page 16)

has actively collaborated with the Federal government in exercises and and incidents to develop processes that provide timely, actionable intelligence from government to industry that can inform common situational awareness for all stakeholders and inform the decision-making processes critical infrastructure owners and operators must continually make. Within the current domestic threat environment, for both cyber concerns and the persistent threat of physical attacks against critical infrastructure and the people within them, effective information exchange requires a unified effort from all levels of government and in collaboration with all stakeholders. Owners, operators, associations, and information sharing entities such as the Information Sharing and Analysis Centers (ISACs)[5] are eager to work with partners in government to improve collaboration and more effectively exchange information to better inform our collective risk-based decisions and national security.

Very correctly, the NSISS states that, "Valid constraints on sharing information exist."[6] The ISACs and other critical infrastructure private sector stakeholders understand and respect that the government must protect sensitive information about intelligence sources and methods as well as on-going investigations. Further, those who receive sensitive information derived from intelligence reporting have a legal and ethical responsibility to properly safeguard that information. The Real Estate ISAC and the other ISACs that comprise the National Council of ISACs,[7] along with our members, look forward to continuing and improving our collaboration with our partners in government to ensure the effective and controlled sharing of information. The NCI and some ISACs, as well as some government partners, have adopted the use of such proven mechanisms as "traffic-light protocols" to ensure quick and easily understandable information handling requirements. We support the use of best practices and lessons learned to improve effective information sharing while ensuring reasonable measures are taken to safeguard information.

Along with much of the wisdom in the Administration's new guidance on information sharing, there are also some areas worthy of further consideration. Two of those areas, briefly addressed below, concern effective information sharing and the role of fusion centers.

Section 4 of the Cyber EO states that "… it is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities."[8] As the government prepares to implement the President's directive, it must be noted that the timeliness and quality of threat information are absolutely critical. Volume, in and of itself, is not necessarily helpful in supporting effective information exchange. Information sharing has a very specific purpose, well captured by the NSISS: "Ultimately, the value of responsible information sharing is measured by its contribution to proactive decision-making."[9] Effective information sharing has a specific intended outcome - informing the decision-making cycle of critical infrastructure owners and operators. That allows the owners and operators to make better informed, risk-based decisions when determining how to use limited resources to protect lives and secure critical infrastructure. Focus must be kept on providing timely, actionable information to the appropriate partners to inform effective decision-making and mitigate threats and hazards.

(Continued on Page 18)

---

[5] ISACs were established in *Presidential Decision Directive / NSC-63 - Critical Infrastructure Protection* (The White House, (1998, May 22)) . Retrieved from http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf).

[6] The White House. (2012, Dec 19). *National Strategy for Information Sharing and Safeguarding*, 5. Retrieved from http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

[7] "The mission of the National Council of ISACs (NCI) is to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. Members of the Council are the individual Information Sharing and Analysis Centers (ISAC) that represent their respective sectors." (National Council of ISACs. [2013]. Retrieved 2013, Mar 24 from http://www.isaccouncil.org/).

[8] The White House. (2013, Feb 12). *Executive Order- Improving Critical Infrastrucutre Cybersecurity.* Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[9] NSISS, at 7.

(Continued from Page 17)

Increasing the volume of information can create too much noise that drowns out the useful information and risks lessening the urgency given to information products.

To use a sports metaphor, information is like offensive yardage in a football game and the decision-making cycle is the like the end zone. An offense can rack up hundreds of yards in a football game but the yards, without penetrating the end zone and resulting in points, are rather useless save improving individual and team statistics. Similarly, the government can provide a tremendous amount of information to the private sector that could potentially satisfy internal metrics and program goals but if that information is largely unable to inform the owners' and operators' risk-based decisions by informing their decision-making cycles, there is little utility and little to celebrate.

Another area that merits additional consideration is the role of fusion centers. Last October, a U.S. Senate Report titled *Federal Support for and Involvement in State and Local Fusion Centers*[10] was completed. The Report drew considerable negative attention to fusion centers, leading Senator Tom Coburn of Oklahoma to say, "It's troubling that the very 'fusion' centers that were designed to share information in a post-9/11 world have become part of the problem. Instead of strengthening our counterterrorism efforts, they have too often wasted money and stepped on Americans' civil liberties."[11] In October, The Heritage Foundation's Matt Mayer wrote that DHS should "dramatically reduce the number of fusion centers."[12] Acknowledging the Report's reasonable findings of deficiencies in fusion centers and the legitimate concerns regarding civil rights and civil liberties, the Report fails to appreciate the necessary maturation of a very new part of the homeland security enterprise. Some fusion centers are effectively partnering with local law enforcement and local critical infrastructure partners through regular reporting and analysis, training, exercises, and other collaboration opportunities. The NIAC Study states that, "The use of fusion centers for sharing intelligence information with the private sector varies dramatically across locations and sectors, but overall seems comparatively modest"[13] but later notes that "Security directors in the Commercial Facilities Sector have shown an interest in actively building relationships with local law enforcement and fusion centers."[14]

