The Critical Infrastructure Protection Program September 2005 / Volume 4, No. 3

THE CIP REPORT

Regional Initiatives

Contact: cipp01@gmu.edu
703.993.4840

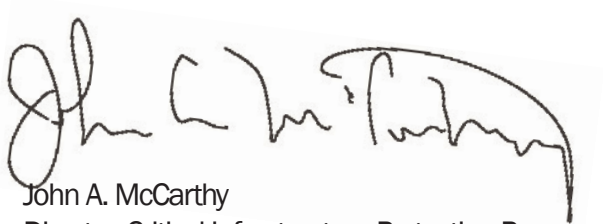
If you would like to subscribe to *The CIP Report* please click here. Visit us online for this and other issues at http://cipp.gmu.edu

This month's edition of *The CIP Report* is focused on regional public/private partnerships to advance critical infrastructure protection and homeland security objectives. At least a dozen such grass-roots organizations have sprung up around the nation and abroad.

This focus is reflected by the CIP Program's role in the National Capital Region (NCR). The Program serves as manager of a six-institution University Consortium for Infrastructure Protection, reporting to a Senior Policy Group (SPG) - the homeland security advisors to the Mayor of the District of Columbia and the Governors of Maryland and Virginia, as well as the Director of the Office of National Capital Region Coordination (ONCRC) of the Department of Homeland Security.

The SPG asked George Mason University and the Consortium to help them determine the state of risk management in each of eight sectors and to make recommendations for improvements. They also asked the Consortium to develop a framework to support regional decision processes to reduce risks due to infrastructure interdependencies that can contribute to cascading failures during disruptions in specific regions. Among the recommendations is a grass-roots public/private/non-profit partnership for critical infrastructure protection in the NCR.

Included in this issue are overviews of other regional public/private partnerships selected to exemplify the range of variation in approach. In addition, we are pleased to provide an interview with Tom Lockwood, Director of the ONCRC and a member of the SPG about the changing role of regions in the nation's CIP plans and his views on future NCR infrastructure protection. Additionally, we include a column by Jerry Brashear, CIP Program Associate Director who manages the Consortium for the NCR Project, which suggests a series of grass-roots regional partnerships, each tailored to the specifics of its region, is the necessary integration for an effective national CIP strategy. Finally, we have also included an opinion piece on the "Privacy, Security and Technology in the 21st Century" Conference.



John A. McCarthy
Director, Critical Infrastructure Protection Program
George Mason University, School of Law

The Necessity of Regional Public/Private Partnerships for Effective Critical Infrastructure Protection

Jerry P. Brashear, PhD
Associate Director for National Capital Region Projects, CIP Program

Preparedness, resilience and restoration of essential infrastructures, collectively "critical infrastructure protection" (CIP) are at present generally approached at two levels: First, industry and public agencies seek to protect their most important assets or systems of assets and to continue to provide services in a crisis. A rich foundation of risk management literature and practice supports this focus. Second, at the national level, broad "sectors" have been defined generally around aggregations of similar or related industries for the sharing of concerns, information, and "best practices" and for speaking with a coherent voice to the federal government on security matters.

A third perspective - the region - is the essential complement to these approaches that allows the whole structure to be integrated and effective.

Critical infrastructures are those systems that provide life-essential services to a defined population. Life-essential services are those that support life, health and safety, economic and national security, and public confidence and morale. In the physical (as opposed to cyber) world, man-made and natural disasters happen in a specific place, potentially affecting the ability of critical infrastructures to provide those life-essential services. That "place" is a specific region.

The significance of that statement is that events occurring in specific regions affect not just the infrastructure system that is the immediate target, but a variety of other infrastructures, creating a cascade of disruptions in life-essential services. The dependencies among infrastructures, especially critical infrastructures, have several causes, including:

- One infrastructure depends on another for services essential to its functioning, e.g., a disruption of electrical power used to pump water can result in a populace with neither power nor water; if some of that water is coolant in natural gas pumps, restoration of power (and, derivatively, water and natural gas) can be difficult.

- One infrastructure is located with another due to the common practice of sharing right-of-ways and water-crossings, e.g., a bridge may not only transport people and goods, but also natural gas pipelines, fiber optic communications lines, power lines, etc. - so a significant disruption to a bridge could deny numerous life-essential services to the residents on the "wrong" side of the bridge.


Jerry Brashear

These dependencies are so pervasive and interconnected that merely defining them is a major challenge. Many infrastructure owner/operators are unaware of the vulnerabilities and risks to them that originate in infrastructures on which they rely. Such dependencies can create circumstances where the infrastructure owner cannot capture the benefits of risk reduction investments because they accrue primarily to the customers of the infrastructure - or even to their customers. This results in systematic underinvestment in risk reduction by the first owner, a "market failure" that suggests government regulatory intervention, incentives or direct investment.

