THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 6 NUMBER 8

FEBRUARY 2008 NATIONAL PLANS AND STRATEGIES UPDATE

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

This month's issue of *The CIP Report* features the national plans and strategies of the United States and serves as an update on recently released documents. The White House has released several National Strategies that center on the security of the Nation. Each strategy or plan focuses on a different area of homeland security, but the goal to keep the Homeland safe from any kind of threat, whether a terrorist attack or natural disaster, is the same throughout.

The articles included in this month's issue review the National Response Framework (NRF), which was just released last month, and the National Incident Management System (NIMS) released in draft revised form last August. In the past months, several National Strategies have also been revised and updated. An overview of the National Strategies is included along with a table showing the release date for each. We take an in-depth look at two strategies that have most recently been released. The *National Strategy for Homeland Security* was updated this past October from its original release in July 2002 and the *National Strategy for Information Sharing* was released for the first time this past October. Another article explains the significance and evolution of decision directives as they have been passed down by different Presidential Administrations. An outline is provided with the Homeland Security Presidential Directives that exist today.

In this issue, *Legal Insights* becomes a regular feature again and highlights the NRF release. James Madison University (JMU) presents a summary on its newly released book titled *Understanding Homeland Security: Policy, Perspective, and Paradoxes*. A summary on the Institute for Information Infrastructure Protection (I3P) is also included and explains I3P's mission and current research. Lastly, brief information about the National Infrastructure Protection Plan (NIPP) and accompanying Sector-Specific Plans (SSPs) is provided.

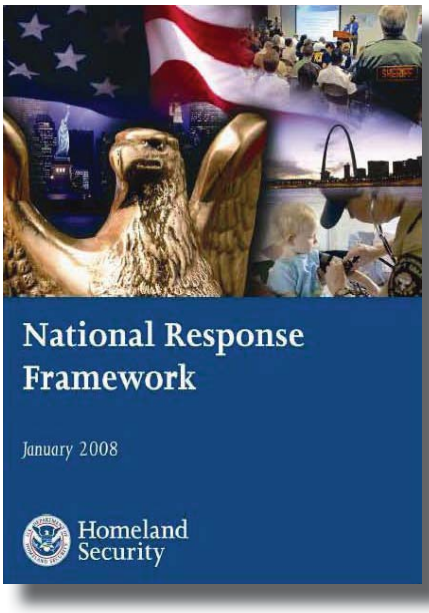
We hope you enjoy this issue of *The CIP Report* and thank you for your continued support of the CIP Program.

U.S. Department of Homeland Security Releases the National Response Framework

On January 22, 2008, the U.S. Department of Homeland Security (DHS) released the National Response Framework (NRF), slated to become effective on March 22, 2008. The release of the document comes after a lengthy review and revision process that began in September 2006, and included public comment periods for the draft NRF Base Plan and Emergency Support Function (ESF), Support, and Incident Annexes made available in September 2007. The NRF and its supporting documents supersede the National Response Plan and its accompanying ESF and Support Annexes; the current Incident Annexes will remain in place until updated ones are issued.

Homeland Security Presidential Directive (HSPD)-5: Management of Domestic Incidents called for both a National Incident Management System (NIMS), to "provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity," and a National Response Plan, to "provide the structure and mechanisms for national level policy and operational direction for Federal support to State and local incident managers." The NIMS was released in March 2004, and the National Response Plan in October 2003 (Initial Plan) and December 2004. Once fully implemented, the National Response Plan superseded the Initial National Response Plan, Federal Response Plan, U.S. Government Interagency Domestic Terrorism Concept of Operations Plan, and Federal Radiological Emergency Response Plan.

As with any planning or guidance document, revisions will be made over time. The December 2004 National Response Plan outlined a one-year review and four-year review and reissuance cycle. Although some changes to the document were made in May 2006, it was determined that the National Response Plan would undergo a comprehensive review and revision shortly thereafter, particularly to address the many recommendations presented in post-Hurricane Katrina and Rita reports and elements of the Post-Katrina Emergency Management Reform Act of 2006.



Like the National Response Plan, the NRF is a guidance document for all-hazards response, helping to facilitate a unified national response to incidents of all sizes. To do so, it establishes a "comprehensive, national, all-hazards approach to domestic incident response." The NRF includes key response principles and information on roles and responsibilities and response organization. While the NRF is especially geared towards senior government officials, those at the Federal, State, tribal, and local levels, it also pertains to the response efforts of the private sector, nongovernmental organizations, and others involved in first-responder or emergency management efforts — and stresses that incident

(Continued on Page 3)

Five Key Principles of Response Doctrine

1. Engaged partnership
2. Tiered response
3. Scalable, flexible, and adaptable operational capabilities
4. Unity of effort through unified command
5. Readiness to act

NRF *(Cont. from 2)*

response should be addressed at the lowest possible jurisdictional levels. Through its emphasis on partnerships among public and private entities, preparedness, and the application of common principles and response structures, DHS states that the NRF will contribute to more effective incident response on the part of government, in turn better serving communities.

The NRF includes much of the same information featured in the National Response Plan, but is credited with being more user-friendly and incorporating lessons learned and best practices from past incident response. Recognizing that the document is intended to frame approaches to domestic incident response, providing information on key considerations rather than step-by-step directions for conducting response efforts, its name was also changed from a "Plan" to "Framework."

