THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 6

DECEMBER 2006

THE YEAR IN REVIEW

Contact: CIPP01@gmu.edu
703.993.4840
Click **here** to subscribe. Visit us online for this and other issues at http://cipp.gmu.edu

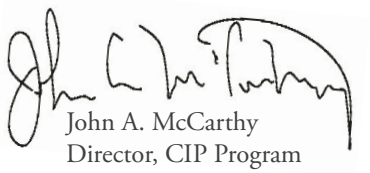
GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Several of the most significant critical infrastructure protection and homeland security initiatives in 2006 were a direct result of an event that happened in August 2005: Hurricane Katrina. Faced with widespread criticism of the response and recovery efforts following Katrina, government and private sector leaders at all levels took an introspective look at what went wrong, what went right, and what changes needed to be made. Four years after 9/11 and a massive ramp up of an entire homeland security sector revealed that the nation still has significant strides to make before it is truly prepared. In many ways, Katrina defined the year in critical infrastructure protection.

This month's issue of *The CIP Report* takes a look back at 2006, beginning with a table of some of the most significant events that took place, from the announcement of a risk-based formula for the Urban Area Security Initiative grants in January to the launch of the Secure Freight Initiative in December. We provide a brief summary of each milestone, and examine some of the initiatives more fully in subsequent articles.

A piece on trends in cyber security R&D discusses priorities that have been identified by three separate bodies working in this field. Additional articles on pandemic preparedness and the public / private partnership review accomplishments made in 2006 and the current status of initiatives in those respective areas. The Legal Insights column examines the amendment in the Defense Authorization Act that provides for additional causes for suspending *posse comitatus*. Finally, we provide a report from "Cyber Tempest," a recent simulation exercise held in New York State.

If 2006 was a year of introspection and lessons learned, I hope that 2007 will witness the full implementation of the highest priority initiatives, many of which were launched this year. The next time our nation faces catastrophe, whether man-made or natural, we will be better prepared. On behalf of the CIP Program, I would like to thank you for your continued support, and wish you and yours the happiest and safest of holidays.



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

Critical Infrastructure Protection in 2006: The Year in Review

January

Risk-based formula announced for Urban Areas Security Initiative Grants

The Department of Homeland Security (DHS) announced that it would be providing high threat urban areas with $765 million in direct funding for unique equipment, training, planning and exercises. The 35 urban areas (encompassing 95 cities) that were identified as eligible for grants, were invited to submit investment justifications that would be assessed through a new risk based formula that considered three primary variables: consequence, vulnerability, and threat. Eleven areas that received grants in 2005 were carried over to the 2006 list in order to continue efforts that were launched but not yet completed.

February

Nation's first full-scale cyber security exercise conducted

Cyber Storm, the first full-scale government-led cyber security exercise to examine response, coordination, and recovery mechanisms within international, federal, state, and local governments, was held in conjunction with the private sector. In total, 115 public, private, and international agencies, organizations, and companies were involved in the planning and implementation of Cyber Storm, which was held in more than 60 locations in five countries. The exercise simulated a sophisticated large-scale cyber attack directed against multiple critical infrastructures, which highlighted interdependencies between and among cyber and physical assets, and exercised coordination and communication between public and private sectors. The exercise report, which was released in September 2006, identified several problems that slowed response times, including inconsistent information sharing, lack of contingency planning, and difficulty correlating multiple events between public and private sectors.

White House releases lessons-learned report on the Federal response to Hurricane Katrina

The Federal Response to Hurricane Katrina: Lessons Learned report identified deficiencies in the Federal response to one of the nation's worst natural disasters. The report stated that emergency plans at all levels of government, including the National Response Plan, were "put to the test and came up short." The Lessons Learned report identified three immediate priorities, including implementation of a comprehensive National Preparedness System, creation of a "Culture of Preparedness" in which all citizens share common goals and responsibilities for homeland security, and implementation of corrective actions to prevent a repeat of the problems Hurricane Katrina revealed.

Study on infrastructure resilience in the National Capital Region released

The CIP Program's National Capital Region Critical Infrastructure Project (NCR-CIP) released the results of a two-year research program on risk-based foundations for increasing infrastructure resilience on the regional level. Topics in the report ranged from individual sector analyses to regional risk management to citizen and community issues. The key recommendation of the report was the creation of a public / private partnership dedicated to critical infrastructure protection within the NCR.

Recommendation of the Committee on Foreign Investment in the U.S. raises questions

The previously little-known Committee on Foreign Investment in the U.S. became the focus of the nation as it recommended approval of the purchase by Dubai Ports World of contracts to provide services at major U.S. ports. The sale was part of a larger deal in which Dubai Ports World purchased the P&O Steam Navigation Company of Britain. Dubai Ports World is owned by the government of the United Arab Emirates and some in Congress questioned the decision to allow the sale to go through. Dubai Ports World ultimately agreed to sell off its U.S. holdings. On December 11th it announced the sale to AGI Global Investment Group.

April

Port worker credentialing program launched

In a measure to secure access to U.S. ports, the Department of Homeland Security launched a program to perform name-based background checks on port workers. This was the initial step in a larger rollout of a nationwide biometric-based Transportation Worker Identification Card (TWIC), which will eventually be required for anyone needing unescorted access to secure areas and will include a full criminal record check. In this initial step, basic identifying information is collected by the U.S. Coast Guard and checked against terrorist watch lists through the Terrorist Screening Center. The Transportation Security Administration will apply the same security threat assessment standards to merchant mariners and workers that it currently does to commercial drivers who transport hazardous materials.