Compounding these dependencies and the market failures they create is the fact that most major metropolitan regions have multiple, overlapping jurisdictions and few if any regional mechanisms fully capable *(Continued, Page 3)*

Effective CIP *(Cont. from Page 2)*

of assessing regional risks, developing regional risk reduction programs and funding them at appropriate levels. Simply, we do not currently have the regional structures robust enough to meet the challenges of all-hazards critical infrastructure protection.

The solution lies in the recognition of regions as the necessary element in the national and local CIP solution. This has several implications:

- Each region must assure that incentives and tools are adequate to induce the owner/operators of critical infrastructures to conduct their own risk management at the asset and system levels and to invest in risk reduction and continuity of operations to the extent the business case can be made. This is the foundation on which a regional approach can be built. Competent risk management tools exist or are in development for virtually all infrastructures, except that they almost universally neglect dependencies - the signature concern of regions.

- Each region must develop its own awareness and understanding of its key dependencies because each region is materially different from all others. Public/private table top exercises focusing on dependencies have been shown to encourage this awareness. Such shared understanding permits an infrastructure that is vulnerable to disruptions of other infrastructures to encourage - or share in - risk reduction investments in reliability by its supplier. This would directly correct part of the market failure.

- Each region must organize a public/private/non-profit partnership for coordination and decision making with full accountability (based on systematic evaluation of risk reduction outcomes) to the regional stakeholders. These reflect the unique characteristics of the specific region and are often initiated by the private sector, which owns and operates the vast majority of the critical infrastructures. Not infrequently, such partnerships have emerged from the table top exercises that raise awareness of the pervasiveness of dependencies.

- Analytic tools beyond those needed for asset risk management are needed for regional risk management. The underlying logic is the same, but the referent is the delivery of life-essential services to the region's populace, as opposed to the asset. Full network analyses of vulnerabilities, consequences and risks are necessary assess the value of risk reduction investments, while accounting for the dependencies. In addition, methods to estimate the full distribution of benefits and costs of risk reduction investments are needed to support decisions as to which investments to make and whose funds should be used. Tools that can address these issues are still in development, but less refined ones can be applied.

These elements complement the asset and sector orientations, but do so in a way that integrates them into a comprehensive and effective whole. Without the regional partnerships, reducing risks of dependency-driven cascading failures of life-essential services cannot be achieved. However, a national strategy encouraging key regions to find their local solutions to common challenges in pursuit of common CIP and homeland security goals would, in aggregate effect, constitute a major positive, comprehensive step toward national resilience.

At least a dozen communities have drawn the conclusion that regional public/private partnerships are necessary for effective homeland security and critical infrastructure protection, a few of which are sketched in this edition of *The CIP Report*. In addition, a National Homeland Security Regional Initiative has been established as the organization of these partnerships for information sharing and coordination. ❖

Leadership Highlight

A Conversation with Thomas J. Lockwood

Director of the Office of National Capital Region Coordination
Department of Homeland Security

Fifteen months ago, Thomas J. Lockwood was appointed as the Director of the Office of National Capital Region Coordination (ONCRC) at the Department of Homeland Security. The office is charged with coordinating the prevention, preparedness and response capabilities of the National Capital Region (NCR). Mr. Lockwood recently sat down with The CIP Report *to discuss the work of his office and the accomplishments and challenges he encounters on a daily basis.*

The NCR is the only region specifically called out in the Homeland Security Act of 2002, where a special Office of National Capital Region Coordination is established. What makes the region so special?

When Congress was debating the Homeland Security Act of 2002, they wanted to have a single point of coordination for this region. This is a unique area because you have the executive, legislative, and judicial branches of government in a very tight geographic area. Along with that goes law enforcement, policy coordination, health and welfare coordination -- and we all have to work together. That is all in tandem with a commonwealth form of government, a state form of government, and the District of Columbia. We have to look at how constitutionally different the Commonwealth of Virginia is from the State of Maryland, and how they work with different levels of government, whether that's the county or municipal level, because again, in homeland security, all participate. We have a very complex area that is also geographically diverse-this is an urban area with a high number of commuters that come in from more rural areas. There are numerous dependencies crossing jurisdictions. We have to coordinate every single day between multiple levels of both public and private sectors.

Congress recognized that the inherent complexities in this region necessitated special focus and coordination.

This newsletter is dedicated to sharing information on critical infrastructure protection. What role does your office play in CIP and what are the particular challenges?

When we take a look at the whole region, people don't want to know how we become safer, they just want to know that we are safe. Americans have an expectation for a quality of life that includes a constant supply of clean and healthy water, reliable energy, access to roadways, the ability to make financial transactions 24/7, etc. The challenge for us behind the scenes is making this all seamless. And more important than quality of life issues *(Continued, Page 5)*

Thomas J. Lockwood is the Director of the Office of National Capital Region Coordination. Prior to this position, he served as the Homeland Security Advisor to Maryland Governor Robert L. Ehrlich, Jr. and as the Deputy Director of the Governor's Office of Homeland Security. Mr. Lockwood has degrees from Maine Maritime Academy and the University of Maryland, and is a graduate of the Defense Systems Management College, the National Defense University, and the Harvard Graduate School of Business.

