THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 2

AUGUST 2006

NATIONAL INFRASTRUCTURE PROTECTION PLAN

EDITORIAL STAFF

EDITORS

Jeanne Geers

Jessica Milloy

STAFF WRITERS

Amy Cobb

Maeve Dion

Colleen Hardy

Randy Jackson

JMU COORDINATORS

Ken Newbold

John Noftsinger

PUBLISHING

Zeichner Risk Analytics

Contact: CIPP01@gmu.edu

703.993.4840

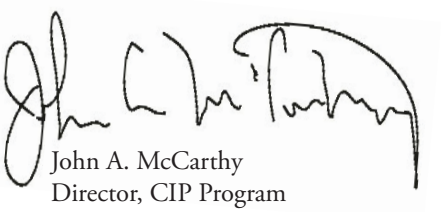
Click here to subscribe. Visit us online for this and other issues at http://cipp.gmu.edu

We are pleased to feature two significant interviews in this month's issue of *The CIP Report* that offer depth and perspective to the topic at hand – the National Infrastructure Protection Plan. The Department of Homeland Security released the National Infrastructure Protection Plan (NIPP) on June 30, 2006, following the February 2005 release of the Interim NIPP. Since its release, the NIPP has been the focus of a great deal of time and attention from both the public and private sectors. Aimed at providing a "comprehensive risk management framework that clearly defines critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies and tribal partners," the NIPP further explains and emphasizes the importance of public-private partnerships.

We believe it is especially important to recognize the immense effort put forth by both the public and private sectors. In this issue, we feature interviews representing government and industry stakeholders and focus extensively on the unique challenges encountered by the Department of Homeland Security in creating this first-ever national risk management roadmap. We greatly appreciate the insight provided by both Robert B. Stephan, Assistant Secretary for Infrastructure Protection at DHS, and Stuart Brindley, Chairman of the Partnership for Critical Infrastructure Security and Chair of the Electricity Sector Coordinating Council.

In addition to these key interviews, we provide background information on the NIPP, Sector Specific Plans, and a 'Legal Insights' column covering the critical role of state, local, and tribal governments in the NIPP. We also welcome Sallie McDonald, a Visiting Scholar to the CIP Program from DHS, and feature a short highlight of the recent Cyber Conflict Studies Association's Legal Workshop, held July 25-26 at Harvard University.

As always, we hope you enjoy this issue and appreciate your continued support of the CIP Program.



John A. McCarthy
Director, CIP Program
George Mason University, School of Law

[1] U.S. Department of Homeland Security. *DHS Completes National Infrastructure Protection Plan*. Press Release. June 30, 2006.

National Infrastructure Protection Plan Represents Collaboration Between Government and the Private Sector

In a recent interview with members of the CIP Program staff, Robert B. Stephan, Assistant Secretary for Infrastructure Protection at the U.S. Department of Homeland Security (DHS), discussed the completion of the National Infrastructure Protection Plan (NIPP). Assistant Secretary Stephan answered numerous questions on the NIPP, ranging from its purpose to current outreach efforts aimed at "rolling out" the completed plan that was released on June 30th. Assistant Secretary Stephan's responses are depicted below.

NIPP Structure

Why did the Department draft the NIPP?

DHS drafted the NIPP to fulfill mandates included in the Homeland Security Act of 2002 and Homeland Security Presidential Directive (HSPD)-7, which was released in December 2003. HSPD-7 provided further granularity on the development of a national plan for critical infrastructure and key resources (CI/KR) protection, including policy perspective and an outline of roles and responsibilities of federal players regarding critical infrastructure protection (CIP).

The NIPP presents a nationally unified, comprehensive approach to critical infrastructure protection and serves as the strategic blueprint to bring together Federal, state, local and tribal governments and the private sector, as well as relevant international players. Roles and responsibilities of these key stakeholders, as they pertain to CIP, are clearly articulated in the NIPP. Moreover, the NIPP provides a baseline for further sector-by-sector action and provides a comprehensive framework for governance, information sharing, risk analysis, risk management, resource allocation and management, and continuous improvement in the CIP mission area. Of note, further refinement of the principles outlined in the NIPP will be found in the sector-specific plans (SSPs), to be developed through public-private sector collaboration by December 31, 2006.

What does the Department hope to accomplish with the NIPP?

Using a football analogy, the Nation has a great set of players at all levels, public and private sector – an "all-star team" – but needs an agreed upon set of plays to move the ball down the field. Previously, the Nation lacked a "strategic level playbook with tactical level plays by sector." This playbook is the NIPP, embodying coordination, information sharing, and risk management and defining the responsibilities of key players.