(Continued on Page 3)

The Year in Review *(Continued from Page 2)*

April

Maritime Infrastructure Recovery Plan introduced

The Maritime Infrastructure Recovery Plan, which includes guidelines for coordinated national efforts to restore the flow of cargo and passenger vessels in response to a major maritime disruption, was introduced in April. The plan also included a periodic exercise that would assess the maritime sector's ability to respond to a large-scale incident. The plan, which focuses on all forms of cargo, would be activated by the Secretary of Homeland Security in the event of a significant national transportation incident.

May

Ready Business Mentoring Initiative introduced by DHS

As an extension of the Ready Business campaign launched in 2004, the Ready Business Mentoring Initiative was introduced through a collaboration of U.S. government agencies in an effort to provide millions of small- to medium-sized business owners with emergency preparedness tools. As part of this initiative, Ready Business Mentoring Guides provide step-by-step information designed to teach business owners and managers about affordable ways to protect their businesses. The Ready Business Mentoring Initiative is the latest resource in the broader Ready Business campaign, which was launched in 2004 to encourage small- to medium-sized business owners (who comprise 99 percent of all U.S. employers) to make an emergency plan, talk to their employees, and protect their assets.

$1.7 billion in homeland security grants announced

DHS announced $1.7 billion in Homeland Security Grant Program (HSGP) awards, with the goal of helping states, urban areas, and territories prepare for and respond to terrorist attacks and other disasters. According to Homeland Security Secretary Michael Chertoff, the money was intended to help make sure that "finite resources are directed to areas most at risk." HSGP funds are highly flexible: they can be used for everything from planning to organization, equipment, training, exercises, management, and administration costs. Currently, they encompass five separate grant programs: State Homeland Security Grant Program, $544.5 million; Urban Areas Security Initiative, $757.3 million; Law Enforcement Terrorism Prevention Program, $396 million; Metropolitan Medical Response System, $29.7 million; and Citizen Corps Program, $19.8 million.

June

Review of nationwide catastrophic event preparedness conducted

Responding to directives from President Bush and the Congress, following Hurricane Katrina, DHS published a national assessment of the country's catastrophic planning capabilities in June. The Nationwide Plan Review looked at whether existing emergency operations plans are currently sufficient to manage a catastrophic national event. While most areas of the country are well prepared to handle standard disaster situations, the National Plan Review findings demonstrate the need for all levels of government across the country to improve emergency operations plans for catastrophic events such as a major terrorist attack or a category-five hurricane strike. Several areas, including evacuation, attention to populations with special needs, command structure, and resource management, were areas needing significant attention.

National Infrastructure Protection Plan released

The National Infrastructure Protection Plan (NIPP)was completed this summer. The NIPP is a comprehensive risk management framework that defines the critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies and tribal partners. The NIPP builds on the principles of the President's National Strategy for Homeland Security and also fulfills requirements in Homeland Security Presidential Directive 7 and the Homeland Security Act of 2002. The National Infrastructure Protection Plan is available online at www.dhs.gov/nipp.

July

Grants awarded to secure nation's rail systems

DHS has funded Federal, state, and local initiatives to improve the nation's rail security. State and local partners have received $375 million since 2003, with $110 million granted in 2006 alone. DHS also trains teams to deal with potential terrorist actions, conducts site assessments, and develops new screening technologies to be used on trains and other rail sites.

(Continued on Page 4)

The Year in Review *(Continued from Page 3)*

July

Four universities collaborate on homeland security research

The Department of Homeland Security selected a team of four universities to conduct research on advanced methods for information analysis and develop computational technologies that contribute to securing the homeland. Rutgers University is serving as the coordinating affiliate center and is joined by the University of Southern California, the University of Illinois at Urbana-Champaign, and the University of Pittsburgh. Their work will advance efforts to identify common patterns from numerous sources of information, which may be indicative of potential threats to the nation. DHS expects to award a total of $10.2 million over three years to these institutions and partners.

August

Threat level change and modifications to security procedures for the aviation sector

In mid-August the threat level was raised to High or Orange for all commercial aviation operating in or destined for the United States as a result of the British authorities arrests of a significant number of extremists engaged in a substantial plot to destroy multiple passenger aircrafts flying from the United Kingdom to the United States. DHS also prohibited any liquids, including beverages, hair gels, and lotions from being carried on airplanes. In September, the Transportation Security Administration announced two modifications to the security procedures put in place in August: (1) Travelers may carry-on travel size medicines and toiletries (3 oz. or less) in one quart-size, clear, plastic, zip-top bag and (2) Passengers may now purchase drinks and other items in the secure boarding area after the checkpoint and carry them on board. The threat level remains at High or Orange.

September

National Preparedness Month 2006

More than 1,150 national, regional, state, and local organizations joined with DHS to launch National Preparedness Month in September 2006. The goal of National Preparedness Month is to educate Americans about the importance of emergency preparedness through hundreds of events and activities in communities across the country. The nationwide effort encourages every American to prepare for emergencies in their homes, businesses, schools, and communities. The focus of this year's National Preparedness Month is family emergency preparedness, reminding individuals to make themselves and their loved ones better prepared.

Fifth Anniversary of September 11th

In September, the nation marked the fifth anniversary of 9/11. Secretary of Homeland Security, Michael Chertoff, reflected on the five years that have passed since the terrorist attacks, noting that there have not been any attacks on American soil since that day. However, he recognized that there have been attacks on American citizens overseas, as well as allies and innocent civilians in London, Bali, and Madrid. Mr. Chertoff underscored the need for a pragmatic approach to emergency prevention, protection, and response. He outlined DHS efforts to secure the border, screen cargo, protect critical infrastructure, improve information sharing, and enhance emergency preparedness and response. The Secretary emphasized the importance of interagency collaboration to test capabilities in emergency circumstances.