Lockwood *(Cont. from Page 4)*
are public safety issues. When people pick up the phone and dial 911 for help, their expectation is that other people have thought through the entire process and that the right help will be on its way immediately. They are never going to pick up the phone and say, "Give me a virologist and an epidemiologist."

There are a number of dependencies, as we found out with Hurricane Isabelle. We saw interdependencies between the energy and water sectors. When we lost energy, because we don't have a gravity system here for water, we lost water as well. Thus the auxiliary generator systems that require water for coolant were in turn affected. So you have cascading infrastructure problems while 1.2 million people are without water. As we look at these issues, and the fact that these systems are owned by the private sector or by municipalities, how can we coordinate for reliability, sustainability, and security, and start thinking through the business models to go do that? Will legislation or regulation be required? Will businesses voluntarily adopt best practices? Furthermore, where do we share the risk for the common good?

How does CIP fit into overall homeland security efforts? What is the right balance between CIP efforts and other security priorities in the NCR, and how are resources spent?

Public funds are of course being spent primarily on public sector homeland security efforts such as first responder equipment or police overtime. But you cannot measure success in the amount of dollars spent. That is not our approach, that is not the approach of the region, nor the approach of either of the Secretaries that we have had, or any of the governors in this region. They understand that in certain areas there are pieces that require additional funds, focus, or support. In some cases, a particular jurisdiction or issue might gain more attention than others. Money spent is not a reliable metric, so when a county receives so many dollars and another county doesn't, or if a sector receives so much in dollars and another sector didn't receive any, it does not necessarily mean that one county or sector is more important than others.

Major regions around the nation are learning from each other and interacting on a regular basis. And that is exactly our expectation at DHS, that we all pull together, that we don't duplicate efforts, that we make the most effective decisions and investments.

When you look at critical infrastructure, you really find interdependencies across jurisdictions and the public and private sectors. How do you establish the forums for coordination between multiple stakeholders? The ONCRC has excellent partners in the private sector-- whether it's the water companies, energy providers, or the financial institutions, we have a very dedicated and informed team. So now the question is how do we sort out that balance of priorities? Are the additional substations that might be necessary in the event of an emergency something that for the public good should be a public capability? Or should that be a capability that the private sector would possess? And if the industry in question is regulated, how do we coordinate that with the regulators themselves and determine an allowable cost? We've seen our challenges here within the region where you have questions with regard to water quality-who pays for the enhancements that are necessary to that infrastructure? It will always be a question of who provides the resources, because the resources are limited.

What are your overall impressions of how much progress has been made and the effectiveness of partnerships across the region?

We have been evolving over the past several years from individual jurisdictions, groups, sets of practitioners, and very divided, compartmentalized pieces to a much more *(Continued, Page 15)*

Regional Public-Private Partnerships in Perspective

Christine Pommerening, PhD
Post-Doctoral Fellow, CIP Program


Christine Pommerening

In the beginning, the earth was without form, and void. No more. In modern societies, the land is divided up into a plethora of *geographical and functional units*; some of them independent, some overlapping, and some almost identical.

There are counties, cities, states, and countries, and military and congressional districts. In addition, localities in the U.S. and other countries are defined - or define themselves - as regions, zones, urban and metropolitan areas. While the first are about *government and jurisdictions* - local, state, and federal, the latter are about *governance and stakeholders* - public, private, not-for-profit, and even international. They are populated not only by people, but by organizations: partnerships, initiatives, alliances, forums, roundtables, coalitions, and networks.

With this abundance of arrangements and configurations, a clear designation of authority and responsibility is becoming more and more complicated. For example, there is no uniform definition of what a *region* really is. In fact, it is often this very ambiguity of an uncharted territory that spurs the formation of a regional partnership. Regions thus fill gaps that are left by even the most elaborate federalist structures and divisions of power within government, and between the public and private sectors.

In the case of homeland security, the traditional geographic and functional structures established by law enforcement and emergency services are still the dominant frame of reference for action. Given the devastation and loss of life in the 9/11 attacks, this is not surprising. But with the increasing understanding of the vital importance of technical and societal infrastructures, and the subsequent designation of 17 such sectors as critical for national and economic security and public confidence, the concept of homeland security has expanded. The protection of critical infrastructures spans the risk management continuum from planning and preparedness to response and recovery. Implementing comprehensive homeland security measures thus requires the integration of a broader spectrum of actors and issues. A regional arrangement seems to be the obvious solution to bridge the differences in mission and organization of public agencies, industry interests, non-profit and community groups for achieving disaster-resilient cities.