In the Real Estate ISAC, we recognize that should there be a direct threat against a facility or when an incident occurs (whether the next big hurricane or a man-made event), the critical coordination will not occur between local commercial facilities and DHS, or with our ISAC, but between local businesses and local law enforcement, fusion centers and emergency management offices. At the end of last year, the National Council of ISACs established a working group focused on improving ISAC and fusion center information exchange and other areas of joint operational interest. Strongly supporting the "unity of effort"[15] referenced throughout PPD-21, the working

(Continued on Page 19)

[10] United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, Levin, C, Chairman, Coburn, T. Ranking Minority Member. (2012, Oct 3). Federal Support for and Involvement in State and Local Fusion Centers. Retrieved from http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

[11] Gerstein, Josh. (2012, Oct 3). *Lawmakers split over fusion center report* retrieved 2013, Mar 24, from http://www.politico.com/blogs/under-the-radar/2012/10/lawmakers-split-over-fusion-center-report-137411.html.

[12] Downing, M. & Mayer, M. (2012, Oct 3). *The Domestic Counterterrorism Enterprise: Time to Streamline* retrieved 2013, Mar 24 from http://www.heritage.org/research/reports/2012/10/domestic-counterterrorism-enterprise-time-to-streamline (the call to reduce fusion centers was repeated in a related article: Mayer, M. (2013, Mar 20). Homeland Security: Streamline America's Domestic Enterprise retrieved from http://blog.heritage.org/2013/03/20/homeland-security-streamline-americas-domestic-enterprise/.

[13] Berkeley, III A., Bush, W., Heasley, P., Nicholson, J., Reid, J., & Wallace, M. (2012, Jan 12). *National Infrastructure Advisory Council (NIAC) Intelligence Information Sharing Final Report and Recommendations*, ES-6, 20 and 41. Retrieved from http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

[14] *Ibid.*, D-18.

[15] The term "unity of effort" is used five times in PPD-21. A good definition of unity of effort is "Combining the assets, capabilities, exper¬tise, and resources of multiple participants." Blum, H.S. & McIntyre, K. (2012, Apr). *Enabling Unity of Effort in Homeland Response Operations.* Retrieved from http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=1108.

(Continued from Page 18)

group includes a number of ISACs, fusion centers, and federal government partners collaborating towards a common purpose focused on improving partnership and effective information exchange. Through the local expertise, fusion center capabilities, sector expertise, and reach of the ISACs, we think there is great opportunity to further develop meaningful, efficient, and effective information exchange to better inform the common operating picture, operations, and risk-based decision-making. This effort can also directly support the NSSIS's Priority Goal No. 9, to "Establish information sharing processes and sector specific protocols, with private sector partners, to improve information quality and timeliness and secure the nation's infrastructure."[16]

Over the next year, there are many details that need to be sorted through and codified in appropriate government plans and procedures. Certainly, the President can direct change and improvements—but that does not ensure they will occur. In a report last March, the Government Accountability Office stated, "The federal government and DHS have made progress, but more work remains for DHS to streamline its information sharing mechanisms and better meet partners' needs. Moving forward, it will be important that DHS continue to enhance its focus and efforts to strengthen and leverage the broader homeland security enterprise, and build off the important progress that it has made thus far."[17]

The recommendations of the NIAC Study, followed by the Administration's release of the NSISS, PPD-21, and the Cyber EO provide an opportunity to make real improvements in our information sharing activities and our national security. We are excited to be a part of this opportunity and are optimistic about the results we can collectively achieve. Carpe Diem; let's get to work. ❖

---

[16] NSSIS, at 9.

[17] Berrick, Cathleen. (2012, Mar 8). *Department of Homeland Security, Actions Needed to Reduce Overlap and Potential Unnecessary Duplication, Achieve Cost Savings, and Strengthen Mission Functions, Statement of Cathleen A. Berrick, Managing Director Homeland Security and Justice Issues,* 13. Retrieved from http://www.gao.gov/assets/590/589125.pdf.

The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks

Budapest, Hungary
June 24, 2013

A resilient system is a system that can, in the face of unknown, large-scale events, recover from failures and maintain its functions. It is known that many systems, such as biological systems, human mind, social systems, and dependable engineering systems exhibit this property. However, it is not clear how we should identify general "resilience" properties or strategies applicable to systems in many different domains. The purpose of this workshop is to bring the insights from various fields of resilient systems and explore common research challenges and design principles in the new discipline of "systems resilience."