The NRF continues to build on foundational elements of the NIMS, utilizing the same core principles of the system — flexibility and standardization. It offers clarifying information on key roles and responsibilities as well as response actions that can be translated across various jurisdictions, and includes the assertion that the Administrator of the Federal Emergency Management Agency (FEMA) serves as the principal advisor to the President, Homeland Security Council, and Secretary of Homeland Security on emergency management matters. For added clarity, the NRF also offers revised definitions for certain terms and expansions to the

National Response Framework Organization

Base Document
- Introduction
- Chapter I - Roles and Responsibilities
- Chapter II - Response Actions
- Chapter III - Response Organization
- Chapter IV - Planning: A Critical Element of Effective Response
- Chapter V - Additional Resources
- Acronyms

Emergency Support Function (ESF) Annexes
- ESF #1 - Transportation
- ESF #2 - Communications
- ESF #3 - Public Works and Engineering
- ESF #4 - Firefighting
- ESF #5 - Emergency Management
- ESF #6 - Mass Care, Emergency Assistance, Housing, and Human Services
- ESF #7 - Logistics Management and Resource Support
- ESF #8 - Public Health and Medical Services
- ESF #9 - Search and Rescue
- ESF #10 - Oil and Hazardous Materials Response
- ESF #11 - Agriculture and Natural Resources
- ESF #12 - Energy
- ESF #13 - Public Safety and Security
- ESF #14 - Long-Term Community Recovery
- ESF #15 - External Affairs

Support Annexes
- Critical Infrastructure and Key Resources
- Financial Management
- International Coordination
- Private-Sector Coordination
- Public Affairs
- Tribal Relations
- Volunteer and Donations Management
- Worker Safety and Health

Incident Annexes (National Response Plan Incident Annexes currently remain in effect)
- Biological Incident
- Catastrophic Incident
- Cyber Incident
- Food and Agriculture Incident
- Nuclear/Radiological Incident
- Oil and Hazardous Materials Incident
- Terrorism Incident Law Enforcement and Investigation

Response Partner Guides (forthcoming)
These guides describe key roles and responsibilities, response structures, actions, and other pertinent information for local, tribal, State, Federal, and private sector response partners.

(Continued on Page 15)

Revision of the National Incident Management System

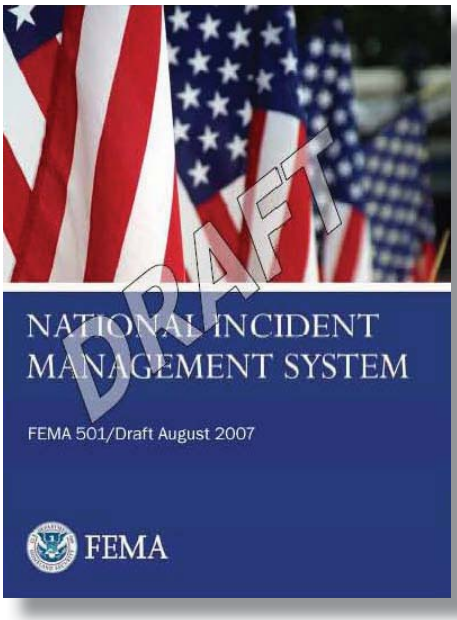
A comprehensive review of the National Incident Management System (NIMS) was performed in conjunction with the review and revision of the National Response Plan that began in September 2006. A draft revised version of NIMS was released in August 2007, allowing for the reflection of any NIMS updates in the final version of the NRF. As with the NRF's review, the public had the opportunity to comment on draft versions of the NIMS made available in early 2007.

HSPD-5 not only mandated the development of the NIMS, but also directed Federal departments and agencies to "use the NIMS in their domestic incident management and emergency prevention, preparedness, response, recovery, and mitigation activities, as well as those actions taken in support of State or local entities." Moreover, it made compliance with NIMS a requirement for the provision of Federal preparedness assistance (e.g., grants).

While not a plan itself, NIMS consists of core policies, concepts and principles, terminology, and organizational processes as well as reference materials and templates built from existing best practices. Together, this information serves as a standardized template for incident management. Additional guidance, standards, and compliance protocols (consisting of implementation activities) are provided by FEMA's National Integration Center Incident Management Systems Integration Division.

The revised NIMS clarifies various concepts and information outlined in the original document, offers an increased number of graphics for visual reference, and provides a greater emphasis on *preparedness.* It also features a more logical organization of content that transitions from emergency management to incident response. Most importantly, it reflects the addition of lessons learned from recent incident response.

The key components of the revised NIMS are: Preparedness, Communications and Information Management, Resource Management, Command and Management, and Ongoing Management and Maintenance. An extensive appendix on the incident command system (ICS) is also offered to complement the Command and Management portion of the document.



For additional information and NIMS reference materials, please see http://www.fema.gov/emergency/nims/. ❖

The National Incident Management System provides a systematic, proactive approach guiding departments and agencies at all levels of government, the private sector, and nongovernmental organizations to work seamlessly to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life, property, and harm to the environment.

Overview of the National Strategies

Since July 2002, numerous "National Strategies" have been released by the White House. These documents, summarized below, primarily represent U.S. Government strategies for addressing security and terrorism detection, deterrence, prevention, and response. In publishing such strategies, the government acted on recommendations and built on elements of previous reports, to include those of the President's Commission on Critical Infrastructure Protection (PCCIP), Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), U.S. Commission on National Security/21st Century (Hart-Rudman Commission), and National Commission on Terrorist Attacks Upon the United States (9/11 Commission), among others. It also answered repeated Congressional calls for adopting national strategic documents.

The National Security Strategy of the United States of America

This *Strategy*, first issued in September 2002 and released in updated form in March 2006, outlines the key national security concerns of the U.S. Government and strategic approaches to addressing such concerns. The document supports the Nation's belief in freedom, democracy, and free enterprise and asserts that combating terrorism for the advancement of liberty will lead to the great security of the American people. The latter-released *Strategy* summarized the U.S. approach to national security as the promotion of freedom, justice, and human dignity and leadership of multinational efforts to develop democracies and meet the challenges of globalization.

