The Critical Infrastructure Protection Program May 2005 / Volume 3, No. 10

THE CIP REPORT

CIP Research and Development

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Research and Development (R&D) has long been a strength of colleges and universities, providing new knowledge directed toward the creation of new materials, products, and processes to speed and enhance our ability to harden and protect our critical infrastructures. HSPD-7 required a national critical infrastructure protection research and development plan to address key areas of science, engineering and technology to prevent and minimize the impact of future attacks on critical infrastructure. This plan, released in April of 2005, is outlined in this issue of *The CIP Report*. Charged with this mandate, DHS has partnered with universities, industry and government agencies to further develop and demonstrate new ideas and technologies through the Homeland Security Advanced Research Projects Agency (HSARPA).

These partnerships have yielded considerable results and have strengthened US leadership in science and technology. In addition to creating numerous undergraduate and graduate scholarships and fellowships, four Centers of Excellence have been created to focus on risk and economic analysis of terrorist events (University of Southern California), the study of terrorism and response to terrorism (University of Maryland), food protection and defense (University of Minnesota), and foreign animal and zoonotic disease defense (Texas A&M University). These Centers represent integrated networks of universities involved in interdisciplinary research activities that result in innovative educational programs for critical Homeland Security missions. The National Science Foundation is also funding critical research at universities through its Cyber Trust program.

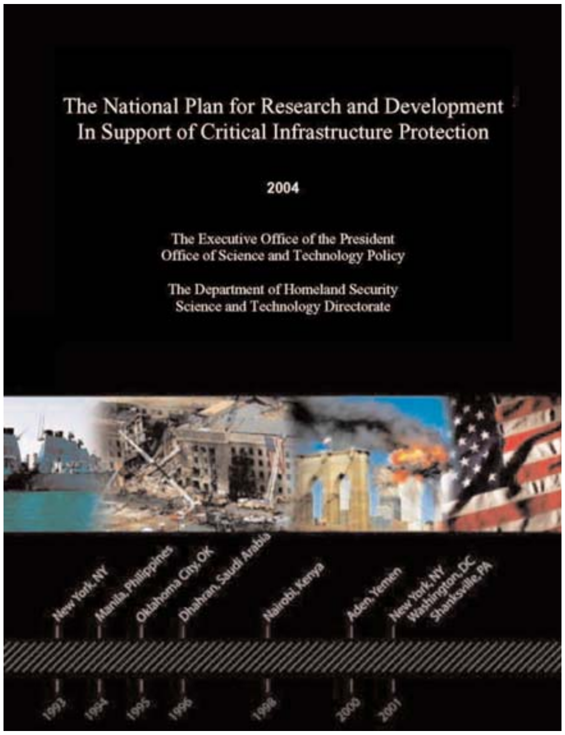
In this month's issue, we are very pleased to include contributions from Touchstone Consulting on R&D in the field of critical infrastructure protection. Touchstone supports the portfolio management for CIP in the Science and Technology Directorate within the Department of Homeland Security, and has provided a number of articles that examine the National CIP R&D Plan, priorities within CIP R&D workshops, and stakeholder integration. In addition to the contributions from Touchstone, we highlight important work being done in government, academia and the private sector. Finally, we have featured abstracts from a number of CIP Program researchers that were selected to present at the April 2005 DHS R&D Conference in Boston, and an overview of the conference proceedings.

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

National CIP R&D Plan

Kisha D. Salters
Touchstone Consulting Group, Inc.

Since Presidential Decision Directive 63, the United States has become more aware of its critical infrastructure dependencies and has made efforts to examine the vulnerabilities that make them susceptible to terrorist attacks. In an effort to re-energize critical infrastructure protection following September 11, 2001, the Executive Branch, under George W. Bush, released Presidential Directive 7 (HSPD 7): Critical Infrastructure Identification (CIP), Prioritization, and Protection in December 2003 to outline a national framework for protecting critical infrastructures. Attacks on any of our critical infrastructures have the potential to cause damage to businesses, government activities, systems, human life, and the economy. However, stating broadly that seventeen infrastructures need to be protected is vague and unlikely to lead to progress. What was needed was a way of organizing R&D and evaluating protective strategies to maximize return on the protective investment dollar. Importantly, HSPD-7 included the following stipulation: On a yearly basis the Secretary of DHS, in coordination with the Director of the Office of Science and Technology Policy (OSTP), will prepare a federal research and development plan in support of the HSPD-7 directive, also known as the annual National CIP R&D Plan.