The following examples give a brief overview of six initiatives that vary in their mission, structure, and programs, but are common in their attempt to bridge geographical and functional boundaries along the risk management continuum.
(Continued, Page 12)

Pittsburgh Regional Business Coalition for Homeland Security

"Safest in America"
Pittsburgh Regional Business Coalition for Homeland Security

During 2004, representatives from the Pennsylvania Region 13 Task Force, the City of Pittsburgh, Allegheny County, several universities and local businesses came together with the goal of improving the region's readiness for disasters and therefore its economic stability. Several incidents such as the crash of Flight 93 on 9/11, the Que Creek mine collapse, and Hurricane Ivan have heightened the region's alert to the need for coordinated emergency response and planning. With seven founding members (Pennsylvania Region 13, *(Continued, Page 7)*

Regional Partnerships, Continued

Pittsburgh *(Cont. from Page 6)* the Allegheny Conference on Community Development, Westinghouse, FirstEnergy, RAND, the University of Pittsburgh, and the University of Pittsburgh Medical Center), membership is now tiered into 10 corporate sponsors, 2 associate sponsors, and 4 participants. The coalition has developed an initial list of program areas for further investigation and implementation, including:

- Compiling an inventory of physical assets, subject matter experts and volunteers, which would be beneficial in time of disaster and would be made available for use by emergency responders.
- Improving business-to-business communication by developing programs that address gaps in information regarding threat and response in the region.
- Working with federal, state and local organizations to determine education needs regarding regional disaster preparedness and disaster response, and support training programs focused on these specific needs.
- Working with other regional initiatives, state and local agencies, and Region 13 emergency responders to ensure that the region has an adequate program and necessary competencies in the area of threat and vulnerability assessment.

For further information and contact: http://www.pittsburghcoalitionforsecurity.org/

PNWER and the Puget Sound Partnership

Pacific NorthWest Economic Region

The Pacific North West Economic Region (PNWER) is a public-private partnership consisting of the American states and Canadian provinces of Alaska, Alberta, British Columbia, Idaho, Montana, Oregon, Washington, and the Yukon Territory. Established in 1991 through legislative statutes in all member states, PNWER's overall mission is to foster sustainable economic development throughout the entire region. In response to 9/11, PNWER established the Partnership for Regional Infrastructure Security, which held its first meeting in November 2001. This was the first bi-national, regional meeting of stakeholders in North America and brought together over 120 private and public sector representatives to begin developing a cooperative preparedness strategy aimed at enhancing the security of critical systems region-wide. The goal was to enable stakeholders to quickly take the actions necessary to deal with disruptions to economy, public health and safety.

PNWER is now fostering the development of local partnerships for developing and sharing best practices. The Puget Sound Partnership, for example, is conducting regional exercises on critical infrastructure interdependencies called Blue Cascades. The most recent one was held in September 2004 in collaboration with the King County Office of Emergency Management (Region 6, Washington Homeland Security District), the Federal Emergency Management Agency (FEMA region X), Public Safety and Emergency Preparedness Canada (PSEPC), and the Washington State Military Department. The exercises are designed so that *(Continued, Page 8)*

The Blue Cascades II regional exercise enables participants to identify the needs, priorities, and resource requirements for an Action Plan to assist the PNWER jurisdictions to become a disaster-resistant/ resilient region. The lessons learned will help sensitize public and private sector decision makers to infrastructure reliability and security issues.

Regional Partnerships, Continued

PNWER *(Cont. from Page 7)* participants can discuss the impacts of attacks and disruptions on each represented infrastructure by "thinking aloud and outside the box." This setting allows participants to become familiar with other infrastructures and the potential for cascading effects as a result of interdependencies, and to develop a strategy for a disaster resistant region.

In February 2005, an Interdependencies Project Working Group (IPWG) has been established to work with technical experts from the U.S. Department of Homeland Security for developing requirements for information sharing protocols and other facilitation mechanisms. The process is intended to lead to a Memorandum of Understanding between the participating public and private sector organizations that identifies what needs to be done, who will do the work, how it will be undertaken, and costs associated with it.

For further information and contact: http://pnwer.org/pris/index.htm

Potomac Conference Emergency Preparedness Task Force

GREATER WASHINGTON Board of Trade POTOMAC CONFERENCE

After the September 11, 2001 attacks the Potomac Conference of the Greater Washington Board of Trade convened a group of the region's leaders to establish a plan to restore public confidence and to build community preparedness. As a way to integrate businesses and non-profit organizations into emergency preparedness planning, the Emergency Preparedness Task Force was organized, initially led by George Vradenburg, Strategic Advisor to AOL Time Warner, John Derrick, President and CEO of Pepco, Catherine Meloy, Senior Vice President of Clear Channel Communications and John Veihmeyer, Partner at KPMG, Inc. The Task Force now meets on a quarterly basis and focuses its efforts on advocacy, business continuity and communications.

The Advocacy Work Group concentrates on identifying policies on state and federal levels to improve emergency preparedness in Greater Washington, which is a complex institutional mix of more than 17 local and state jurisdictions, plus numerous agencies of the federal government.

The Business Continuity Work Group develops continuity plans through seminars and direct support and mentoring, in particular for small and medium sized businesses. It is maintaining a private sector inventory for support of first responders, and has funded an economic impact study to assess risk and determine best practices for regional economic recovery. *(Continued, Page 9)*

The Potomac Conference was instrumental in achieving the re-opening of National Airport after the 9/11 attack on the Pentagon. At the time, the loss of its closure was estimated at $326 million dollars, affecting 18,000 workers. A longer or even permanent closure would have been a major impediment of economic recovery of the region.