National Strategy to Combat Weapons of Mass Destruction

This *Strategy* outlines the U.S. approach to prevent, deter, defend against, and respond to threats of weapons of mass destruction (WMD) attack. Acknowledging potential terrorist use of WMDs, the *Strategy* advocates the further development of alliances and new partnerships with nation-states, to include those previously considered adversaries. It also encourages the use of new technologies and of intelligence collection and analysis to counter threats. Additionally, it advocates the implementation of strong counterproliferation policies and nonproliferation measures to minimize the likelihood of use and adversary control of WMDs. The text of this *Strategy* is also found in *Homeland Security Presidential Directive (HSPD)-4.*

The National Strategy to Secure Cyberspace

This document focuses on the protection of cyber assets, encouraging active participation in the security of cyberspace among all levels of government, the private sector, and the populace. The *Strategy* features the following objectives: prevent cyber attacks against America's critical infrastructures; reduce national vulnerability to cyber attacks; and minimize damage and recovery time from cyber attacks that do occur. It promotes the development and use of effective public-private partnerships to enhance information sharing and coordinate response to both threats and attacks. It also notes that the government must protect critical cyber networks and support research and development to enable private sector owners and operators to better protect their assets.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

Like the protection of cyberspace, the physical protection of critical infrastructure is vitally important to the Nation's security. This *Strategy* includes the following objectives: identifying and assuring the protection of those infrastructure and assets we deem most critical; providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat; and assuring the protection of other infrastructures and assets that may become targets over time by pursuing specific initiatives and enabling a collaborative environment between the public and private sector. The document offers information on roles and responsibilities, cross-sector security initiatives, and general steps that can be taken to improve critical infrastructure protection.

(Continued on Page 6)

National Strategies *(Cont. from 5)*

National Strategy for Combating Terrorism

First issued in February 2003 and released in updated form in September 2006, this *Strategy* discusses the War on Terrorism and builds on concepts from *The National Security Strategy of the United States of America.* The updated *Strategy* focuses on the following objectives: advance effective democracies as the long-term antidote to the ideology of terrorism; prevent attacks by terrorist networks; deny terrorists the support and sanctuary of rogue states; deny terrorists control of any nation they would use as a base and launching pad for terror; and lay the foundations and build the institutions and structures we need to carry the fight forward against terror and help ensure our ultimate success. It offers a review of perceived successes and challenges, analysis of the terrorist threat, and information on the transformational structures needed to continue combating terrorism.

The National Strategy for Maritime Security

This *Strategy* offers a broad review of the maritime domain, to include its importance to the United States, the threats it faces, and strategic actions that can be taken to improve its overall security. It highlights four strategic objectives: prevent terrorist attacks and criminal or hostile acts; protect maritime-related population centers and critical infrastructures; minimize damage and expedite recovery; and safeguard the ocean and its resources. Supporting this *Strategy* are eight plans that address specific threats and challenges: National Plan to Achieve Domain Awareness; Global Maritime Intelligence Integration Plan; Interim Maritime Operational Threat Response Plan; International Outreach and Coordination Strategy; Maritime Infrastructure Recovery Plan; Maritime Transportation System Security Plan; Maritime Commerce Security Plan; and Domestic Outreach Plan. For additional information, see *HSPD-13*.

National Strategy for Pandemic Influenza

To better prepare the Nation to address the threat of a pandemic influenza, this *Strategy* describes the U.S. approach to a pandemic in terms of preparedness and communication, surveillance and detection, and response and containment. The *Strategy* focuses on the following objectives: stopping, slowing or otherwise limiting the spread of a pandemic to the United States; limiting the domestic spread of a pandemic, and mitigating disease, suffering and death; and sustaining infrastructure and mitigating impact to the economy and the functioning of society. The document also addresses the roles and responsibilities of Federal, State, and local governments, the private sector, the populace, and international partners.

National Strategy for Victory in Iraq

This *Strategy* concentrates on the war in Iraq as part of the broader War on Terrorism. The ultimate goal expressed in the *Strategy* is to help the Iraqi people defeat the terrorists and build an inclusive democratic state. The U.S. strategy to achieve this goal is organized into three tracks: political (isolate, engage, build); security (clear, hold, build); and economic (restore, reform, build). The descriptions of each track include core assumptions, strategic logic, progress, and challenges, and are followed by a discussion of eight strategic objectives ranging from defeating terrorists and neutralizing the insurgency to strengthening public understanding of Coalition efforts and public isolation of insurgents.

National Strategy to Internationalize Efforts Against Kleptocracy

Complementing a pledge made by the President at the July 2006 G-8 Summit, this *Strategy* addresses high-level, large-scale corruption by public officials and promotes transparency and responsible governance to curtail public corruption and its associated consequences. The *Strategy's* objectives include: preventing and detecting grand corruption; tracing and recovering proceeds of corruption; transferring assets and ensuring responsible use; and strengthening international will and ability to combat grand corruption, coordinate responses, and implement and enforce international standards. Recognizing that kleptocracy is a global problem, the *Strategy* is dedicated to furthering international partnerships and encouraging multilateral action to combat corruption.

(Continued on Page 7)

National Strategies *(Cont. from 6)*

National Strategy for Aviation Security

This *Strategy* addresses the security of the Air Domain, providing information on past attacks, threats, security initiatives, and strategic actions that can be taken to improve its security. The document features the following strategic objectives: deter and prevent terrorist attacks and criminal or hostile acts in the Air Domain; protect the United States and its interests in the Air Domain; mitigate damage and expedite recovery; minimize the impact on the Aviation Transportation System and the U.S. economy; and actively engage domestic and international partners. Supporting the *Strategy* are seven plans addressing various aspects of aviation security: Aviation Transportation System Security Plan; Aviation Operational Threat Response Plan; Aviation Transportation System Recovery Plan; Air Domain Surveillance and Intelligence Integration Plan; International Aviation Threat Reduction Plan; Domestic Outreach Plan; and International Outreach Plan. Additional information can be found in *HSPD-16*.