The National Plan for Research and Development
In Support of Critical Infrastructure Protection

2004

The Executive Office of the President
Office of Science and Technology Policy

The Department of Homeland Security
Science and Technology Directorate

On April 8, 2005, the Department of Homeland Security released the 2004 National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan. The 2004 NCIP R&D Plan blazed the trail for what will become an annual assessment of National CIP R&D requirements and the federal government's efforts to address these requirements - also incorporating perspectives gathered about R&D requirements efforts underway among the private sector owners and operators of critical infrastructure. The responsibility for leading the preparation of this interagency plan was shared between DHS and the White House Office of Science and Technology Policy. The OSTP National Science and Technology Council's Infrastructure Sub-Committee (ISC) provided the interagency forum for preparing the NCIP R&D plan, gathering Subject Matter Expert (SME) recommendations, and reviewing the results.

The federal government will use the initial 2004 NCIP R&D Plan as a baseline from which to develop future year plans and to understand how these allocations of federal R&D resources support CIP work. Efforts carried out that support this NCIP R&D Plan will help the country build towards the strategic goal of a more resilient state for our critical infrastructure systems.

The 2004 NCIP R&D Plan offers an unusual convergent approach to pursuing a research and development roadmap for critical infrastructure protection and takes an in-depth look at long-term strategic direction, cross cutting themes, and existing research efforts. Incorporating priorities from multiple sectors, the plan adopts a theme-based, rather than a sector-based, approach to R&D. The nine critical infrastructure plan themes are on the following page.

The identified themes were selected as a result of their repeated appearance *(Continued, Page 17)*

Critical Infrastructure Protection R&D Plan Themes

Theme 1: Detection and Sensor Systems

- Intrusion
- Small Arms
- Explosives
- Intent
- Humans (Actors and Victims)
- Intelligent Sensor Systems
- Assessment and Response to an Event

Theme 2: Protection and Prevention

- Intrusion
- Blast
- Debris and Fragments
- Projectiles
- Fire
- Electromagnetic, Laser, and Particle Beam Weapons
- Disruption and Denial of Service/Access
- Small Arms
- Gaseous and Aerosol Plumes
- Exfiltration of, Tampering with, the Destruction of, or the Monitoring of Data
- Water

Theme 3: Entry and Access Portals

- Identification
- Authentication
- Authorization
- Access Control
- Tracking
- Dynamic Situational Control

Theme 4: Insider Threats

- Intent
- Detection and Monitoring
- Protection and Prevention

Theme 5: Analysis and Decision Support Systems

- Risk Analysis for Prioritizing CIP Investments
- Threat Evaluation
- Vulnerability / Performance Evaluation and Design of Upgrades
- Forensic Analysis and Reconstruction
- Consequence Analysis and Modeling of Interconnected CI Sectors
- Integrated Systems Modeling

Theme 6: Response, Recovery, and Reconstitution

- Response - Saving Lives, Property, and CI Capabilities
- Recovery - Temporary Restoration of Services
- Reconstitution - Permanent Restoration Techniques

Theme 7: New and Emerging Threats and Vulnerabilities

- Anticipate and discover the formulation of threats that exploit existing technologies in innovative ways
- Anticipate and discover the formulation of threats that exploit new technologies while they are in the making or at least before they mature to a state where they can be reliably delivered by our enemies

Theme 8: Advanced infrastructure architectures and systems design

- Re-examination of Fundamental Theory behind Systems
- Legacy Systems Design and Architecture
- System Design Concepts for Next-Generation Critical Infrastructure
- Auto-Responsive and Self-Healing Systems
- Flexible, Robust, and High-Confidence Critical Infrastructure
- Platforms, Standards and Technology Layers