Assistant Secretary for Cyber Security and Telecommunications appointed

Greg Garcia was appointed as the Assistant Secretary for Cyber Security and Telecommunications at DHS. Mr. Garcia joined the Department from the Information Technology Association of America, where he was Vice President for Information Security Policy and Programs. He has also worked for Americans for Computer Privacy, the Americans Electronics Association, the IT Sector Coordinating Council, and the U.S. House of Representatives Committee on Science. Mr. Garcia's expertise in the debate on cyber security policy and national cyber readiness gives him the ability to focus the priorities within the cyber and telecommunications communities according to a risk-based approach.

$399 million in grants to secure the nation's critical infrastructure

The Department of Homeland Security has distributed grants to critical port, transit, and intercity bus systems to strengthen the nation's ability to prevent, protect against, respond to and recover from terrorist attacks, major disasters, and other emergencies. The trucking and intercity passenger rail security, buffer zone, and chemical buffer zone programs received funding earlier in the year as part of the Infrastructure Protection Program (IPP). DHS has awarded a total of $399 million to the seven programs comprising the IPP in 2006. The grant distributions were based on threat, vulnerability and consequences, as well as the unique characteristics of each critical infrastructure asset.

(Continued on Page 5)

The Year in Review *(Continued from Page 4)*

October

2007 Homeland Security Appropriations Bill passed

The Fiscal Year 2007 Homeland Security Appropriations Bill, enacted in 2006, focuses resources on strengthening FEMA and improving border and chemical security. The $34.8 billion bill also increases transportation, port, and nuclear detection funds. FEMA remains in DHS, but is granted greater autonomy, authority, and funding by the bill to prepare for and respond to national disasters.

Cyber Security Awareness Month

DHS designated October 2006 National Cyber Security Awareness Month to remind Internet users to take responsibility for their own cyber security. As part of the awareness program, the National Cyber Security Division informed Internet users of the need to install anti-virus and firewall protection, and to continually check for system and anti-virus updates. DHS released cyber-security tips, held national awareness events, and worked with more than 20 states to publicize state-wide cyber security awareness events.

President signs SAFE Port Act

The President signed the Security and Accountability for Every Port Act (SAFE Port Act) into law to improve cargo and personnel security at the nation's ports. The SAFE Port Act authorizes and funds new technology to scan incoming cargo for dangerous materials. The Act also authorizes an initiative to inspect cargo bound for the U.S. at foreign ports, public and private efforts to encourage voluntary security measures, and resumption of trade protocol.

John Warner National Defense Authorization Act for Fiscal Year 2007

The President signed the John Warner National Defense Authorization Act for fiscal year 2007 which includes funding for military construction, national security energy programs, and maritime security transportation programs. The Act also outlines several areas where the executive branch should, when appropriate, communicate with Congress on national security, execution of the law, and other various subjects.

November

Aircraft cargo screening program begins testing at Seattle-Tacoma airport

The $30 million Air Cargo Explosives Detection Pilot Program (ACEDPP) which was announced earlier in the year started a testing program at Sea-Tac airport in order to better understand the technological and operational issues associated with detecting hidden persons or explosives that could be in air cargo. ACEDPP, which is a collaboration of several Federal agencies and national laboratories, is intended to provide critical knowledge that will help transportation officials make future decisions on air cargo. The Seattle test will focus on areas that include assessing the flow of air cargo and how quickly it must be screened, detection of carbon dioxide, which may indicate the presence of a human in the cargo, and detection of the most effective technologies for vulnerability reduction.

December

Secure Freight Initiative launched

The Secure Freight Initiative is an unprecedented effort to build upon existing port security measures by enhancing the federal government's ability to scan containers for nuclear and radiological materials overseas and to better assess the risk of inbound containers. This initial phase involved the deployment of a combination of existing technology and proven nuclear detection devices to six foreign ports: Port Qasim in Pakistan; Puerto Cortes in Honduras; Southampton in the United Kingdom; Port Salalah in Oman; Port of Singapore; and the Gamman Terminal at Port Busan in South Korea. Beginning in early 2007, containers from these ports will be scanned for radiation and information risk factors before they are allowed to depart for the United States.

R&D Trends for Federal Cybersecurity – Hard Problems and Soft Priorities

Christine Pommerening, Ph.D., Senior Research Associate, CIP Program

The year 2006 featured a number of high-level attempts to lay out the research agenda for critical information infrastructure protection; both for federal IT and telecom systems and within the industry at large. Given the long-term nature of basic and applied R&D, the issues and challenges identified in those reports are likely to form the core of extensive research efforts by government, industry, and academia well into the second decade of the millennium.

The first milestone was set in late 2005, when the Infosec Research Council (IRC) updated its six-year old original "Hard Problems List." The IRC represents the major sponsors of information security research within the federal government, and aims at identifying a set of key issues in the context of their member agencies' missions. The list contains cybersecurity problems that are unlikely to be solved in the next five to ten years, unless a concerted effort is undertaken within the government and in close collaboration with private industry developers and vendors. It should be noted that the eight problem areas listed explicitly focus on the technical challenges, and thus do not address for example the educational, economic, financial, and legal issues, even though it is recognized that these are inextricably linked to the development and adoption of new technologies.

IRC Hard Problems List

- Global-Scale Identity Management
- Insider Threat
- Availability of Time-Critical Systems
- Building Scalable Secure Systems
- Situational Understanding and Attack Attribution
- Information Provenance
- Security with Privacy
- Enterprise-Level Security Metrics

Source: www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf

In the spring of 2006, the National Science and Technology Council (NSTC) released the Federal Plan for Cyber Security and Information Assurance Research and Development; partly in response to the IRC list and earlier guidelines such as the President's Information Technology Advisory Committee (PITAC) report, the National Strategy to Secure Cyberspace, and the Cyber Security Research and Development Act. The Plan provides baseline information and a technical framework for coordinated multi-agency R&D. But like the IRC list, it does not deal with law, economics, or policy issues impacting potential solutions, nor does it outline operational IT security approaches and best practices.