The all-star team consists of:

- Federal, state, and local government officials, to include Homeland Security Advisors and Emergency Managers;
- Private owners and operators, CEOs, and security managers;
- International stakeholders;
- Academia; and
- Non-governmental organizations.

What are, generally speaking, the roles and responsibilities outlined by the NIPP?

Infrastructure protection is a complex puzzle with interlocking pieces, and various people hold the key to putting the puzzle together. The NIPP organizes these pieces, acting as the fabric that stitches people, capabilities, and resources together. Some aspects of the NIPP framework operate in regulatory space at various levels of government, but most of the NIPP framework relies on voluntary cooperation and collaboration between security partners that share a common, complex threat environment and the need to interact extensively to get the CIP job done.

Critical infrastructure typically resides outside federal jurisdiction. The private sector controls approximately 85 percent of the Nation's CI/KR; Federal, state, local, and tribal governments control the rest. These partners represent very complex "inside-the-fence" and "outside-the-fence" security equities that the NIPP helps stitch together in an *(Continued on Page 3)*

Colonel Bob Stephan was appointed to serve as the Assistant Secretary of Homeland Security for Infrastructure Protection in April 2005. In this capacity, he is responsible for the Department's efforts to catalog our critical infrastructures and key resources and coordinate risk-based strategies and protective measures to secure them from terrorist attack. His prior experience as Senior Director for Critical Infrastructure Protection in the Executive Office of the President (EOP) made him a well qualified choice for the Assistant Secretary position. During his tenure with EOP, his duties included developing and coordinating interagency policy and strategic initiatives to protect the United States against terrorist attack across 13 critical infrastructure sectors.

Previous to his position within IAIP, Colonel Stephan served as Special Assistant to the Secretary and Director of the Secretary's Headquarters Operational Integration Staff. In this capacity, he was responsible for wide range of activities that included headquarters-level planning in the areas of strategic and operational planning, core mission integration, domestic incident management, training and exercises. He also directed the Interagency Incident Management Group, integrating Department and interagency capabilities in response to domestic threats and incidents.

Colonel Stephan is a distinguished graduate of the USAF Academy, and holds a Bachelors Degree in Political Science. He is an Olmsted Scholar, and has earned Masters Degrees in International Relations from the University of Belgrano, Buenos Aires, Argentina, and The Johns Hopkins University.

NIPP *(Continued from Page 2)*

organized manner. The private sector and local governments represent the "front lines" of the CIP mission area. Baseline capabilities at this level must often be reinforced very quickly from the State and Federal level based upon emergent threats or incidents. The key to success in making this happen is joint planning, training and exercising, and joint vulnerability reduction programs and activities. Federal grant programs, targeted against our most critical assets, systems, and networks, facilitate this engagement and attendant capabilities enhancements that link the public and private sector together.

The public-private partnership is important to infrastructure protection. No one working alone has the tools, resources, and authorities to protect infrastructure and properly handle planning, response, and recovery; everyone's efforts must be interwoven. The NIPP is a forum to bring people together and look, by sector, at what is important, what gaps exist, and what resources are needed to close gaps. Through collaborative partnership, we need to look at: threat, vulnerability, and consequence; planning; target sets; and joint requirements.

What have you learned in the process of developing the NIPP?

Most importantly, I learned that the NIPP is all about partnerships. The heart of the plan is partnership, collaboration, and information sharing. In developing the NIPP, there is a need to build upon the partnership framework, first and foremost, to make the plan come alive.

The lesson learned from the Interim NIPP, published in February 2005, was to use the NIPP development process itself to help shape the partnership framework, develop concepts, then use the partnership to develop SSPs and work on interlocking programs and activities. Most understand the vital implications of the CIP mission area and know they can't go it alone – they need to be part of a larger network. Leadership, organization, and the strategic blueprint provided by the NIPP are essential to moving this "coalition of the willing" in the right direction, in a measurable way that will reduce our risk in a very complex and dynamic threat environment.

What progress have you witnessed since the release of the Interim NIPP?