"Media and the First Response" is a national model for helping federal, state and local public information officers and the media better communicate to the public during a crisis. In May 2004, this program was rolled out nationally in 10 cities across the country by the U.S. Department of Homeland Security.

Regional Partnerships, Continued

Potomac Conference *(Cont. from Page 8)*
The Communications Work Group addresses Greater Washington's emergency communications gaps including cross-jurisdictional coordination, infrastructure expansion, and contingency plan development. It has launched "Media and the First Response" a national model for helping federal, state and local public information officers and the media better communicate to the public during a crisis. In May 2004, this program was rolled out nationally in 10 cities across the country by the U.S. Department of Homeland Security.

For further information and contact: http://www.potomacconference.org/preparedness.html

The Business Executives for National Security and the New Jersey Business Force

The New Jersey Business Force (NJBF) was launched in March 2003 as a partnership between the Governor of New Jersey and its state agencies, and the Business Executives for National Security (BENS; founded in 1982). NJBF aims at complementing state efforts by providing private sector resources in preparing for and responding to catastrophic events or terrorists attacks. NJBF now includes over 30 companies, and is funded through corporate contributions and a grant by the DHS Office of Domestic Preparedness (ODP). Its initiatives focus on asset availability, business volunteers, medical preparedness support, information sharing, and training & exercise.

In April 2005, the New Jersey Business Force held a Private Sector Roundtable that served as a gap analysis of the TOPOFF 3 exercise. Twenty private sector companies and organizations along with the DHS T3 Private Sector Controller and a NJOEM Private Sector Liaison Desk representative participated, as well as observers from academic, local, state, and federal agencies.

Through the Business Response Network and its inventory database, private sector companies pledge resources (e.g., trucks, warehouses) to the State during a major disaster based on pre-identified needs. Companies agree to have employees identified and trained as volunteers as part of an overall community response to a terrorist event or other major disaster. In partnership with the Center of Disease Control' s Strategic National Stockpile, a Point-Of-Distribution (POD) demonstration project for mass immunizations has been conducted on-site at a member company. In conjunction with NJN Public Television & Radio, a private channel Datashare Datacasting Program for NJBF members has been developed and piloted. In addition, NJBF private sector members received pro bono access to the NC4 system, a real-time, two-way communications capability. The BENS-NJBF model is now being implemented in other regions as well, among them Georgia, MidAmerica, and Bay Area Business Force.

For further information and contact: http://www.njbusinessforce.org/NJBF_About.htm

Regional Partnerships, Continued

London Resilience

London Resilience is a strategic partnership of key emergency preparedness and response organizations and bodies in the British capital in both the public and private sectors. Created in 2001 in the wake of the 9/11 attacks in the U.S., its task is to ensure the preparedness of the Greater London area for major incidents or catastrophes. There are two main components: The London Resilience Team as operative arm, and the London Regional Resilience Forum as strategic leadership arm.

The London Regional Resilience Forum oversees the work of all London Resilience actions. It is composed of senior officials representing the main emergency organizations and key sectors within the partnership. It is chaired by the cabinet-level Minister for London Resilience, with the Mayor of London as deputy chair. The Forum reports directly to the government, and has a number of sub-committees and working groups that concentrate on particular aspects of London's preparedness. These include:

- The Blue Lights Sub-Committee (dealing with matters related to the emergency services)
- The Utilities Sub-Committee (dealing with matters affecting the key utilities such as water, gas and telecommunications)
- The Business Sub-Committee (representing the general business community)
- The Health Sub-Committee
- The Transport Sub-Committee
- The Communications Sub-Committee (warning and informing the public)
- The Local Authorities Sub-Committee
- The Voluntary Sector Sub-Committee

The London Resilience Team grew out of an inter-agency team that reviewed the status quo of London's preparedness in 2001. The core of the team consists of civil servants, complemented by specialists from private sector organizations. The team is based within the Government Office for London, and has currently members from:

- The Metropolitan Police Service, the City of London Police, and the British Transport Police
- The London Fire Brigade and the London Ambulance Service *(Continued, Page 11)*

The new strategic emergency planning regime embodied in the concept of London Resilience was put to the test during the London Underground and bus bombings that hit the city on July 7, 2005 and the repeat attempts only two weeks later. During those incidents, the Commissioner of the Metropolitan Police took charge of the so-called "Gold Coordinating Group", which brought together the top management of the London health service, local councils, emergency services, utilities, transport and port authorities. While a detailed review is still being conducted, the fact that most buses and trains were running and the City was 'open for business' again the very next day appears to have proven the concept.