The list below contains the 14 (out of 49) topics that have been identified as technical priorities across agencies. For a variety of reasons, they are not necessarily identical with intra- or interagency funding allocations, but that discussion would go beyond this brief review of technology-centered R&D plan-

(Continued on Page 7)

NSTC Top Technical Priorities

- Authentication, Authorization, and Trust Management
- Access Control and Privilege Management
- Attack Protection, Prevention, and Preemption
- Large-Scale Cyber Situational Awareness
- Secure Process Control Systems
- Wireless Security
- Security of Converged Networks and Heterogeneous Traffic
- Detection of Vulnerabilities and Malicious Code
- Software Testing and Assessment Tools
- IT System Modeling, Simulation, and Visualization
- Inherently Secure, High-Assurance, and Provably Secure Systems and Architectures
- Composable and Scalable Secure Systems
- Architectures for Next-Generation Internet Infrastructure
- Privacy

Source: www.nitrd.gov/pubs/2007supplement/07%20Supp%20Sections/07Supp_FINAL-CSIA.pdf

R&D Trends *(Continued from Page 6)*
ning documents. What is interesting from the perspective of overall CIP is that problems identified by many infrastructure owners and operators such as standards, metrics, risk-based decision making, CI dependencies and interdependencies, recovery, reconstitution, and resilient systems, did not reach either the technical or the financial priority threshold. They may still be mission priorities in individual departments such as DHS, however.

Subsequently, the Office for Networking and Information Technology R&D (NITRD) has issued a call for white papers that shall help in developing a roadmap based on the priorities list. Input is sought primarily from outside the government, which provides an opportunity for industry experts and academia stakeholders to establish interactions with the federal side and shape the future direction of research.

In September 2006, the National Security Telecommunications Advisory Committee (NSTAC) held its seventh R&D exchange; an international workshop intended to stimulate and facilitate a dialogue among industry, government, and academia on emerging security technology research and development issues. During the five thematic sessions, experts from the public and private sectors were asked to identify key R&D areas that are particularly relevant in the international context. In contrast to the other two reports, the participants formulated a number of underlying policy issues along with the technical themes, most prominently the need to develop global standards and metrics, a trusted collaborative environment, economic incentives for adoption, and liability issues. The list to the left is a summary of a draft report on those breakout sessions; hence it is more generic than the other lists.

Even this brief review reveals that federal R&D planning is not confined to government systems, and encompasses fundamental IT security problems. While the emphasis on certain problems might be different in private sector-led research or in academic departments, the complexity and interdepen-
(Continued on Page 16)

NSTAC RDX Key Areas

International Internet Governance
- 3rd Party Evaluation of Current Oversight Processes
- Common Frameworks for Information Management
- Common Assessment and Mitigation Tools
- Preemptive Discovery
- Multi-Lateral Sharing and Response

Global-Scale Identity Management
- Platform-Independent Credentials
- Interoperability of IDM Systems
- Assurance Models and Reliability Metrics
- Trust Agreements and Acceptable Error Rates
- Cost Models for Global-Scale Deployment

Collaborative Mechanisms for Network Security Protocols
- Wide-Scale Situational Awareness for Attack Prediction and Detection
- Resilient and Secure Protocols
- Global Scale Authentication and Identity Management
- Secure and Scalable Routing Infrastructure
- Security Metrics

Cross-Border & Cross-Sector Challenges
- Incentives for Private Sector
- Inventory of Existing R&D Initiatives
- Move beyond Bilaterals between Governments
- Establish "Ground Truth"
- Establish Priorities for Restoration

Wireless and Mobile Ad Hoc Network Applications
- Global Deployments / Registry
- Group Key for Interoperability, Dynamic Changes and Scale
- Test Bed / Standards / Certification / Requirements
- Biometric Authentication
- Location-Based Service

Source: http://www.ncs.gov/nstac/rd/rd_docs/Ont_Breakout_Session_Reports.pdf

Legal Insights

The Insurrection Act (Title10, U.S. Code, sections 331-335) and the John W. Warner Defense Authorization Act of 2006 (PL109-364)

Randall Jackson
Senior Legal Research Associate , CIP Program

The John W. Warner Defense Authorization Act of 2006 (Defense Act), signed into law by President Bush on October 17, 2006, as PL 109-364, has within it a section entitled "Use of the Armed Forces in Major Public Emergencies," section 1076. This section amends the Insurrection Act (Title 10, U.S. Code, sections 331-335), by listing other contingencies that can create the authority to use the military to enforce domestic law. The authority itself remains the same, requiring a situation in which U.S. law cannot be carried out. The amendment recognizes the fact that reaching such a level can be the result of events other than "insurrection" or "rebellion." In such cases, using the military for domestic law enforcement, and therefore the temporary suspension of *posse comitatus*, can occur.

The idea behind the *posse comitatus* statute is an important one within the American democratic structure. It plays the important role of prohibiting the use of the military for domestic law enforcement. In comments at a September 29, 2006, breakfast hosted by the ABA's Standing Committee on Law and National Security, featured speaker Mr. Paul McHale, Assistant Secretary of Defense for Homeland Defense, commented upon the importance of the limited role of the military in domestic affairs. Assistant Secretary McHale reflected on the Federalist Papers writings of Alexander Hamilton. Rather than a fear of some kind of overt take-over, for Hamilton the main threat to be avoided would be the dependency that can arise should a civilian government look to the military to secure its internal order. Hamilton feared that as soon as the government started deferring to the military, it would embark upon a path that would finally lead to a total reliance at the price of civil liberties. It is for these reasons that the Founding Fathers created a system in which civilian authority is supreme, and the military remain focused on their primary function: protecting the United States from external threat.