Now, I see partnership between the government and private sector. A year and a half ago, there was a lot of misunderstanding and even

(Continued on Page 4)

NIPP *(Continued from Page 3)*
mistrust between many elements of government and the private sector in the CIP arena. Through the work we've done together and the bridges we've built through the NIPP framework, there is an incredible level of engagement that takes place in an environment of trust and collaboration. Don't get me wrong, there are still an enormous number of different perspectives on this animal called CIP, but the big difference is that key public and private sector partners have agreed to let these different perspectives play out through a structured process according to mutually developed "rules of engagement". The individual sectors represent very distinctive operating environments, business landscapes, risk factors, and protective architectures. This factor should not represent a weakness, but rather a strength; the basic approach outlined in the NIPP is designed to be further tailored to individual requirements and realities at the individual sector and sub-sector level as the situation warrants.

The NIPP partnership is now alive and well. It has been developed, pushed out the door, and is undergoing further refinement. We are working together on common ground.

Do you have a strategy for rolling out the final NIPP Base Plan?

There was a formal press announcement noting the completion of the NIPP. In addition, we hope to hold individual sector announcements. For example, the completion of the NIPP was announced at the Chemical Security Summit, co-hosted by the Synthetic Organic Chemical Manufacturers Association and the American Chemistry Council, in Baltimore, MD on June 29th. An event was also held at Calvert Cliffs Nuclear Power Plant on July 19th to announce the document's completion before an audience consisting of representatives from the Nuclear Sector, private sector, state and local government, law enforcement, and Federal government. Events such as these have allowed me to explain publicly what the NIPP is about, show partnership, and demonstrate that tangible initiatives – signature initiatives such as Risk Analysis and Management for Critical Asset Protection (RAMCAP), Comprehensive Reviews, Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and Buffer Zone Protection Program – are underway. They afforded me the opportunity to reference these and *(Continued on Page 5)*

NIPP Chapter Two
Primary roles for CI/KR security partners include:

- **Department of Homeland Security:** Manage the Nation's overall CI/KR protection framework and oversee NIPP development and implementation.
- **Sector-Specific Agencies:** Implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CI/KR sectors designated in HSPD-7.
- **Other Federal Departments, Agencies, and Offices:** Implement specific CI/KR protection roles designated in HSPD-7 or other relevant statutes, executive orders, and policy directives.
- **State, Local, and Tribal Governments:** Develop and implement a CI/KR protection program as a component of their overarching homeland security programs.
- **Regional Partners:** Use partnerships that cross jurisdictional and sector boundaries to address CI/KR protection within a defined geographical area.
- **Boards, Commissions, Authorities, Councils, and Other Entities:** Perform regulatory, advisory, policy, or business oversight functions related to various aspects of CI/KR operations and protection within and across sectors and jurisdictions.
- **Private Sector Owners and Operators:** Undertake CI/KR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matter expertise to the Federal Government;
- **Homeland Security Advisory Councils:** Provide advice, recommendations, and expertise to the government regarding protection policy and activities.
- **Academia and Research Centers:** Provide CI/KR protection subject matter expertise, independent analysis, research and development (R&D), and educational programs.

NIPP *(Continued from Page 4)*
other initiatives and programs outlined in the NIPP that are already being implemented. I hope to hold similar events for other sectors and have turned to the Sector Coordinating Councils (SCCs) for assistance in doing so.

The completion of the NIPP was also featured in DHS's grants announcement. Moreover, the NIPP is regularly briefed to Congress and discussed over conference calls with state and local officials. The U.S. Chamber of Commerce hosted a cross-sector discussion of the NIPP and key framework items on July 18th and plans to schedule comparable discussions on the regional level, also pulling in state and local officials.

How do you look at the delay of the NIPP? Has it allowed for more time to incorporate comments and release a more meaningful document?

The Interim NIPP was not collaborative, accepted, or developed in partnership with others. The NIPP needs broad participation, vetting, and development – something that takes time. The process of seeking nationwide input from government and private sector partners took approximately eight months. Taking the time to collaborate and have additional people take part in the development process was well worth the delay. The document today is accepted, understood, and embraced by those who will implement it, but it's an evolutionary process; much remains to be done on the national and sector levels. ❖

Sector- Specific Agency	Critical Infrastructure / Key Resources Sector
Department of Agriculture[1] Department of Health and Human Services[2]	Agriculture and Food
Department of Defense[3]	Defense Industrial Base
Department of Energy	Energy[4]
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security Office of Infrastructure Protection	Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology and Telecommunications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration United States Coast Guard[5]	Transportation Systems[6]
Immigration and Customs Enforcement Federal Protective Service	Government Facilities

[1] The Department of Agriculure is responsible for agriculture and food (meat, poultry, and egg products).
[2] The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.
[3] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DOD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.
[4] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.
[5] The U.S. Coast Guard is the SSA for the maritime transportation mode.
[6] As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

Private Sector Perspective on the National Infrastructure Protection Plan

Stuart Brindley, Chairman of the Partnership for Critical Infrastructure Security (PCIS) and Chair of the Electricity Sector Coordinating Council, offered CIP Program staff a "private sector perspective" on the NIPP, portrayed below.