National Strategy for Public Health and Medical Preparedness

This *Strategy* concerns the health of the populace given the occurrence of a catastrophic health event and identifies the four most critical components of public health and medical preparedness: biosurveillance; countermeasure distribution; mass casualty care; and community resilience. The *Strategy* addresses the following key principles: preparedness for all potential catastrophic health events; vertical and horizontal coordination across levels of government, jurisdictions, and disciplines; a regional approach to health preparedness; engagement of the private sector, academia, and other nongovernmental entities in preparedness and response efforts; and the important roles of individuals, families, and communities. Importantly, it directs Federal departments to take certain actions to contribute to the maintenance of public health and the Nation's medical systems; these actions will be incorporated into the U.S. Department of Health and Human Services' *National Health Security Strategy*. The text of this National Strategy is found in *HSPD-21*.

See pages 8 and 10 in this issue of *The CIP Report* for information on the *National Strategy for Homeland Security* and *National Strategy for Information Sharing,* respectively. ❖

National Strategy for Homeland Security	July 2002
The National Security Strategy of the United States of America	September 2002
National Strategy to Combat Weapons of Mass Destruction	December 2002
The National Strategy to Secure Cyberspace	February 2003
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets	
National Strategy for Combating Terrorism	
The National Strategy for Maritime Security	September 2005
National Strategy for Pandemic Influenza	November 2005
National Strategy for Victory in Iraq	
The National Security Strategy of the United States of America (updated)	March 2006
National Strategy to Internationalize Efforts Against Kleptocracy	August 2006
National Strategy for Combating Terrorism (updated)	September 2006
National Strategy for Aviation Security	March 26, 2007
National Strategy for Homeland Security (updated)	October 2007
National Strategy for Public Health and Medical Preparedness	
National Strategy for Information Sharing	

National Strategy for Homeland Security

After the September 11, 2001 attacks, the White House issued the first *National Strategy for Homeland Security*. This 90-page document, released in July 2002, emphasized three major goals:

- Prevent terrorist attacks within the United States;
- Reduce America's vulnerability to terrorism; and
- Minimize the damage and recover from attacks that do occur.

The goals of the first *Strategy* primarily focused on terrorism and failed to evaluate the real threat of natural events. It did, however, provide important initial groundwork. The roles of Federal departments and agencies were outlined and they were provided with direction related to homeland security. It presented State and local governments and private companies and organizations with information on how to improve security. The first *Strategy* was the beginning framework on homeland security and organization of the different roles involved in keeping the Nation safe.

The updated *Strategy* was released on October 9, 2007 and built upon the first release in 2002. Although it still very much focuses on terrorism, it also includes non-terrorist events. Catastrophic events, whether man-made or natural disasters, pose just as much a threat to the Nation as terrorist attacks. The updated *Strategy* also addresses additional initiatives and approaches such as risk management and the essential role it plays, as well as incident management, science and technology, and leveraging instruments of national power and influence. A fourth goal was added to the updated *Strategy* while the other three goals were slightly revised. The following include the major goals of the updated document:

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources;
- Respond to and recover from incidents that do occur; and
- Continue to strengthen the foundation to ensure our long-term success.

According to the *Strategy*, risk management underlies the full spectrum of homeland security activities; it is important when effectively and efficiently trying to secure the Nation. Risk management allows for the identification of potential hazards, determination of their level of risk, and prioritization and allocation of resources. This in turn aids in prevention, protection, and response and recovery from any type of incident.

A "Culture of Preparedness" is also vital in homeland security. One of its principles puts responsibility on individual citizens and community as much as it does on the different levels of government and the private sector. Individual responsibility helps take the burden off of emergency responders and allows them to concentrate their efforts where help is more urgently required. Community preparedness is identified as one of the most effective means of securing the Homeland.

Incident management is as equally important to consider as risk management because there will be times when crisis-oriented decisions will have to be made. The implementation of an incident management system will build upon the current NIMS. The consideration of overseas threats, law enforcement and public health actions and investigations, and protective measures put in place at critical infrastructure sites are to be incorporated into the system. Another aspect to be included will be conducting exercises, consistent with the National Exercise Program. These exercises will be conducted so that all stakeholders can be certain of their roles and responsibilities.

Incorporating a Homeland Security Management System is outlined as part of the long-term success of the *Strategy*. This approach is managed through the National Preparedness Guidelines (NPG). It integrates four phases to secure our Homeland. These phases include: Guidance, Planning, Execution, and Assessment and Evaluation.