> ***"...It is for these reasons that the Founding Fathers created a system in which civilian authority is supreme, and the military remain focused on their primary function: protecting the United States from external threat."***

Nevertheless, there are exceptions to *posse comitatus*. Such exceptions must be "expressly authorized by the Constitution or by act of Congress…" (Posse Comitatus Act, Title 18, U.S. Code, Section 1385). An example of such an exception is the Insurrection Act (Title 10, U.S. Code, sections 331-335). The Insurrection Act empowers the President to use the military to enforce domestic law in the event that "unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States, make it impracticable to enforce the laws of the United States in any State or Territory by the ordinary course of judicial proceedings…" (Insurrection Act, Title 10, U.S. Code, section 332). Before calling the military into action, the President must issue a proclamation to disperse to the insurgents (Insurrection Act, Title 10, U.S. Code, section 334). The Insurrection Act has not been often used since its passage in 1807. Examples of its activation include the 1992 Los Angeles Riots and the enforcement of school desegregation in Little Rock in 1957.

In the Defense Act, the Insurrection Act has been amended to recognize other triggers to the President's authority to use military resources to enforce domestic law without violating *posse comitatus*. The major

(Continued on Page 9)

Legal Insights *(Continued from Page 8)*
change occurs in section 1076 of the Defense Act. In this section, the legislation amends the Insurrection Act's section 333 by explicitly allowing the President to use military resources not just in the event of insurrection or rebellion, but also to:

> "restore public order and en force the laws of the United States when, as a result of a natural disaster, epidemic, or other serious public health emergency, terrorist attack or incident, or other condition in any State or possession of the United States, the President determines that (i) domestic violence has occurred to such an extent that the constituted authorities of the State or possession are incapable of maintaining public order; and (ii) such violence results in a condition described in paragraph (2)…" (John W. Warner Defense Authorization Act of 2006, section 1076(a)(1)'(a)).

The paragraph (2) to which the passage alludes delineates the inability to execute the laws of the United States in the State or possession in which the unrest takes place and marks the level of disorder to which the insurrection must rise in order to activate the authority of the provision.

The Defense Act has expanded the list of possible causes that can create the high level of disorder necessary for the authority to use the military to enforce domestic law. Rather than simply as a result of insurrection, the disorder could be caused by natural disaster, terrorism, epidemic, etc. There is no change in the level of disorder that must be attained to activate the authority; only an expansion of possible underlying causes.

The President must still issue a proclamation to disperse pursuant to Title 10, U.S. Code, section 334 (the language of to whom the proclamation must be issued has been amended in the Defense Act); and he "shall notify Congress of the determination to exercise the authority…as soon as practicable after the determination and every 14 days thereafter during the duration of the exercise of that authority" (John W. Warner Defense Authorization Act of 2006, section 1076(a)(1)'(a)'(3)'(b)).

The situation in the aftermath of Katrina played a large part in motivating lawmakers to re-examine the two-hundred year old Insurrection Act. With the breakdown of a functioning public sector, stories emerged of looting and other lawless behavior (even gun fire) on the ground in New Orleans and the areas hit hardest by the storm. Many of these reports turned out to be false, however the premise remained that in a situation as severe as Katrina, the potential for societal breakdown is real. In such a situation, it may become impossible to execute U.S. law without turning to the military. However, it could be difficult to define the underlying reason for the unrest as an "insurrection." It could therefore be problematic, and politically risky, for a President to invoke the Insurrection Act knowing that he will have to defend his actions after the fact as having been necessary to put down an "insurrection." By changing the language in the Insurrection Act, Congress has explicitly acknowledged that the unrest may be the result of emergencies other than insurrection: natural disaster, epidemics, terrorism, etc. It would have been difficult to define any looting and other lawless behavior in New Orleans as an insurrection. There was no attempt to gain political power or other actions to which one could point as typical of an insurgent uprising.

In February, 2006, CIP Program Director and Principal Investigator John McCarthy and Sr. Legal Research Associate Randall Jackson were part of the ABA Standing Committee on Law and National Security's Hurricane Katrina Task Force Subcommittee. McCarthy and Jackson (with additional research support from CIP Program Legal Research Associate Maeve Dion) contributed a chapter to the report in which this issue was briefly touched upon. In the aftermath of Katrina, questions emerged as to why President Bush did not invoke the Insurrection Act at a time of supposed chaos in New Orleans and other areas. The ABA Report talks about political impediments arising from the presence of a Democratic Governor and a Republican Administration. Given this context, defining even a storm as destructive as Katrina as an "insurrection" seems problematic and fraught with potential political landmines, particularly in any post-emergency reviews. By explicitly including natural disasters, etc., the hope is that at least to some extent politi-
(Continued on Page 16)

Key Issues Addressed in 2006 Concerning Pandemics

Colleen Hardy, Senior Research Associate, CIP Program

The possibility of a flu pandemic was a major topic examined and discussed in great detail in 2006. Many government agencies, academics and health care experts met to discuss preparation plans and responses to the possibility of a flu pandemic. Both federal and state government agencies have rigorously worked together to prepare plans and responses for an outbreak of the flu.

In May 2006, the *Implementation Plan for the National Strategy for Pandemic Influenza* was released. The plan asked each federal department to create an implementation plan which describes how it will execute it's responsibilities detailed in the national plan. It additionally asked each department how they will prepare their employees. President Bush stated, "Building upon these efforts, the Implementation Plan for the National Strategy for Pandemic Influenza ensures that our efforts and resources will be brought to bear in a coordinated manner against this threat."

The National Infrastructure Advisory Council put together a report to determine which, if any, critical infrastructure workers should be first in line to receive vaccinations should a flu pandemic occur? The council discussed the importance of critical infrastructure workers and how their jobs are essential to the United States' daily operations and functions. The council noted that law enforcement, healthcare and communication workers are vital and need vaccination. However, they went on to note that employees in information technology, water, power lines and banking also play an essential role in the nation's well-being. The National Infrastructure Advisory Council's report is expected to be released in January.