The NIPP enabled DHS to describe how the obligations laid out in HSPD-7 would be carried out by all of us in the private sector and government who have a stake in infrastructure protection. From the perspective of the private sector, the NIPP describes the overall framework for how government coordinates efforts related to infrastructure protection, response, and recovery. It outlines the roles of government in partnership with the private sector and provides overall direction for these activities.

For many sectors, the Interim NIPP was overly prescriptive and did not provide the necessary flexibility to recognize the diverse nature of each of the critical infrastructure sectors in areas such as determining critical assets and assessing risks. Additionally, the Interim NIPP seemed almost entirely focused on protecting against terrorism-related threats, to the exclusion of other risks and hazards. Last year's hurricanes, for example, underscored the need to recognize all threats - all hazards. I believe we have come a long way since the release of the Interim NIPP. The final NIPP shows us that, from a private sector perspective, it is possible to influence and shape government plans by contributing at an early stage. Invariably, early collaboration creates an opportunity to learn from each other, and allows us to arrive at pragmatic solutions that meet both our needs.

"The final NIPP shows us that, from a private sector perspective, it is possible to influence and shape government plans by contributing at an early stage."

As the private sector owns or operates the vast majority of the critical infrastructures, I see the private sector as a primary audience for the NIPP. The private sector ultimately bears many of the costs associated with infrastructure protection, and so needs to be actively involved in understanding threats and risks and taking the appropriate action to enhance the protection, response and recovery of our critical assets, networks, and systems. Infrastructure protection and response capability are subjects that are not altogether new to the private sector. Business continuity is incredibly important to the private sector, and events such as the 9/11 terrorist attacks, the 2003 Blackout, and hurricanes of fall 2005, as well as daily world incidents, remind us that we need to continue to seek opportunities to increase our collective level of readiness and response. The NIPP provides us with an additional incentive to ensure these efforts are integrated with government and across sectors.

Unfortunately, the NIPP is a lengthy document, and I would have preferred a more concise, "Gettysburg Address" version that would inspire government and private sector leaders to recognize the NIPP for what it is – a first-ever voluntary collaboration of government with the private sector on matters related to homeland security. From this broad perspective, I view the interdependencies between

(Continued on Page 7)

Stuart Brindley, Chairman of the Partnership for Critical Infrastructure Security, is Manager for Training & Emergency Preparedness with the Independent Electricity System Operator (IESO) in Ontario, Canada. In this role, he is responsible for coordinating the Ontario electricity industry's emergency preparedness program, involving electricity market participants and government. This requires ensuring that generators, transmitters, distributors, and direct-connect customers all have emergency plans in place and tested.

Private Sector Perspective on NIPP *(Continued from Page 6)*
and amongst the various infrastructures as being the biggest opportunity for improved understanding and coordinated action. It is with this collaborative national plan that interdependencies can be formally recognized and, in turn, be considered in the planning and execution of all sectors' protection efforts.

Under the NIPP, the Federal government provides leadership and commitment to meet its overall objective in the broadest sense – enhance the reliability of our critical infrastructures. While it is important that all of us recognize the fundamental role of the individual states in infrastructure protection, particularly with regard to state lead role in emergency response, we must acknowledge that most critical infrastructures owned and operated by the private sector are not only multi-state, but often multinational. Therefore, a national plan for infrastructure protection, rather than individual plans that are unique to each state, appears to provide the most value.

The NIPP does a great job of defining the partnership framework developed to enable government and private sector collaboration. This framework was, in fact, developed with substantial input from the private sector, and hopefully the NIPP will help lay the foundation for further collaboration on key matters such as information sharing and risk assessment. The quality of the government-private sector relationships that develop will ultimately be a result of the real actions that we successfully undertake.