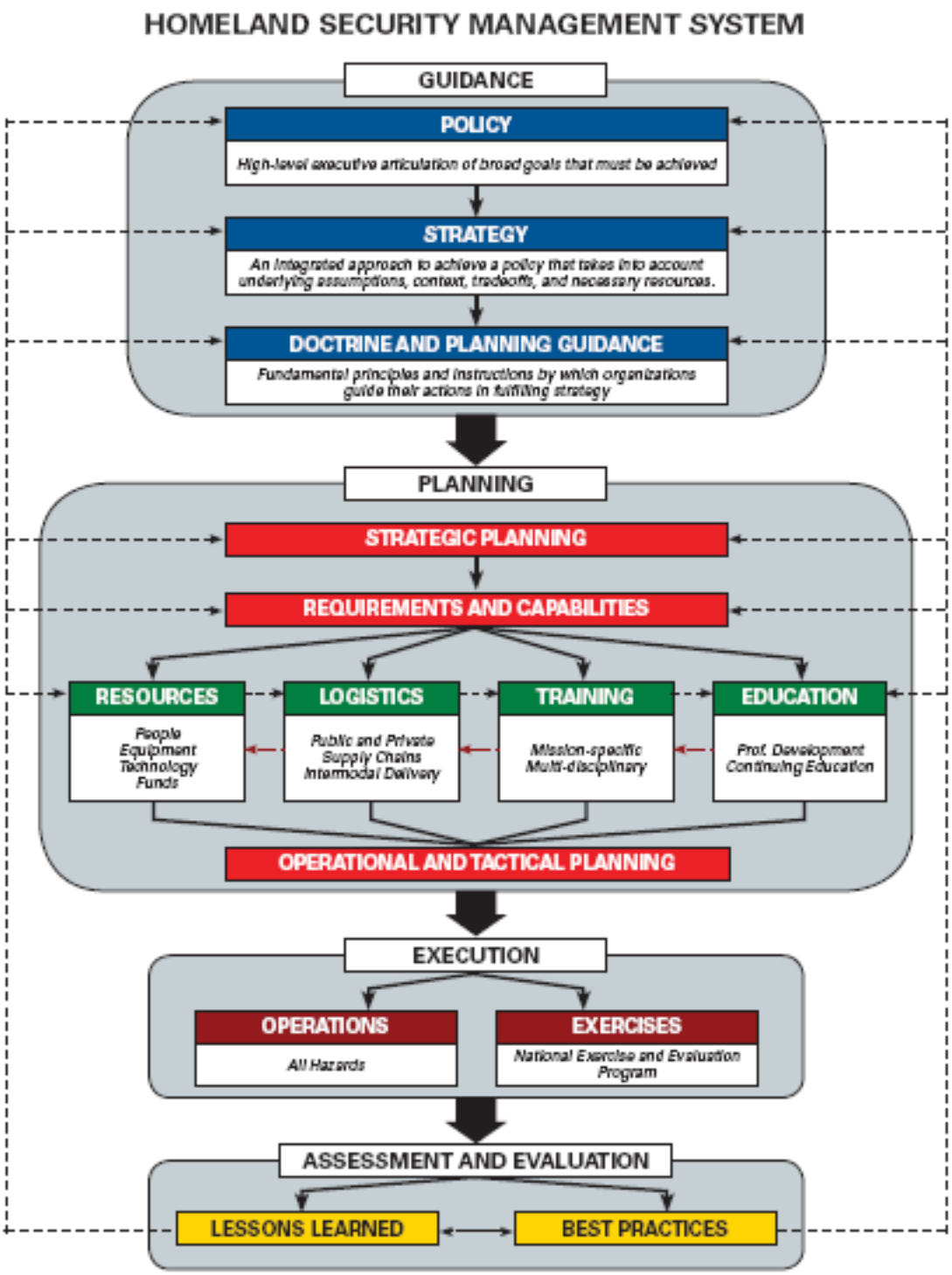
(Continued on Page 9)

Homeland Security *(Cont. from 8)*

Science and technology, and instruments of national power and influence, also support the effort to ensure long-term success. Science and technology aids the research and development used in protecting and defending the Nation against natural and man-made threats. According to the *Strategy*, development and application of chemical, biological, radiological, and nuclear countermeasures are helping to prevent terrorism as well as natural and man-made disasters. Types of instruments of national power and influence include: diplomatic, information, military, economic, financial, intelligence, and law enforcement. The strategic use of these instruments can help prevent terrorism, and respond to and recover from incidents.

Lastly, Congress is also considered an important part of the long-term success of the updated *Strategy*. According to the *Strategy*, Congress should take bold steps to fulfill its responsibilities in the national effort to secure the Homeland and protect the American people. The efforts of Congress should include prioritizing funding, ensuring the proper tools to address changing technologies and security threats while protecting privacy and civil liberties, and maintaining a strong partnership throughout.

Figure 1



For more information and a complete version of the *National Strategy for Homeland Security*, please visit the CIP Library on our website: http://cipp.gmu.edu/clib/reports.php ❖

National Strategy for Information Sharing

On October 31, 2007, the White House issued the *National Strategy for Information Sharing*. The document emphasizes the importance of and need to ensure communication of vital information between agencies at the Federal, State, local, and tribal levels, as well as with the private sector and foreign partners. The goal of the strategic document is to have a more integrated information sharing process, and the focus is on information related to terrorism and the reality that this information comes from different sources and is used for different purposes. The *Strategy* brings all these aspects together and provides guidelines for sharing information to protect the Nation from another terrorist attack.

The *Strategy* presents a plan to share information and begins at the Federal level. The Intelligence Community has been the main source of terrorist information, and improving information sharing means going into other Federal communities. Communities such as law enforcement, defense, homeland security, and foreign affairs broaden U.S. capabilities and provide a unified approach to protecting the Nation. The National Counterterrorism Center (NCTC), whose primary responsibility is to disseminate terrorism-related information, will aid in the effort to improve collaboration between communities. The NCTC analyzes information, then distributes it to the appropriate agency or department and allows for a much more integrated assessment of information.

Foundations of the National Strategy for Information Sharing

An Interagency Threat Assessment and Coordination Group (ITACG) has been established within the NCTC to aid in information sharing between the Federal government and State, local, tribal, and private sector entities. Members of the ITACG include DHS, FBI, representatives of the Intelligence Community, and State and local representatives. According to the *Strategy*, the ITACG will disseminate "federally coordinated" terrorism-related information products to State, local, tribal, and private sector entities.

Fusion centers have also been established by states and major urban areas to distribute information concerning law enforcement, homeland security, public safety, and terrorism in a more coordinated manner. The *Strategy* explains that fusion centers will serve as the focal point for the receipt and sharing of terrorism-related information within the states. Fusion centers will also serve as the primary catalyst for Federal departments and agencies to provide information to State, local, and tribal authorities.

Another important information sharing relationship exists with the private sector. Critical infrastructures are primarily owned and operated by the private sector, who maintain a primary role in keeping the Nation safe. Information sharing between sectors is just as crucial as information sharing between the private sector and the government. The flow of information sharing within and among sectors has been aided by the use of different mechanisms. For instance, private sector owners/operators have utilized the following: Sector Coordination Councils, Government Coordination Councils, National Infrastructure Coordinating Center, Sector-level Information Sharing and Analysis Centers, DHS Protective Security Advisors, the DHS Homeland Infrastructure Threat and Risk Analysis Center, and state and major urban area fusion centers.