The Department of Health and Human Services released a report last month which detailed the ongoing preparation and efforts the government has taken in the past year. The report stated that Congress provided $5.6 billion for research and preparedness. The report went on to declare that vaccine research "continues at a frantic pace." Currently there are millions of avian flu vaccines available to Americans. The report also stated that every state has drafted a preparedness plan.

The Centers for Disease Control and Prevention is producing and finalizing a vaccination distribution plan. Response officials in local communities are concerned that the distribution plan will not operate efficiently and effectively due to the lack of communication between government agencies and local private sector employees who will actually distribute the vaccines. According to preliminary reports, the plan would send vaccinations to affected communities overseas in the hope of preventing the flu from reaching the U.S.

The above efforts are not inclusive of all discussions and preparations but an overview of a few key issues currently being researched and examined. While much attention and effort was put forth towards preparing and determining appropriate response roles and responsibilities, there are still issues and questions that need to be addressed so that the U.S. is fully prepared to respond to a flu pandemic. The government and other health experts are continuing to work diligently on these issues and response plans. The CIP Program's law team has invited several leading experts to write an essay for a monograph about two important issues concerning pandemics. The first section will address the prioritization of distributing vaccines. Specifically, if a pandemic were to occur and vaccines needed to be distributed, should critical infrastructure employees have priority to receive the vaccines? The second section will examine the mechanism for vaccination distribution. In particular, who would provide security for those distributing the vaccinations or medicines? Where is the best place for vaccinations to be distributed? How should the state and/or local government notify the public about where to go to receive their vaccinations? The CIP Program will compile these essays into a monograph and publish it on our website. If you would like to contribute to the monograph, please contact chardy@gmu.edu or 703.993.4793. ❖

Cyber Tempest

Regional Cyber Exercise / Dec. 4-5, 2006

Maeve Dion, Legal Research Associate, CIP Program

Sponsored by
New York State Office of Cyber Security and Critical Infrastructure Coordination, and
the Multi-State Information Sharing and Analysis Center,
and Supported by
Department of Homeland Security, National Cyber Security Division

It started as a typical day: software vendors released routine patches; US CERT issued an alert on unexploited vulnerabilities in a common Internet browser; and there was some increase in underground chat activity, but nothing extraordinary.

However, within a short period of time, electric utilities, financial institutions, healthcare facilities, and some northeastern state governments began to suffer intermittent failures of their telephone networks (PSTN).

Meanwhile, false information injected into state department of transportation websites resulted in interstate traffic congestion at unparalleled levels.

In the financial and electricity sectors, customers were locked out of their online accounts. Government employees in five northeastern states were locked out of government networks. Healthcare providers were unable to access their Health Provider Network accounts. DDoS attacks were hitting email servers of institutions in all of these sectors.

As part of the Cyber Tempest exercise, these events were played out in four rooms at a state conference center outside of Albany, New York. The approximately 100 participants represented federal, state, and local agencies; businesses and associations in the financial, electric, healthcare, information technology, and telecommunications sectors; the MS-ISAC, FS-ISAC, Communications ISAC, and IT-ISAC; and observers from academia and the Canadian government.

In addition to the above scenarios, the participants had to address numerous problems, including: unreliable T1 lines and frame relays; unreliable ATM communications; intermittent 911 service; discovery of physically-installed keyloggers; corruption of the northeastern states' Criminal Justice Information System databases; and extortion demands and threats of additional damage.

All this on only the first day of the exercise.

The second day heralded additional problems, including failure of the
(Continued on Page 12)

The approximately 100 participants in the Cyber Tempest exercise included representatives from federal, state, and local agencies; businesses and associations in the financial, electric, healthcare, information technology, and telecommunications sectors; the MS-ISAC, FS-ISAC, Communications ISAC, and IT-ISAC; and observers from academia and the Canadian government.

Cyber Tempest *(Continued from Page 11)*
elevators and heating, ventilation, and air conditioning (HVAC) systems in healthcare and financial institutions; escalating reports of insufficient funds in commercial customers' financial accounts; widespread water purification problems due to corrupted process control systems for purification applications; failure of electric utilities' energy management systems; failure of electric utilities' frame relays; and wide area rolling electrical power disruptions in the northeast.

This two-day Cyber Tempest was organized by the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), and was supported by the Department of Homeland Security's National Cyber Security Division (NCSD).

As stated by William F. Pelgrin, Director, New York State CSCIC and MS-ISAC Chair, the primary goal of Cyber Tempest was "to exercise the interaction (e.g., information-sharing, coordination, etc.) and consequences of regional cyber network disruptions, as well as explore the vast complexities of interrelated effects." Pelgrin continued, "It's a great collaboration between levels of government and with the private sector. It's not about how good we are -- it's about how good we can be."

Jeff Wright, Deputy Director for Strategic Initiatives, and Director for Exercises, NCSD, gives the opening address.

The exercise was similar to a war game, in that the participants' responses, decision-making, and information sharing affected the exercise. Cyber Tempest focused on a wide area of cyber disruption from a regional perspective, and thus was artificially bounded to avoid addressing the scope of events resulting from a declared Incident of National Significance or a Federal Emergency Declaration. The participants were also instructed to discuss only the cyber implications, and not the technical causes of the events or the possible physical consequences.

Throughout the exercise, participants focused on how to (1) gain and maintain situational awareness; (2) develop strategy / actions with an integrated response; (3) mitigate consequences; (4) allocate limited resources; and (5) collect, analyze, formulate, and disseminate information to stakeholders (including the media). The participants also developed recommendations for sector regulators. The control group facilitated the exercise and created a process to record the inter-group communications (who initiated the communication; to whom they communicated; content of the communication; and response / outcome).