Theme 9: Human and Social Issues

- Communication and Cooperation among Government and Private Sectors
- User-Centered Designs
- Resiliency of Commercial Enterprises and the Economy Related to Infrastructure
- Risk Communication and Management

Working Together: Research & Development Partnerships in Homeland Security

Dr. Rafal Kicinger, CIP Program Post Doctoral Fellow
Department of Civil, Environmental, and Infrastructure Engineering, GMU

From April 26 to April 28, 2005, the Department of Homeland Security hosted its inaugural research and development conference in Boston, MA, which attracted more than 900 researchers and policy makers from the US and abroad. The focus of the conference was on state-of-the-art methods, models, and tools to anticipate, prevent, respond to, and recover from high-consequence chemical, biological, radiological, nuclear, explosives and cyber terrorist threats. The technical sessions were divided into four major topic areas:

- Awareness
- Countermeasures: biological, chemical, radiological and nuclear explosives
- Threat and vulnerability assessment
- Critical infrastructure protection and cyber security

The technical sessions were accompanied by four poster sessions organized around the same topic areas. Research on homeland security by George Mason University and James Madison University was presented during six poster presentations on critical infrastructure protection.

Security of Transportation Systems: An Evolutionary Approach

Dr. Tomasz Arciszewski, George Mason University, presents his work during the poster session on critical infrastructure protection.

One of the distinguishing features of this conference was its interdisciplinary character. A broad range of problems addressed by homeland security research brought together researchers representing almost the entire spectrum of scientific disciplines. The technical sessions provided an excellent overview of the state-of-the-art in homeland security related research from different perspectives.

Dr. Sanjay Jain, National Institute of Standards and Technology, presents his research on "Integrated Modeling and Simulation for Multiple Phases of Emergency Response."

The conference provided exceptional opportunities for meeting researchers working in different fields on similar problems and the dissemination of scientific ideas. It also encouraged establishment of partnerships among scientists and engineers from government, national laboratories, universities, and private sector firms.❖

More information about the conference can be found at http://www.homelandsecurityresearchconference.org.

Beginning on Page 5, you can find abstracts of research presented at the Boston conference by CIP Program researchers.

CIP Program Researchers Present at Department of Homeland Security R&D Conference

The following abstracts are from projects selected for presentations and poster sessions at the April 26 - 28 DHS Research and Development Conference in Boston, MA.

A Vulnerability Assessment Methodology for Critical Infrastructure Facilities

George H. Baker III, Ph.D., James Madison University

Highly efficient, complex, and interdependent infrastructure systems including electric power, telecommunications, transportation, water utilities, food distribution, housing and shelter, public health, finance and banking are foundations of modern societies. Over the last 3 years, the United States has become acutely aware of the importance of civil infrastructures and their criticality to the nation's economy and quality of life. Our reliance on these systems makes them especially attractive targets for attack. To understand and correct exploitable susceptibilities of critical infrastructure facilities, infrastructure providers and regional planners need a common, repeatable, systematic methodology to understand the comparative risks and vulnerabilities and determine where to invest scarce resources.

This paper proposes and describes a common vulnerability assessment methodology for individual critical infrastructure facilities. It briefly discusses the integration of critical facility results into a regional-scale assessment. The methodology is designed to be comprehensive in terms of accommodating physical and cyber threats against the complete suite of mission-critical systems making up a facility. While the emphasis is on vulnerability assessment, the results provide many of the essential ingredients of a risk assessment. The methodology is applicable for self-assessment by infrastructure service providers or for use by external assessment teams.