The *Strategy* also touches upon the importance of privacy. While information sharing is vital when it comes to the Nation's security, it

(Continued on Page 15)

The Evolution of Presidential Decision Directives

Presidential Administrations have long issued decision directives as a form of communicating policy decisions on national security. Although the intent of such directives has remained static, specific categories of directives have changed over time. Past categories include the National Security Council decision directives (Truman and Eisenhower), National Security Action Memoranda (Kennedy and Johnson), National Security Decision Memoranda (Nixon and Ford), Presidential Directives (Carter), National Security Decision Directives (Reagan), National Security Directives (G.H.W. Bush), and Presidential Decision Directives (Clinton). While previous directives remain in effect until superseded, with new administrations came new categories.

In February 2001, the issuance of *National Security Presidential Directive (NSPD)-1*: *Organization of the National Security Council System* by the current Bush Administration announced the replacement of Presidential Decision Directives (PDDs) by NSPDs as "an instrument for communicating presidential decisions about the national security policies of the United States." Later in 2001, the President issued the first Homeland Security Presidential Directive (HSPD). Similar to NSPDs, so similar that some fall under both the NSPD and HSPD categories of directives, HSPDs are statements of presidential decisions on U.S. homeland security policies. These new categories offer a distinction between policy decisions in an area of traditional focus, *national security*, and an area of steadily increasing focus following the 9/11 terrorist attacks, *homeland security*.

The U.S. Commission on National Security/21st Century put it best in its Phase III Report, "Homeland security is not peripheral to U.S. national security strategy but central to it." This report spurred the development of the first *National Strategy for Homeland Security*, released in July 2002. Complementing this and other National Strategies developed in recent years, HSPDs detail U.S. approaches to protecting the Nation, its people, and its assets. To date, there are 21 HSPDs; these directives are outlined below.

(Continued on Page 16)

1	Organization and Operation of the Homeland Security Council	October 29, 2001
2	Combating Terrorism Through Immigration Policies	October 29, 2001
3	Homeland Security Advisory System	March 11, 2002
4	National Strategy to Combat Weapons of Mass Destruction	December 2002
5	Management of Domestic Incidents	February 28, 2003
6	Integration and Use of Screening Information	September 16, 2003
7	Critical Infrastructure Identification, Prioritization, and Protection	December 17, 2003
8	National Preparedness	December 17, 2003
9	Defense of United States Agriculture and Food	January 30, 2004
10	Biodefense for the 21st Century	April 28, 2004
11	Comprehensive Terrorist-Related Screening Procedures	August 27, 2004
12	Policy for a Common Identification Standard for Federal Employees and Contractors	August 27, 2004
13/NSPD-41	Maritime Security Policy	December 21, 2004
14/NSPD-43	Domestic Nuclear Detection	April 15, 2005
15/NSPD-46	on the War on Terrorism (classified)	March 2006
16/NSPD-47	Aviation Security Policy	June 22, 2006
17	(classified)	2006
18	Medical Countermeasures against Weapons of Mass Destruction	January 31, 2007
19	Combating Terrorist Use of Explosives in the United States	February 12, 2007
20/NSPD-51	National Continuity Policy	May 9, 2007
21	Public Health and Medical Preparedness	October 18, 2007

Legal Insights

Final National Response Framework Release Praised by Key Players

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

The new NRF — formerly the National Response Plan — is the primary federal document designating governmental disaster roles and responsibilities under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act).[1] State and local homeland security officials scrutinize the NRF for guidance on the deployment of federal resources in the event of a disaster. When DHS began circulating a draft NRF for public comment last year, the agency received nearly 5,700 comments.

At his news conference in January announcing the new NRF, DHS Secretary Michael Chertoff touted outreach by DHS during the NRF drafting process to incorporate the views of state, local and tribal officials, the emergency response community and the private sector. Chertoff's comments were noteworthy given the long tradition of state/federal tension in disaster response and preparedness. Unfortunately, since the terrible days of Hurricane Katrina it seems there has been little or no improvement of the rift between the federal government and the states over homeland security. According to a 2007 survey of state homeland security directors by the National Governors Association (NGA), the communication between the states and DHS has deteriorated significantly in the past 18 months.[2]

While these state/federal tensions can be attributed to fights over perpetually limited grant funding there are deeper, more fundamental and long-standing disagreements. In the NGA study concerns went beyond the usual disagreement over funding with state homeland security directors complaining that DHS initiatives were often developed and designed by contractors and states' input limited to the back end of this process.

The state/federal relationship is frayed particularly over the disaster roles of the military and the National Guard. Hurricane Katrina only served to demonstrate in stark terms how such conflicts, left unresolved, can result in tragedy. A recent bipartisan, blue ribbon commission examined the tangled lines of authority regarding the command and control of National Guard units and recommended that Governors be given greater statutory authority to direct all military forces with their respective states in the event of an emergency.[3] The Bush Administration and military leaders have strongly objected to this recommendation citing the President's constitutional role as Commander and Chief of the Armed Forces.[4]

Given this history, almost any action or decision by DHS in the current environment is bound to provoke outcry from some state or local official. So when the final version of the NRF was released by DHS, it was remarkable that there were few if any complaints from state and local officials. Indeed the release prompted little public reaction and garnered mostly praise

(Continued on Page 15)

[1] Robert T. Stafford Disaster Relief and Emergency Assistance Act as amended (Public Law 93-288) authorizes the President to provide assistance to state and local governments following presidential declared major disasters and emergencies.

[2] "If there is an area where states are reporting unsatisfactory progress, it is in their relationship with the federal government, specifically with DHS. More than half the states (57 percent) reported being dissatisfied or somewhat dissatisfied with their overall communications with DHS, and 60 percent said the quality of their communications with the department had either not changed or had deteriorated since 2006. Only slightly more than one-third, or 34 percent, said their communications with DHS had improved in that one-year period." National Governors Association, *2007 State Homeland Security Directors Survey*, December 18, 2007. http://www.nga.org/Files/pdf/0712HOMELANDSURVEY.PDF

[3] National Commission on the National Guard and Reserves, *Final Report*, January 31, 2009, pp. 21-22.