Information and registration at: HTTP://2013.DSN.ORG/

InfraGard: A Time Tested Success in Results Oriented Public and Private Partnership for Information Sharing

Serving our Nation's critical infrastructure communities, InfraGard is a public-private partnership led by the Federal Bureau of Investigation (FBI). From its foundation in 1996 as a grass-roots effort to leverage the private sector information technology subject matter expertise providing vital insights for the FBI's Cleveland field office, Infragard has emerged as the Nation's premiere information sharing and collaborative effort between the public and private sector.

The local success of the Cincinnati initiative led to national adoption with InfraGard being positioned under the FBI's National Infrastructure Protection Center (NIPC). Like so many areas of critical infrastructure protection, the events of September 11, 2011 and the creation of the Department of Homeland Security (DHS) generated considerable changes. The NIPC moved to DHS with InfraGard retained under the FBI. In 2003, the FBI's Cyber Division was created containing the Public/Private Alliance Unit. The Public/Private Alliance Unit, later renamed the National Industry Partnership Unit (NIPU), supported the InfraGard program. Since its inception, InfraGard's scope has also grown from outreach to the IT community to much broader relevance across all critical infrastructure/key resource (CI/KR) sectors. InfraGard's membership base mirrors the sectors identified in the National Infrastructure Protection Plan (NIPP) and now across the 16 sectors identified in Presidential Decision Directive 21 (PDD-21) signed on February 12, 2013. InfraGard's roots in cybersecurity transcend all sectors of PDD-21 and its positioning under the FBI's Cyber Division ensures continued focus on the pervasive and dynamic cyber threat environment. However, InfraGard's service to the CI/KR communities of interest extends beyond cybersecurity to include the blending of all threat and hazards vectors in alignment and coordination with the FBI's other private sector outreach initiatives like the Domestic Security Alliance Council and the Strategic Partnership Program, as well as with other Federal, State, and local government and law enforcement entities, like DHS, fusion, and regional intelligence centers.

InfraGard's Organization

As a volunteer organization of over 50,000 members, InfraGard's mission is to protect the Nation's critical infrastructure through facilitated information sharing among vetted stakeholders. InfraGard's organizational structure is unique in terms of both its relationship with the FBI, a Federal law enforcement agency, and the incorporation of its 86 nationally dispersed chapters as 501(c)(3) non-profit organizations. This structure ensures retention of InfraGard's local-based, grassroots effectiveness with each chapter working closely with its FBI Field office from which there is a special agent assigned as InfraGard coordinator. Because of its affiliation with the FBI, InfraGard members have a direct conduit through which they can share information and intelligence with the FBI. Historically, information provided has been criminal, cyber, terrorism, and intelligence related. It is the trusted relationship between InfraGard members and the FBI which makes this information sharing mechanism work. Local and national FBI offices have a ready, vetted pool of subject matter expertise from which they can call upon as needed.

InfraGard chapters generally meet on a monthly basis and distinguished speakers from government—including FBI—and the private sector provide chapter members with valuable threat and security information as well as exceptional networking opportunities. InfraGard-hosted presentations address current and emerging threat dynamics, response and mitigation best practices, and information enhancing resilience applicable to InfraGard members. InfraGard also partners with sector specific

(Continued on Page 21)

(Continued from Page 20)

organizations of like interest, thereby extending the information sharing collaboration well beyond any single constituency. Many chapters mirror Federal, State, and local awareness programs broadening the public's understanding of cyber and other threats. For example, during Cyber Security Awareness Month in October 2012, the InfraGard National Capital Region Members Alliance chapter partnered with another non-profit organization to host a discussion about cybersecurity, threats, and mitigation strategies for small businesses.

InfraGard's Membership

InfraGard members are subject matter experts and leaders in private sector security. InfraGard membership represents the full spectrum of CI/KR sectors with specialties that are generally organized in Subject Interest Groups (SIGs). Member leaders within the InfraGard chapters design event programs and initiatives that connect experts with the membership to share and alert one another to the latest threats and effective countermeasures. All InfraGard members are vetted by the FBI and are provided access to a secure portal where unclassified intelligence products are posted by the FBI and other Federal and State agencies. Information shared within the InfraGard partnership includes alerts and advisories featuring cyber threats and vulnerabilities, terrorism and criminal trends and tactics, as well as severe weather alerts and security best practices.

InfraGard is a noteworthy example of a true public/private partnership generating tangible results in protecting our Nation's critical infrastructure. Together the FBI, businesses, and a vast array of subject matter experts collaborate on a daily basis across our Nation to share timely, relevant, and actionable information safeguarding vital CI/KR across the whole of communities across America.

Learn more about the InfraGard program and join at: www.InfraGard.org ❖

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

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