To help advance the NIPP, DHS has invited each of the sectors to consider how they might assist in the roll-out of the NIPP to their individual sectors. For many of us, the NIPP only really becomes meaningful in the form of the Sector-Specific Plans (SSPs), required to be developed within six months of the release of the NIPP. These SSPs represent the "rubber-on-the-road" for the private sector as they will describe the plans and initiatives that are necessarily unique to each sector. It is clear that the private sector plays a significant role in the implementation of the NIPP through the public-private partnership and I believe that all infrastructure sectors are committed to do so. ❖

Estimating the Size of Critical Infrastructure Sectors

CIP Program research looks at economic and employment value of the industry

According to the NIPP, there are 17 critical infrastructure sectors and key assets. But how many facilities and businesses encompass these sectors? How many people work there and what revenue do they generate? These questions become increasingly important as they provide a baseline for planning everything from employee training programs to cost-benefit analyses of sector-wide protection measures; however, answering them is rather complicated. First, the size and complexity of the U.S. economy is enormous. The 2002 Economic Census counted almost 7 million establishments and 109 million paid employees, without even including the public sector or the agriculture industry. Second, the industry classification system (NAICS) used for census data are not identical with sector definitions used in the NIPP and elsewhere.

The CIP Program has recently begun initial research on best methods for estimating the 17 sectors in terms of their economic and employment value. A first, very rough estimate of 10 of the 17 CI/KR indicates that these sectors alone comprise around 30% of the total U.S. economy in terms of employees and establishments, but more research is necessary.

For insights and suggestions on this issue, please contact Christine Pommerening at cpommere@gmu.edu. ❖

About the National Infrastructure Protection Plan

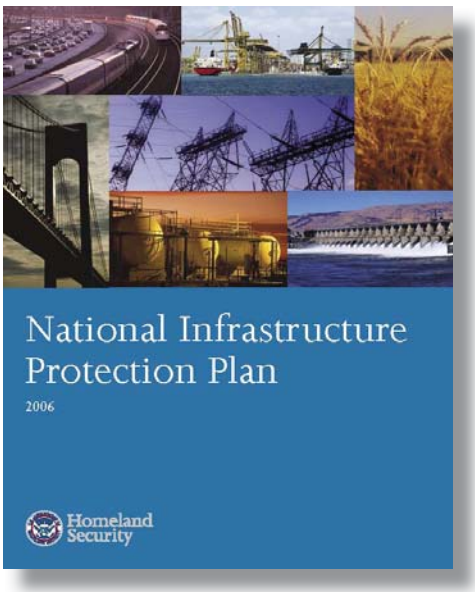
The National Infrastructure Protection Plan (NIPP) was developed by the U.S. Department of Homeland Security (DHS) in response to the Homeland Security Act of 2002 and Homeland Security Presidential Directive (HSPD)-7: Critical Infrastructure Identification, Prioritization, and Protection. The NIPP also takes into consideration the elements outlined in the National Strategy for Homeland Security, released by The White House Office of Homeland Security in July 2002.

The Homeland Security Act of 2002 tasked the new department to develop a "comprehensive national plan for securing the key resources and critical infrastructures in the United States."[1] HSPD-7 further defined the Act's original mandate and called for DHS to draft "a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives," to be completed one year from the issuance of the directive.[2] The Interim NIPP was released by DHS shortly after this deadline and signified a step towards developing a national, cross-sector plan for the protection of our Nation's CI/KR. On June 30, 2006, DHS released the completed NIPP.

The Interim NIPP provided the framework for the development and implementation of a national critical infrastructure protection (CIP) program and addressed plan elements mandated by HSPD-7, including:

a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, state and local governments, the private sector, and foreign countries and international organizations;
b) a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources;
c) a summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sector; and
d) coordination and integration, as appropriate, with other Federal emergency management and preparedness activities including the National Response Plan and applicable national preparedness goals.[3]

These elements were encompassed in the document's six chapters and referenced in its five goals and objectives. The Interim NIPP's goals and objectives were:



1) Protect CI/KR against plausible and specific threats;
2) Long-term reduction of CI/KR vulnerabilities in a comprehensive and integrated manner;
3) Maximize efficient use of resources for infrastructure protection;
4) Build partnerships among Federal, state, local, tribal, international, and private sector stakeholders to implement CIP programs; and
5) Continuously track and improve national protection.[4]

In releasing the Interim NIPP, DHS clearly stated that the plan was not meant to replace the security plans of State, local, and tribal governments or the private sector. Rather, it was meant to complement these plans and create a unified program for CIP. The plan acknowledged that CIP

(Continued on Page 9)

[1] 6 U.S.C. 121(d)(5) (2006)

[2] The White House. *Homeland Security Presidential Directive-7.* December 17, 2003. Available at: http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[3] The White House. *Homeland Security Presidential Directive-7.* December 17, 2003. Available at: http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[4] U.S. Department of Homeland Security. *Interim National Infrastructure Protection Plan.* February 2005. p. 7-8.