Decision Support Systems for Local EMS
The Poison Next Door: Preparedness, Planning, and Response to Hazardous Chemical Accidents and Terrorism

Michael L. Deaton, Steven P. Frysinger, Mark A. Kirk, and Charles Werner
James Madison University

Chemicals stored and transported in a community provide ready-made terrorist weapons and pose a significant threat to critical infrastructures. While information on chemical inventories and toxicities exists in various forms, local communities lack a decision support environment that integrates this information into a comprehensive view of the risks posed by the chemicals in each locality. Such a view is necessary for local industry, government and health professionals to evaluate their readiness to respond to catastrophic chemical releases. This paper describes a prototype decision support system under development through a partnership between the University Of Virginia School of Medicine, James Madison University, and the Charlottesville, VA Fire Department. This DSS is designed to facilitate hazardous chemical vulnerability assessment and real-time incident management at the local level, and it provides an integrated tool set that can be adapted to any community (rural or urban) and expanded to a regional or even national scale. The system incorporates a chemical inventory, toxicity information, EMS readiness data, population data, risk assessment models, and air dispersion models. These elements are incorporated into a geographic information system and joined with expert guidance on medical response in the event of a chemical release. Emergency response planners, police, and health care providers can use the system to evaluate community preparedness in response to catastrophic spills or releases, thereby guiding training and resource priorities. The presentation describes the system and the practical issues that are addressed during a pilot deployment within the EMS in Charlottesville, Virginia.

(Continued, Page 6)

Boston R&D Conference *(Cont. from Page 5)*

A Data Model and Architecture for Critical Infrastructure Protection

Anoop Singhal and Sushil Jajodia
Center for Secure Information Systems
George Mason University

Vulnerability Assessment (VA) of modern systems that contain interdependencies among critical infrastructures such as buildings, telecom/cyber networks, information and software systems is a challenging task. In this paper we present a data model and software architecture of a system to evaluate existing VA frameworks and recommend how they can be improved to do vulnerability assessment of modern complex systems. A flexible data model and a relational database was used to store information about the existing open source vulnerability assessment frameworks and the current state of practice in government agencies and private industries. Database sorting and searching techniques were used to analyze this information and to make policy recommendations to improve the VA of critical infrastructures.

A data model was created in Unified Modeling Language (UML) and XML to capture the information about the categories, sub-categories, questions and methodology in thirty different VA procedures, processes and tools. This data model was used to create a database schema with sorting/searching capability in ORACLE Relational Database System. A GUI was designed using JAVA/HTML to query and analyze this data. Some sample queries are:

a. Give all questions for a certain category (e.g. building envelope)
b. Give all questions pertaining to a pattern such as "passwords" or "encryption"
c. Export the results of the query to a file.
d. Given a source document, give all the categories and sub-categories that are contained in that document.

Our software architecture and the flexible data model were useful to compare and contrast different VA methodologies and make recommendations on how to improve them. This system was developed to help identify infrastructure interdependencies in the National Capital Region as part of the NCR/CIPP project.

Methodology and Description of High Consequence Event Decision Matrix

Joshua Barnes
James Madison University

After a review of literature and existing terrorism response plans, it was discovered that such plans are very lengthy. This is a concern, as in the midst of a weapon of mass destruction (WMD) incident, all responders must be keenly aware of the master plan. A response without this awareness would become catastrophic if different response groups lacked a clear vision of the divisions of duties and responsibilities. It is unlikely that all first responders will have a working knowledge of the lengthy response plans; a situation could arise where the response becomes disjointed and haphazard. To mitigate a potentially catastrophic inefficiency, a High Consequence Event Decision Matrix was created to classify the CBRNE+I (incendiary) WMD incidences at different severity levels. Once classified, the necessary emergency actions first responders must employ are also detailed. The High Consequence Event Decision Matrix is comprised of four components, when combined creates a tool that: classifies each WMD by category and severity, indicates the essential emergency actions that must be employed to sufficiently address the type and severity of the event, indicates the protective actions that are suggested for the public in the affected areas for each WMD at each severity level, and a matrix detailing how some historical events would be classified. Once distributed and widely used, the Decision Matrix will put all responding parties on "the same page." The Decision Matrix is designed to be implemented in a complementary manner through the National Incident Management

(Continued, Page 7)

Boston R&D Conference *(Cont. from Page 6)*

Critical Infrastructure Protection

Professor Tomasz Arciszewski and Dr. Rafal Kicinger
Department of Civil, Environmental, and Infrastructure Engineering,
George Mason University

Prof. Arciszewski and Dr. Kicinger presented 3 posters of ongoing research on various aspects of critical infrastructure protection. The first poster, called "Proactive Infrastructure Security: From Evolutionary Approaches to the Use of Cellular Automata," provided an overview of research activities conducted by a team of researchers in the CEIE Department at GMU. It discussed several novel approaches to security of complex infrastructure systems (based on evolutionary, co-evolutionary, and cellular automata models), which were utilized in the development of a class of computer tools for infrastructure protection. The poster also presented various computer tools for evolutionary and co-evolutionary generation of terrorist and security scenarios developed at George Mason University for infrastructure protection.