Regional Partnerships, Continued

London *(Cont. from Page 10)*

- The National Health Service
- The Greater London Authority
- Corporation of the City of London, Emergency Planning Department
- London Fire & Emergency Planning Authority (LFEPA)
- The Government Information and Communications Service
- Transport for London, and the London Underground
- British Telecom
- The Salvation Army

For further information and contact: http://www.londonprepared.gov.uk/resilienceteam/index.htm

ChicagoFIRST

ChicagoFIRST is indeed the first regionally based organization in the U.S. dedicated to enhancing the resiliency of the financial community in a specific geographic region. Formed as a coalition for business continuity in 2003, it fosters business recovery coordination and planning among its members, and implements programs at crucial interfaces between private businesses and governments at all levels.

In January 2004, the organization became a limited liability company owned by the following firms: LaSalle Bank/ABN AMRO; Chicago Board Options Exchange; Chicago Mercantile Exchange; The Northern Trust Bank; UBS Warburg; Harris Bank; Archipelago; Chicago Stock Exchange; BankOne; William Blair & Company; Mesirow Financial; Mizuho Securities; The Options Clearing Corporation; and Bank of America.

ChicagoFIRST's key strategic partners include the City of Chicago, Department of Treasury, Department of Homeland Security, BITS, Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Deposit Insurance Corporation, Illinois Commissioner of Banks and Real Estate, Federal Reserve Bank of Chicago, Board of Governors of the Federal Reserve, Office of the Comptroller of the Currency, U.S. Secret Service, Federal Bureau of Investigation, Financial Services Sector Coordinating Council, and the Futures Industry Association.

ChicagoFIRST public-private partnership activities focus on three issues: crisis communication credentialing, and evacuations/sheltering in place.

The coalition has a seat at Chicago's Joint *(Continued, Page 12)*

ChicagoFIRST, along with the City of Chicago, the City of Chicago Police Department, and Chicago's Building Owners and Management Association, is developing an interim system to credential business personnel essential to the continuity of operations so that they can access sites otherwise restricted to emergency personnel in the aftermath of a disaster.

Regional Partnerships, Continued

ChicagoFIRST *(Cont. from Page 11)* Operations Center (JOC) and thus first-hand information about any disaster or emergency and how the city plans to respond. ChicagoFIRST members staff the center on a 24x7 basis when the threat alert level is elevated to orange or red, or the JOC is otherwise activated by local authorities.

A project team consisting of ChicagoFIRST, the City of Chicago, the City of Chicago Police Department, and Chicago's Building Owners and Management Association is developing an interim system to credential business personnel essential to the continuity of operations so that they can access sites otherwise restricted to emergency personnel in the aftermath of a disaster.

Finally, the coalition has participated in exercises with the City of Chicago to test evacuation procedures, and works on ways to coordinate how the central business district can be evacuated, if necessary, and ensure that the financial community's procedures complement those of the government.

For further information and contact: https://www.chicagofirst.org

Regional Partnerships *(Cont. from Page 6)* There are several lessons from the experience to date in establishing regional initiatives. One is that contrary to prior issues such as environmental protection, the main problem is not so much overcoming federal barriers, but intra-regional disconnect and discord. The federal government provides funding through various grants such as the Urban Area Security Initiative, and if not an outright enabler through such programs, DHS is at least continually inviting participation and feedback from regional and private sector representatives. But devising a membership and leadership structure that is inclusive of all stakeholders while remaining operationally and financially independent seems to be the biggest challenge for regional coordination efforts.

Another is that in the aftermath of 9/11, safety and security were, and still are, widely shared goals to rally around. There is a tremendous amount of goodwill by individuals in both public and private sectors. Translating this into actionable programs proves more difficult. There are some low-cost/high-benefit projects such as private sector inventories for use in disaster response, or electronic alert notification systems. More difficult and long-term issues such as cost recovery for investments in infrastructure service reliability require more than technical or administrative support through a regional initiative.

The obvious dilemma of homeland security preparedness in general and CIP in particular is that it usually takes a worsening crisis and regular failures of systems to maintain alertness and investments, while the very purpose of these initiatives is just the opposite - to avoid crises and increase reliability.

At the same time, while the need for more regional coordination due to the interdependency of systems is generally acknowledged among the stakeholders, it is difficult to sustain the initial level of awareness and action. The obvious dilemma of homeland security preparedness in general and CIP in particular is that it usually takes a worsening crisis and regular failures of systems to maintain alertness and investments, while the very purpose of these initiatives is just the opposite - to avoid crises and increase reliability. In light of this dilemma, the greatest strength of the regional approach might well be providing a platform for partnerships based on stable relationships and shared resources rather than one contingent upon changing threat environments or vulnerability levels. ❖

Legal Insights

Privacy and Security: A Procedural and Structural Approach

Maeve Dion
CIP Program Legal Research Associate

This summer, the CIP Program held a conference titled "Privacy, Security and Technology in the 21st Century: Addressing the Legal Landscape of Today and Tomorrow." The conference was co-hosted by Distinguished Adjunct Professor of Law John O. Marsh and Angie Chen, and speakers included Nuala O'Connor Kelly, Stewart Baker, John Poindexter, M.E. Bowman, Kate Martin, Paul Rosenzweig, and others. Some speakers and attendees have written opinion articles in response to the conference debates, and the CIP Program looks forward to offering a collection of these articles soon.