About the NIPP *(Continued from Page 8)*
programs had been operating on varying levels in the time prior to its release, but asserted the explicit need for a coordinated effort to protect CI/KR. Such a coordinated effort requires involvement from all stakeholders, whether from Federal, state, local, or tribal governments or the private sector. To help guide this coordinated effort, the plan outlined key roles and responsibilities of government and the private sector and described public-private partnership.

The Interim NIPP outlined the conceptual framework for the sector partnership model, a model based upon recommendations made by the National Infrastructure Advisory Council. This public-private partnership, consisting of the Government Cross-Sector Council, Government Coordinating Councils, Private Sector Cross-Sector Council, also known as the Partnership for Critical Infrastructure Security (PCIS), and Sector Coordinating Councils, seeks to enhance communication and coordination of CIP activities among stakeholders. The Councils also explore policy development, plans relating to response and recovery, and research and development needs. Additional information on the sector partnership model and public-private partnership can be found in the April 2006 issue of *The CIP Report*.

Although the Interim NIPP addressed numerous elements outlined in HSPD-7, the government stressed that its completion proved only a starting point. Following the release of the Interim NIPP, DHS developed and released two draft NIPP Base Plans for stakeholder review. The draft Base Plans built upon the Interim NIPP and elaborated on the framework outlined in the original document. The recently completed NIPP took into account approximately 10,000 comments made during draft Base Plan review periods and offered a greater breadth of relevant information.

The completed NIPP was deemed by DHS a "comprehensive risk management framework that clearly defines critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies and tribal partners."[5] Further defining the roles and responsibilities of those involved with CI/KR protection, the document seeks to integrate CI/KR protection efforts and provide a coordinated approach to help set priorities, goals, and requirements. Moreover, it takes an all-hazards approach when addressing risk, considering both natural and man-made disasters *and* terrorism. The completed plan also lends increased emphasis to interdependencies and cross-sector characteristics, information sharing and the protection of sensitive CI/KR information, cyber security, the human element, international considerations, and long-term, sustainable CIP activities. The importance of public-private partnership continues to be a critical component of the NIPP.

To meet the completed NIPP's goal of improving our Nation's security by better protecting its CI/KR, the plan outlined the following objectives:

- Understanding and sharing information about terrorist threats and other hazards;
- Building security partnerships;
- Implementing a long-term risk management program; and
- Maximizing the efficient use of resources.[6]

As demonstrated by these objectives, the NIPP is based on:

- Strong public-private partnerships which will foster relationships and facilitate coordination within and across critical infrastructure and key resource sectors;
- Robust multi-directional information sharing which will enhance the ability to assess risks, make prudent security investments, and take protective action; and
- Risk management framework establishing processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.[7]

Protecting our Nation's CI/KR is a daunting task, and one that requires extensive cooperation and collaboration among stakeholders. Any plan aimed at guiding

(Continued on Page 12)

[5] U.S. Department of Homeland Security. *DHS Completes National Infrastructure Protection Plan.* Press Release. June 30, 2006.

[6] U.S. Department of Homeland Security. *National Infrastructure Protection Plan.* June 2006. p. 9.

[7] U.S. Department of Homeland Security. *National Infrastructure Protection Plan.* Available at: http://www.dhs.gov/nipp.

Legal Insights

The Critical Role of States in the NIPP

Randy Jackson
Senior Legal Researcher, CIP Program

The Homeland Security Act of 2002 (Act) and Homeland Security Presidential Directive-7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, issued on December 17, 2003, outline the way in which the Federal government was to establish "a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." In response, DHS drafted the NIPP to address the protection of CI/KR from major events such as terrorism attacks or natural disasters.

The development of a CI/KR protection plan for a nation as large and diverse as the United States is a formidable task. DHS must coordinate activities with not only the private sector, which owns or operates the majority of the Nation's CI/KR, but also state, local, and tribal governments. DHS will also coordinate with state, local, and tribal governments to help facilitate information sharing with the private sector within their jurisdictions. It is this kind of cooperation that will lead to essential cross-sector dialogue and information flow, and is necessary if we as a nation are to effectively protect our homeland.

Under the U.S. federal system, the Constitution delineates the powers held by the Federal government. These enumerated powers include the power to tax and spend, the power to declare war, and the power to control interstate commerce. The Federal government also has the power to control foreign commerce (this includes commerce with the sovereign tribes) and enter into treaties. Finally, the Federal government has the power to act in a way "necessary and proper" to execute its enumerated powers. Anything outside of these express powers is reserved to the state governments (unless prohibited by the Constitution). This is codified in the 10th Amendment.