Cyber Tempest was structured so that there were four separate groups during the gaming sessions -- Government, Financial, Healthcare, and Utilities (IT/Telecom, and Electricity). The groups communicated with each other via couriers. Members of the Control Group monitored the gaming groups to ensure that the participants adhered to the scenario injects. The Control Group also acted as "extras" (software vendors, Federal intelligence organizations, etc.) to respond to the participants' queries. During the gaming sessions, there were also periodic ISAC meetings, drawing participants from each group. After each gaming session, there was an outbrief attended by all participants.

The exercise exposed the diverse decision-making thresholds among industries (e.g., when to contact an ISAC, when to assume certain problems were correlated, when to report to law enforcement, when to ask for government help, etc.). During the first outbrief, participants wondered if, in the normal workday setting, they would have correlated the events, and if so, when (i.e., too late?). As one participant commented, "if we were not all in the same room, would we have reached these conclusions? Would we have asked, 'is this happening somewhere else?'"

Confidentiality, reputation cost, and other trust issues were another big factor. Not only did institu-
(Continued on Page 15)

Highlights of the CIP Public / Private Partnership in 2006

Olivia Pacheco, CIP Program

Two important milestones in the public / private partnership during 2006 were the establishment of the Critical Infrastructure Protection Advisory Council (CIPAC) and the Department of Homeland Security's release of the National Infrastructure Protection Plan (NIPP).

CIPAC was established by the Secretary of Homeland Security in March to create a collective, collaborative working space in which to conduct joint activities and have discussions on sensitive security issues between the government and private sector. This environment has allowed important discussions to occur on critical infrastructure protection, pandemic influenza planning, and hurricane preparedness.

The completion of the NIPP by DHS in June 2006 called for each sector to complete its own Sector-Specific Plan (SSP). Security partners in the government and the private sector have devoted the past six months to developing an SSP for each sector. The goal of the SSP is to compliment the NIPP by addressing sector-specific concerns. The Sector Coordinating Councils (SCCs) were asked to focus on specific questions when working on their SSP. These questions included: What are the sector's priorities? Is there a process for conducting risk assessments? As threats change, is there a process to revisit and update vulnerabilities? What are the research and development needs? How does a sector measure progress? The process of writing the SSPs was discussed in-depth throughout the year. Interdependencies between sectors were also addressed and held significant value in the structuring of certain sector plans. SCCs met regularly with the Government Coordinating Councils (GCC) to develop their SSPs. Final SSPs are due to be completed by December 31, 2006.

Private sector pandemic influenza planning centered on ensuring that key resources maintain functionality. DHS published a "*Critical Infrastructure/Key Resource (CI/KR) Pandemic Influenza Preparedness, Response and Recovery Guide*," which provided a planning tool for the private sector to draft their own pandemic planning documents. DHS has made this document available at http://www.ready.gov/business/_downloads/pandemic_influenza.pdf.

Hurricane preparedness activities focused on regional coordination and preparation. Many reflected on the 'lessons learned' from Hurricane Katrina reports at stakeholder meetings and exercises held in targeted areas. DHS officials thought it was important to strategize with the private sector to address the problems identified in the 2005 hurricane season. Information was sent out by DHS on evacuation and reentry plans and routes and the status of services, to include roadways, to help industry representatives make appropriate determinations for business operations. DHS recently engaged stakeholders in government and the private sector to review the National Response Plan (NRP) and the National Incident Management System (NIMS). Efforts are underway now and will continue in 2007 to engage the private sector to address support to critical infrastructure during the restoration of essential services. ❖

Florida District Court does not allow pat-down searches at Tampa Bay Buccaneers home games

Colleen Hardy, Senior Research Associate, CIP Program

Commercial facilities are an important part of critical infrastructure in the United States. Shopping malls, concert halls, and stadiums are all considered commercial facilities. Commercial facilities have received much attention since the terrorist attacks on September 11, 2001. For example, security frisks or pat downs are required at almost all National Football League (NFL) stadiums. These pat downs are performed for a variety of security reasons, including checking for IEDs (improvised explosive devices). Gordon Johnston, a high school teacher and ordained minister, sued Tampa Sports Authority (TSA), and their Executive Director, Henry G. Saavedra, claiming that the pat downs conducted at Raymond James Stadium violate his Constitutional right to be free from "unreasonable searches and seizures…"[1] Tampa Sports Authority owns and operates Raymond James Stadium where the Tampa Bay Buccaneers play.

Johnston bought season tickets to the 2005-2006 National Football League Tampa Bay Buccaneer games. He was notified shortly before the first home game that Tampa Sports Authority implemented a new pat down procedure which required all patrons to be patted down before entering the stadium. The pat downs would be performed by a private security company hired by the TSA.

Johnston, with the help of the American Civil Liberties Union of Florida, filed an injunction in the Circuit Court of Hillsborough County, Florida. Johnston asked the court to enjoin TSA from performing the pat downs. Johnston argued that TSA's new pat down policy violates his constitutional right to be protected from unreasonable and intrusive searches. According to the ACLU, Johnston stated, "Football fans should not be forced to surrender our constitutional rights as the price of admission to the stadium." Rebecca Harrison Steele, the ACLU's West Florida Regional Director and an attorney involved in the case, stated on the ACLU's website, "There are far more effective ways to protect the security of football fans than sacrificing the constitutional freedom to be free from a pat-down search without probable cause or even any individualized suspicion."