Stewart Baker has argued that fears of theoretical privacy abuses limited our ability to guard against the terrorist acts of September 11, 2001. These same, valid fears seem to motivate Kate Martin's critiques of proposed government technologies. At the conference, we witnessed Kate and Stewart, and then Kate and Admiral Poindexter, tossing the conversational ball back and forth as they sought to find an acceptable set of rules to keep technology from violating individual privacy.

However, to cite a well-used phrase, technology doesn't abuse privacy; people do. Framing the "Security and Privacy" conversation around specific, rules-based technological mandates is an entertaining, but distracting disservice to the importance of our discussion. This discussion should address flexible, comprehensive, structural protections, not merely protections based on technology rules. Technology restrictions cannot be the focus of our privacy and security dialogue for several reasons.

First, prohibiting the government from developing certain technologies will not stop the technology from being created. In fact, many of the scary, potentially privacy-invading technologies already exist -- because they are useful for various beneficial purposes in the private sector. As conference attendee Professor John Bagby commented, the genie is out of the bottle.

Second, the cycle of proposing software, and then being forced to scrap it because its technology rules do not protect against theoretical privacy abuses, could become a never-ending process that ultimately does little in the real world to provide a proper blend of privacy and security. We have already seen several iterations of this kind of cycle. And in the meantime, the government is using technology now, perhaps overprotecting or under protecting both privacy and security.

Third, even if the government were "banned" from setting up certain technologies, that wouldn't stop abuses of privacy. Creative people can always get around rule restrictions. For example, if the government were prohibited from running a certain targeted search in an interlinked system of databases, the same result could be obtained by creatively combining several searches in distinct databases. If these searches resulted in an abuse of privacy, the abuse would be neither detected nor prohibited by a rule that banned interlinked databases and specific targeted searches.

Fourth, no legislative privacy "rule set" could independently ensure protection. Rules might govern technology contracts, but to be confident in privacy protection, we need oversight and compliance enforcement. For example, recent studies have shown government agency improvements in including security and privacy protection provisions in contracts with private-sector providers; but the same studies have shown a lack of follow-up to see if the contractors have complied with the written requirements. Even if we could magically define the full set of proper technology restrictions, we would *(Continued, Page 14)*


Maeve Dion

Legal Insights *(Cont. from Page 13)* still need to develop a structure to oversee compliance and enforcement. Further, with the speed of technology changes, a legislative "rule set" could become outdated before it is enacted.

Thus, although technology should be an aspect of our "Security and Privacy" conversation, it should not be a central or controlling concept. I agree with Kate Martin that the speedy electronic assembly, searching, and sharing of comprehensive, individual dossier is a modern concern that poses very real dangers. However, our fears of privacy abuses may be better assuaged by a flexible, comprehensive, structural protection rather than by a protection based on technology rules.

Perhaps history can help us figure out how to create these structural protections. Our current, high-technology society was not the first to be concerned about protection from the specter of an overreaching government. In his introductory comments, Secretary Marsh mentioned our Constitutional checks and balances, developed by the Founders to help secure justice and liberty. One of the Founders' concerns was to provide protections for the people against abuses by a tyrannical national government.

Kate Martin said the Founders' concerns of protection from the government were not comparable to today's concerns of personal privacy protection from the government because the Founders did not face today's reality of "having the FBI in your living room." I acknowledge that today's government possesses impressive surveillance tools, but the Founders faced British soldiers bivouacked in their private residences. Although the comparison is not exact, the Founders were well aware of the dangers of tyrannical government infiltrating every-day private lives.

Just as our privacy concerns today were valid in the 1780s, the privacy protections the Founders introduced may be valid and useful today. Fears of abuses of power were integral to the Founders' decisions of how to structure our government. The concepts of separated powers, checks and balances, and Article III courts act as mechanisms for protection against aggrandizement and abuses of power. These are critical concepts to keep in mind during our "Security and Privacy" debates.

The Founders developed a flexible solution that focused on the structure of government; they did not establish strict rules regarding the minutiae of every-day life. Kate Martin argued that the Bill of Rights, a "set of rules" ratified a few short years after the Constitution, provided strong protection for the people. On one hand, she is of course right; but on the other hand, the Bill of Rights needs the Constitutional procedures that give it teeth. The words of our Bill of Rights, similar to the words of any legislation attempting to limit government databases, provide little protection standing alone. Rather, the structure of our Constitution empowers these rights and empowers the people by establishing oversight and enforcement mechanisms.