"DHS will also coordinate with state, local, and tribal governments to help facilitate information sharing with the private sector within their jurisdictions. It is this kind of cooperation that will lead to essential cross-sector dialogue and information flow, and is necessary if we as a nation are to effectively protect our homeland."

An important power reserved to the states is police power. Through their police power, state governments take steps to protect the health and safety of their citizens. Protecting CI/KR assets from acts of terrorism and/or assisting in their recovery in the event of a natural or other type of disaster would fall under this state power. Moreover, in the event of an overwhelming catastrophe, the governor has the state National Guard at his/her disposal to help reconstitute essential services and CI/KR assets as appropriate. The Guard is non-federal (but may be federalized under certain conditions) and, unlike the federal military, is not subject to posse comitatus.

Given that CI/KR protection falls under states' police power, it is imperative to the successful implementation of the NIPP that states cooperate with the Federal government in executing the plan and its components. This notion is reflected in the language of federal documents such as HSPD-7 and the Homeland Security Act of 2002, which direct DHS officials to "coordinate with" or "consult with" state officials rather than "direct" such officials. Although the Federal government cannot demand states' cooperation, it is not powerless to compel states to act in support of the NIPP. The Federal government has the ability, through its tax and spend power, to condition the receipt of federal preparedness grant funding on its review of state and urban area preparedness plans.

(Continued on Page 11)

Sector-Specific Plans Add to the National Infrastructure Protection Plan

Sector-Specific Plans (SSPs) are currently being developed by each Sector-Specific Agency (SSA), in collaboration with government and private sector security partners, to complement and support the NIPP as stand-alone annexes. SSPs are tailored for each sector's landscape and detail the respective sector's CIP activities and protective programs. In addition, SSPs offer information on public-private investment in CIP and sector resources. Essentially, they describe each sector's basic approach to securing its critical infrastructure.

Each SSP consists of eight chapters:

1. Sector Profile and Goals
2. Identify Assets, Systems, Networks, and Functions
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs
6. Measure Progress
7. CI/KR Protection R&D
8. Sector Management and Coordination

Topics addressed within these chapters include: roles and responsibilities; interdependencies; information sharing mechanisms; goals and objectives aimed at establishing, or enhancing, protective posture; international considerations; identified government actions to supplement those depicted in the sector risk model(s); and sector-specific approaches and methodologies for assessing and managing risk, assessing and prioritizing CI/KR, using metrics to gauge the effectiveness of CIP activities, directing research and development, and furthering intra-sector governance.

Information provided in the SSPs will allow DHS and SSAs to conduct cross-sector comparisons and facilitate greater collaboration between all levels of government and the private sector through a better understanding of the Nation's 17 CI/KR sectors. To adequately address changes in sector characterization, CI/KR mission, or the overall CIP environment, SSPs should be regularly reviewed and updated by the SSAs as appropriate. Edits made to the NIPP during its triennial review may also necessitate SSP updates.

The SSPs are due to DHS by December 31, 2006, 180 days following issuance of the completed NIPP. Of note, many sectors are revising their existing SSPs to meet the added requirements of the 2006 SSP guidance, released on April 4, 2006. SSP guidance was previously released in April 2004 and April 2005; draft SSPs were submitted to DHS in September 2004. ❖

Legal Insights *(Continued from Page 10)*

Through the State Homeland Security Grant Program, DHS provides funding to state, local (including direct support to urban areas), and tribal governments to develop CI/KR protection plans in support of the NIPP. The Federal government can influence the development of states' CI/KR asset protection plans by requiring NIPP-supportive steps, such as using the NIPP's Risk Management Framework, to be taken in order to secure the funding. Thus, the Federal government acts under its enumerated tax and spend power without infringing on states' reserved powers.

The original United States' Articles of Confederation envisioned a set of completely sovereign units gathered together simply for mutual defense – even taxation was not allowed. When the Articles of Confederation were replaced by the Constitution and the Federal government came into existence, the states retained considerable powers. In order to effectively carry out the protection of people and assets, such as the Nation's CI/KR, under police power, states need to work with the Federal government to coordinate actions and share information. It is the effectiveness of the Federal and state governments' cooperation and coordination efforts which will enhance the protection of our critical infrastructure. ❖

Visiting Scholar Contributes to CIP Program's Coordination with DHS

Sallie McDonald is a Senior Executive within the Department of Homeland Security's (DHS), Preparedness Directorate. She is currently the Special Assistant to the Assistant Secretary of Infrastructure Protection, advising him on cyber security and telecommunications issues. She is also serving a one year assignment to George Mason University's Critical Infrastructure Protection Program, where she serves as a visiting scholar.