TSA argued, among other things, that the limited pat downs do not violate the 4th amendment rights because Johnston knew the pat down was a prerequisite to entering the stadium and therefore he consented to the search by attending multiple games. The pat downs are also constitutional because the searches complied with the Supreme Court's special needs doctrine for reasonable suspicionless searches. TSA cited a U.S. Supreme Court case that held, "a search unsupported by probable cause may be reasonable when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[2] TSA argues they met the special needs requirement because Congress recognized NFL stadiums as a potential terrorist target and because Buccaneer games draw huge crowds and are highly publicized, therefore they are a very attractive target.

The Circuit Court granted Johnston's injunction prohibiting pat down searches. TSA removed the case to federal court, asserting federal question jurisdiction. The United States District Court for the Middle District of Florida, Tampa Division, denied TSA's motion to reconsider, vacate and dissolve Johnston's injunction. The District Court held that TSA did not meet the requirement for the special needs doctrine and that the pat down searches violated Johnston's constitutional rights. The District Court ruled that the TSA did not meet the special needs requirement because TSA failed to prove a substantial and real risk of a terrorist attack at their stadium. Additionally, they held Johnston did not consent to the search because he was not notified of the searches before he purchased his season tickets. The court emphasized that because Johnston would lose the value of his tickets, parking and deposit if he did not attend the

(Continued on Page 16)

Cyber Tempest *(Continued from Page 12)*
tions have to consider obligations and consequences of reporting to regulators and law enforcement, but information sharing with ISACs carried different implications depending on the sector. One ISAC operated so that the institutions could share information on new and ongoing incidents (helping to identify patterns of behavior / problems), but another ISAC operated so that the member institutions only reported incidents after they were resolved.

The exercise showed that of the four groups, the Government group was the first to ask "Who is doing this? Why? What will they do next?" While all the groups were actively involved in containing and mitigating the problems, the Government group showed early leadership and creative thinking regarding prediction of future events, expending resources to ask (if not answer) these questions. In the second day of the exercise, as the escalating events highlighted various interrelationships and interdependencies, the private and public sectors responded with an excellent level of information sharing, both volunteering and requesting information.

Cyber Tempest also provided opportunity for both public and private sector participants to understand just how quickly a regional problem could outstrip the coordination and analysis resources of law enforcement. Similarly, the law enforcement participants observed the different industries' thresholds and concerns for involving law enforcement when the institutions may need to rebuild their networks on a priority basis. As one law enforcement participant said, the exercise provided "excellent insight into the critical thinking and decision-making that occur in businesses before law enforcement gets involved." This understanding helps the state police to respond better to business concerns.

As a regional exercise, Cyber Tempest caused the participants to examine the prioritization and allocation of resources. Some Disaster Recovery (DR) and Business Continuity plans were serviced on a "first come, first served" basis. Some DR facilities may have faced the same vulnerabilities as the main network / systems, since the DR centers used the same (flawed) software or connected back to the same (infected) network.

Some of the participants noted that when it comes to cyber events, a regional response may not be practical. For example, once an event is beyond the control of a financial or telecommunications institution, it likely will require a national response (e.g., failure of the frame relay, the need to provide and disperse cash after the ATMs and regional financial facilities went down, etc.).

However, this regional exercise did result in questions that were new to some of the participants. For example, who coordinates prioritization of restoration in a region? Each state government would have its own plan, but if an event is regional (yet not national), should there be a regional restoration plan?

As the Control Group announced at the end of Cyber Tempest, the "bad guys" were two hacker groups who were competing with each other to gain prestige in the black market economy. The goals were to remain below the level of a cyber Incident of National Significance and to keep their identities secret, and the group with the most money "won." As the Control Group leader explained, "it was about money, not about killing people." The hacker groups had begun their assault six months earlier, by buying insiders at various institutions; however, as the game progressed, the cyber incidents got out of the hackers' control.

As explained by Glenn Fiedelholtz, Deputy Director of Exercises, NCSD, "Cyber Tempest was a unique cyber exercise in that it was one of the first Northeastern regional exercises in the United States, which tested the information sharing and communication path capacities of the public and private *(Continued on Page 16)*

A member of the Utility Group reporting to all participants during an outbrief.

Cyber Tempest *(Continued from Page 15)*
sectors -- IT, communications, utilities, finance / banking, health, and government -- to respond to a cyber event. Additionally, the exercise examined interdependent responses and their cascading effects within and across sectors."

Although the gaming aspect of Cyber Tempest is complete, the exercise itself is not yet over. The New York CSCIC expects to have a Cyber Tempest after-action report out to all participants before the end of December. Then, during the month of January, CSCIC will organize several conference calls among designated leads in each participating group, to analyze the report and discuss actionable items. Finally, these designated leads will meet in February, at the GMU Law School, to finalize action items and recommendations that will be distributed to all participants. Where possible, the CIP Program will share additional results and information via *The CIP Report* and our website.

A more detailed version of this article is available at: http://cipp.gmu.edu/research/CyberTempest.php ❖

R&D Trends *(Continued from Page 7)*
dence of solutions is similar. While the issues listed here amount to a daunting number of tasks, the fact that multiple efforts are underway to address them should be seen as a positive redundancy, rather than an unnecessary duplication. Once the R&D solutions become clearer, a consolidation is likely that will make adoption and implementation more streamlined. ❖

Legal Insights *(Continued from Page 9)*
cal concerns can be removed from the equation. Again, the threshold a situation must cross to invoke the use of the military remains at the same high level, only now the underlying reasons for attaining that level are more diverse and perhaps more reflective of present day realities. ❖

Johnston vs. TSA *(Continued from Page 14)*
game, his consent was not free from constraint. On November 17, 2006, TSA appealed to the United States Court of Appeals for the Eleventh Circuit. At present, the parties are waiting to be heard during their oral arguments. ❖

[1] U.S. CONST. amend IV
[2] *Board of Educ. Of Indep. School Dist. No. 92 of Pottawatomie City v. Earls*, 536 U.S. 822 (2002)

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