So instead of defining rigid, technologically-focused, temporally-limited legislative rules, perhaps we should be developing checks and balances--procedural and structural capabilities to ensure that theoretical abuses of power do not occur. Then, private individuals can more confidently trust that theoretical abuses of power will either remain theoretical or will be detected and corrected before our essential liberties are violated. And our government can more confidently move forward in using technology to improve our security. ❖

Lockwood *(Cont. from Page 5)* integrated community. We look at issues that affect the region and try to think about those issues cohesively, learning from each of these major events and folding them back into what we do. That requires active participation of public, private, and volunteer communities as a matter of course. How do we set up forums that need to be established, and how do we leverage existing bodies? For example the Metropolitan Washington Council of Governments, where you normally are gathering the practitioner community and policy makers, should be encouraged and supported in their work. We also need to identify the forums that exist and that with additional support could be very effective. And there are many coordinating forums within the federal government as well. We are much more integrated than in the past.

One of the challenges is getting a large group of people to start having a shared vision. There is no governor, mayor, police chief, fire chief, or health officer that is going to walk away from their primary responsibilities. They are hired, elected, or nominated for their positions because of their leadership qualities. And now that they're in that job, how do they respect their own jurisdictional duties but also come together as part of a regional community? One of our big challenges is developing an integrated vision for where we want to go as a region--and this is what we've been working on for some time now. In fact, we will be releasing a document outlining our vision, goals, and strategies during National Preparedness Month in September.

The thing about homeland security is that everyone participates. Look at the work of the CIP Program in supporting federal, state and local initiatives. They have been good neighbors in engaging with us and providing guidance and advisors.

We have recently been building bridges in the areas of continuity of government and continuity of services. We have an issue of people having to cross jurisdictional boundaries with no way of identifying themselves as who they are except for the badge that they use to enter their work buildings. As we look at this, how do we get people to go where they need to go? Doctors need to get to hospitals, first responders need to get to incidents. As you look at this complicated area, how do we better coordinate emergency management? Many people are talking about "credentialing" which means different things to different people. How do you do this in a more effective way than just having people obtaining the right badges?

What we've been seeing as we work with different communities is how they come together as a region, defining what they want as an outcome, determining how community members are going to take different lead roles, and creating the information exchanges so that we can cut the learning time, we can commit to projects, and we can move forward at a much more accelerated schedule. It just takes a lot of effort.

Outside of partnership building, what other steps and initiatives for the NCR are underway to advance homeland security and critical infrastructure protection?

The first part of our job was identifying policy and priorities, the second part is addressing those. For example, a very methodical approach has been taken on the rail sector in the NCR. Federal, state, and local governments teamed up to look at the rail corridor, thinking through tactics, operations, procedures, risk assessment, and the best way to effectively spend and target limited resources to reduce risk. The Transportation Security Administration and the DHS Directorate for Information Analysis and Infrastructure Protection have been actively engaged in this project for some time, and have worked with many partners - local government, state government, the private sector and other federal agencies. The team is now implementing some of the piloting efforts, such as camera technology and fusion sensors. This has been a *(Continued, Page 16)*

Lockwood *(Cont. from Page 15)*
coordination effort in which multiple parts of DHS including Science and Technology, the Department of Transportation, the Federal Railroad Administration, local and municipal jurisdictions and industry have integrated well. We are implementing similar coordination efforts in the water sector.

Another area we've been focusing on is an information campaign for leveraging federal messages at the local level. We've developed an awareness campaign with all of the jurisdictions in the NCR which we will launch during September and October, in conjunction with National Preparedness Month. We want communities to know where to go for information and ultimately to raise the overall preparedness of the region. Two points that we will emphasize in the NCR have to do with water and communication plans. Through surveys we have recognized that while many people in our region are prepared with a radio, extra food supply, and other materials that could be helpful in an emergency, most people do not have a supply of extra water nor have they developed a communications plan with family, friends and colleagues. If we were able to address these two items alone we would double the preparedness of the region. ❖

Protected Critical Infrastructure Information (PCII) Program Announces Electronic Submissions Capability

The Department of Homeland Security is now accepting electronic submissions for the Protected Critical Infrastructure Information (PCII) Program. This new capability allows the private sector to quickly and easily submit its critical infrastructure information (CII) to DHS, which, in turn, may share this information with government entities that have infrastructure protection responsibilities, thereby helping to safeguard and prevent disruption to the nation's economy and way of life.

CII can be submitted electronically through a secure Web portal accessed from the PCII Program Web site at www.dhs.gov/pcii. Submitted files are encrypted in transit and strict safeguarding procedures prevent unauthorized access. This information is used by government analysts to assess threats and vulnerabilities, evaluate physical security risks, and create reports which may improve the government's ability to respond to terrorist attacks and aid in recovery efforts.

The PCII Program, created as a result of the Critical Infrastructure Information Act of 2002 (CII Act), enables the private sector to voluntarily submit sensitive information regarding the nation's critical infrastructure with the assurance of protection from public disclosure, state and local sunshine laws and use in civil litigation. CII that meets the qualifications for protection under the CII Act will be exempt from the Freedom of Information Act and will not be divulged to competitors.

Visit the PCII Program Web site at www.dhs.gov/pcii for more information about the electronic submission process including guidelines, a checklist and Frequently Asked Questions. For questions, call the PCII Program Office at 202-360-3023 or send an email to pcii-info@dhs.gov. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

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