Throughout her tenure at DHS, Sallie has worked with public and private sector organizations to develop working relationships with the Department. She has been particularly active in the international arena, briefing foreign governments on critical infrastructure protection measures, sharing best practices and encouraging others to adopt measures to protect their country's critical assets.

While working at the General Services Administration (GSA), she was the Assistant Commissioner for Information Assurance and Critical Infrastructure Protection, and was responsible for the Federal Computer Incident Response Center (FedCIRC), which on March 1, 2003 was transferred to DHS. FedCIRC was the Federal government's focal point for computer security incident recognition, reporting, handling and prevention. Sallie is an active participant in the Cyber Security community at the highest levels of government and has participated in the evolving face of critical infrastructure protection. She has testified on cyber security issues numerous times to both the Senate and the House. She also serves on the National Institute of Standards and Technology's Information Security and Privacy Advisory Board, which examines issues affecting the security and privacy of sensitive (unclassified) information in federal computer and telecommunications systems.

Sallie worked at GSA from1977 until her transfer to DHS. While at GSA, she also spearheaded programs such as E-Authentication, Safeguard, Access Certificates for Electronic Services (ACES) and Managed Security Services. She also led the national effort for the Y2K Information Coordination Center.

She began her career in the telecommunications area at GSA, where she served in a variety of technical and management positions.

Sallie is a graduate of Harvard's Senior Executive Fellows Program and the Federal Executive Institute. Sallie attended the University of Miami and received a Master of Public Administration from American University. She resides in Washington DC.

About the NIPP *(Continued from Page 9)*

CI/KR protection efforts must also adapt to changing times and new requirements. To ensure that the NIPP remains a meaningful document, it will be continuously reviewed and revised as appropriate. Re-issuance of the NIPP will occur a minimum of every three years.

Additional information on the NIPP may be found at http://www.dhs.gov/nipp. Select government reports on infrastructure protection, to include HSPD-7, may be found in the CIP Library on the CIP Program's web site (http://cipp.gmu.edu/clib/). ❖

CIP Program Participates in Cyber Conflict Legal Workshop

Harvard Faculty Club

Cambridge, Mass.

On July 25-26, the CIP Program sent Maeve Dion and Brett Callahan to participate in a Legal Workshop organized by the Cyber Conflict Studies Association (CCSA). The workshop was held on the campus of Harvard University, and was co-sponsored by the Program on Humanitarian Policy and Conflict Research.

This two-day brainstorming event was organized by CCSA in order to explore the legal issues related to cyber conflict. One goal was to develop a research agenda and networking base for students in law, public policy, and information technology, as well as for other researchers.

The workshop participants included both government and private sector legal professionals, information technologists, policy experts, and academics. There was an impressive attendance by representatives of the military and intelligence communities.

The first day opened with a keynote speech from Michel Bourbonniere, of the Canadian Department of Justice, and continued with presentations from David Dittrich, University of Washington Center for Information Assurance and Cybersecurity; Thomas Dukes, U.S. Department of Justice; Col. Charles Williamson, Air Intelligence Agency; and Lt. Col. Guillermo Carranza, Joint Task Force / Global Network Operations.

After the presentations, the participants separated into two working groups -- *Cyber Conflict as a Use of Force and Armed Attack,* and *Cyber Conflict as Crime, Espionage, and Terrorism*. The CCSA kept minutes of the working groups' discussions, and at the end of the second day, each working group reported a distilled list of suggested research topics. For information on the final work products from this workshop (not yet released), please watch the CIP Program website or contact Maeve Dion.

In addition to this legal workshop, the CCSA is organizing similar events that will hopefully enhance the cyber conflict research agenda in the areas of theory, policy and strategy, and infrastructure. CCSA currently has a Call for Papers for its 2006 Fall Symposium, and is also accepting submissions for the January issue of the *Cyber Conflict Journal*.

As described on its website, CCSA is "a non-profit entity organized to promote and lead a diversified research and intellectual development agenda to advance knowledge in the cyber conflict field." CCSA is supported by Norwich University and the National Center for the Study of Counter-Terrorism and CyberCrime at Norwich University. ❖

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 (ZRA) 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