[4] John Gramlich, *Governors' Military Role Debated*, Stateline.org, February 7, 2008. http://www.stateline.org/live/details/story?contentId=279163

Understanding Homeland Security: Policy, Perspectives, and Paradoxes

James Madison University, Institute for Infrastructure and Information Assurance (IIIA) authors John Noftsinger, Kenneth Newbold, and Jack Wheeler offer a comprehensive analysis of homeland security in the post-9/11 world by exploring the current public policy security issues in the textbook *Understanding Homeland Security: Policy, Perspectives, and Paradoxes*. In chapter one, the authors thoroughly define the "nature of the threat," terrorism, by providing a historical overview of terrorist ideologies and tactics, culminating in a case study on suicide terrorism against the Russian government in Chechnya. The responsibility of DHS is often hard to comprehend for the general public. Noftsinger, Newbold, and Wheeler address this problem in chapter two, "What is Homeland Security," by discussing the mission and strategic goals of DHS with an emphasis on the private sector's role in R&D and delivery of services. The authors' continued commitment to strengthening the relationship between the public and private sector is apparent through IIIA's third annual research symposium's theme – "Fostering Public-Private Partnerships."

Public Policy issues are highlighted in the third chapter, with the authors deciphering the 132 pages of the USA PATRIOT Act into clearly stated objectives. For example, the monitoring of financial transactions is an integral component to the Act, as described on page 59, "Therefore, the Act also incorporated various statutes that addressed the financing of terrorist operations, many of which modified the Bank Secrecy Act of 1970. . . . As the tracking of assets and financial transactions may provide government agencies with additional information regarding the operation of terror cells, these specific provisions greatly bolstered their investigative abilities." Chapter four examines the information sharing and analysis responsibilities of the Intelligence Community under the leadership of the Director of National Intelligence (DNI). The authors educate the reader on the intelligence cycle from planning and direction to dissemination, concluding with a case study of the intelligence failures leading to 9/11. The reader is introduced to critical infrastructure protection in chapter five by a table top exercise examining the complexity within a nuclear power plant's supervisory control and data acquisition (SCADA) system. In this chapter, Noftsinger, Newbold, and Wheeler re-visit public and private partnerships, calling for enhanced information sharing between all vested stakeholders in order to heighten the resiliency and redundancy of U.S. critical infrastructure sectors.

Chapter six presents preparedness strategies focusing on risk communication, shelter-in-place, and community shielding techniques. This emphasis on "plan for the worst and hope for the best" is particularly relevant in light of the 9/11 attacks and Hurricanes Katrina, Rita, and Wilma. With immigration policy at the forefront of public debate, chapter seven's examination of the hot button policy issue of border security is quite timely. The final chapter provides a future outlook on homeland security policy with a call for innovation in education, enabling the United States to, "[Respond] to a new world of changing boundaries, global competition, rising expectations, finite resources, exploding technologies, changing societal norms, national security concerns, and a changing economy. . . ." *Understanding Homeland Security* touches on a variety of relevant subjects, which ideally suits the text for college students, professionals, or concerned citizens seeking a better understanding of homeland security policy.

The book is available on-line and through Palgrave Macmillan (www.palgrave-usa.com).

John Noftsinger, Kenneth Newbold, and Jack Wheeler, *Understanding Homeland Security: Policy, Perspectives, and Paradoxes*, New York, NY, Palgrave Macmillan, 2007, 205 pages

Dr. John B. Noftsinger, Jr. currently serves as Vice Provost at James Madison University. Mr. Kenneth F. Newbold, Jr. is the Director of Research Development at James Madison University. Mr. Jack K. Wheeler is a consultant with IBM in the areas of security, wireless, and privacy. ❖

Joint Research and the National CIP Agenda: The I3P Model

by Christine Pommerening, PhD, Senior Research Associate

Inter-disciplinary, multi-institutional, cross-sectoral — these buzzwords are ubiquitous in today's R&D world. Oftentimes, they merely indicate that there is more than one discipline, or more than one institution, or more than one sector involved in a particular project. Yet to make those terms meaningful, a deliberative and sustained effort is necessary.

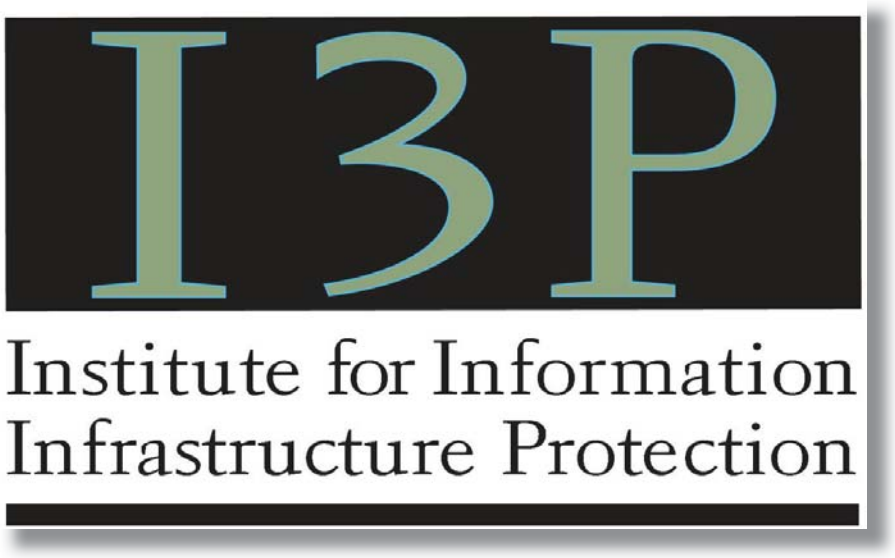
The Institute for Information Infrastructure Protection (I3P) is a consortium of 28 leading cyber security institutions, including academic research centers, national laboratories, and non-profit organizations, among them the George Mason University CIP Program. It was founded in September 2001 to help meet the need for improved research, development, and education to protect the nation's information infrastructure against catastrophic failures.

The I3P genesis and development of the I3P reflects in many ways the evolution of the cyber-security research agenda in academia, as well as the institutional changes within the federal government in relation to this type of research. Initially, the I3P was affiliated with the Institute for Security Technology Studies (ISTS) at Dartmouth College, which received funding from the National Institute for Standards and Technology (NIST). In 2003, the I3P was awarded an appropriation which was administered through DHS's Office of Domestic Preparedness. In 2006, the management of the grant was placed under DHS's National Cyber Security Division (NCSD).

The I3P has dedicated increasing effort and resources to actively coordinating and funding joint research projects that target specific areas of concern, rather than isolated technology development. The projects combine the efforts of different institutions under one topic, for example:

- Survivability and Recovery of Process Control Systems
- Business Rationale for Cyber Security
- Assessable Identity and Privacy Protection
- Human Behavior, Insider Threat and Awareness

The research topics are selected through dialogue within the consortium and with industry and government, considering gaps in national efforts, the criticality of the topic, and the impact the I3P could have as opposed to research conducted anywhere else. This approach is manifested in the identification of "grand challenges." For 2007, the grand challenge was: "Identity and Privacy Protection in a Digital World combined with aspects of Measuring Cyber Security." The idea is that this work will not only advance knowledge and foster collaboration among researchers, but will also contribute to demonstration projects with industry stakeholders. The success of this approach depends not on technology, but on people — the faculty and students, of course, but also on champions within industry and government who are willing to partner with the researchers, sponsor the projects, and implement the solutions. ❖



NRF *(Cont. from 3)*

scope of select ESFs. In revising the supporting documents, a limited number of annexes were combined and a new Support Annex dedicated to the coordination and integration of public and private critical infrastructure and key resources (CI/KR)-related incident response efforts was added.

The organization and content of the NRF are depicted in the textbox on page 2. Additional information on the NRF can be found in FEMA's NRF Resource Center at: http://www.fema.gov/nrf.

See the *Legal Insights* article on page 12 for information on reactions to the release of the NRF.

Note: The December 2004 National Response Plan, along with the modifications outlined in the May 25, 2006 Notice of Change, remains in effect until March 22, 2008. ❖

Legal Insights *(Cont. from 12)*

from officials normally used to criticizing DHS such as New York City Mayor Michael Bloomberg and U.S. Senator Joseph Lieberman, Ranking Minority Member of the Senate Homeland Security and Government Affairs Committee.

Senator Lieberman lauded DHS's outreach efforts saying: "I am pleased DHS consulted with state and local stakeholders to produce a comprehensive and coherent plan for responding to disasters of all sorts when they occur."

It is hoped that the NRF represents a turning point in the relationship between DHS and the states from the time of Hurricanes Katrina and Rita. However, revising one document is not enough to overcome the legacy of mistrust and misunderstanding between federal, state and local governments. As is typical in emergency preparedness and response, it is when the next major disaster strikes that these conflicts resurface. ❖

Information Sharing *(Cont. from 10)*

is also important to remember to protect the legal rights and privacy of Americans. The government has put in place Privacy Guidelines for Federal departments and agencies to follow. These include:

- Share protected information only to the extent it is terrorism information, homeland security information, or law enforcement information related to terrorism;
- Identify and review the protected information to be shared within the Information Sharing Environment (ISE);
- Enable ISE participants to determine the nature of the protected information to be shared and its legal restrictions;
- Assess, document, and comply with all applicable laws and policies;
- Establish data accuracy, quality, and retention procedures;
- Deploy adequate security measures to safeguard protected information;
- Implement adequate accountability, enforcement, and audit mechanisms to verify compliance;
- Establish a redress process consistent with legal authorities and mission requirements;
- Implement the guidelines through appropriate changes to business processes and systems, training, and technology;
- Make the public aware of the agency's policies and procedures as appropriate;
- Ensure agencies disclose protected information to non-Federal entities — including State, local, tribal, and foreign governments — only if the non-Federal entities provide comparable protections; and
- State, local, and tribal governments are required to designate a senior official accountable for implementtion.

This *Strategy* is part of the foundation that has been laid out to help better protect the Nation. All partners will benefit from establishing a fully coordinated and integrated information sharing capability. The expectation is that the *Strategy* will help facilitate the sharing of terrorism-related information and ultimately help combat terrorism.

For more information and a complete version of the *National Strategy for Information Sharing*, please visit the CIP Library on our website: http://cipp.gmu.edu/clib/reports.php ❖

Decision Directives *(Cont. from 11)*

For links to HSPD text and other pertinent information, please visit the CIP Program's CIP Library, Selective Government Reports on Infrastructure Protection webpage. ❖

The **National Infrastructure Protection Plan** (NIPP), featured in the August 2006 issue of *The CIP Report*, can be viewed on our website: http://cipp.gmu.edu/archive/NIPP_Plan6-06.pdf.

Sector-Specific Plans are available with unrestricted access for the following sectors:

CI/KR Sector-Specific Plans	Federal Sector-Specific Agency (SSA)
Agriculture and Food	Food and Drug Administration Department of Agriculture
Banking and Finance	Department of Homeland Security
Communications	Department of the Treasury
Defense Industrial Base	Department of Defense
Information Technology	Department of Homeland Security
National Monuments and Icons	Department of the Interior
Transportation Systems	Department of Homeland Security
Water	Environmental Protection Agency

Additional information on the NIPP and the SSPs can be found at: http://www.dhs.gov/nipp. Sector stakeholders can also request access to the For Official Use Only (FOUO) SSPs through DHS's website.

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