The second poster, "Security of Transportation Systems: An Evolutionary Approach," reported preliminary results on using evolutionary models to determine the most vulnerable points of a transportation system. This work was conducted by Zbigniew Skolicki, Professor Mohan Venigalla, and Professor Tomasz Arciszewski. Evolutionary models were applied in the specific context of the National Highway Planning Network inside Washington, DC. It considered approximately 300 links, 210 miles, and about 20 external & 10 internal zones. In the course of this research a Route Optimization Model for Evolutionary Networks (ROMEN) has been developed and evolutionary tools working with ROMEN allowed the evolution of terrorist attacks and identification of corresponding countermeasures.

The third poster, "Improving the Security of Water Distribution Systems using a Co-evolutionary Approach," presented advanced co-evolutionary approaches to determine strategies for protecting water distribution systems from contamination attacks. This research was conducted by Zbigniew Skolicki, Professors Mark Houck and Tomasz Arciszewski. A hypothetical water distribution network was selected as a representative for a typical community of 10,000-20,000 people. It provided a realistic network configuration covering the area of about 4 square miles and production of 2-3 million gallons of water per day. Co-evolutionary tools were combined with a state-of-the-art water simulation system called EPANet to allow the evolution of terrorist attacks and defense strategies. The obtained results provided interesting insights into the existing vulnerabilities of the water distribution system as well as best mitigation strategies.

LEGAL INSIGHTS

Stakeholder Integration and the Future of CIP R&D

Guest Columnist Emily Frye
Touchstone Consulting Group, Inc.

The team of scientists, managers, and writers who constructed the first National CIP R&D Plan deserves praise and thanks from the CIP community and the nation. The Plan maps out the elements of a solution to an incredibly complex problem - as Justice Lewis Brandeis once remarked, a problem where "the private interest is affected with the public good." The problem of protecting critical infrastructures spans sectors, multiple levels of government, public and private ownership, and many tiers of technology.

The 2004 NCIP R&D Plan, however, is not the final word. Instead, it is an invitation to the R&D community - writ large - to engage in an ongoing dialogue about at least two serious issues:

- First, how can we improve the 2004 NCIP R&D Plan?
- Second, what can we do right now to deploy the R&D community's existing work for a hardened infrastructure?

The Plan could and should lead to dialogue on any number of other issues. But these two questions are broad and hard enough that the research community could examine them all year without finding a complete answer.

How, then, might we at least begin to address them? The key is this: integration. More specifically, stakeholder integration in the nation's CIP R&D dialogue. Several possible approaches might lead to increased knowledge management for purposes of the National Plan. The one that the Plan's developers have chosen is to identify stakeholders and ask for their input.

So who are the stakeholders?

Stakeholders, for purposes of the National CIP R&D Plan, are members of identifiable - although not necessarily cohesive - communities that currently rely or that imminently will rely on CIP in order to function. For simplicity's sake, we might say that there are four sets of stakeholders:

- Federal
- Academic and national lab
- Industry
- International

Defined in this way, the stakeholder groups clearly include an enormous number of potential participants in the process. The key is to develop, over time, links into the individuals within those groups who have an interest in and aptitude in Critical Infrastructure Protection R&D.

One of the most important steps taken over the past year by the DHS CIP team is reaching out to existing communities that already have a foothold in one or more of these stakeholder groups. The CIP Program at George Mason University (GMU), for example, brings together a large number of researchers and industry personnel who are interested in, and knowledgeable about, Critical Infrastructure issues. When The CIP Program generously offered space in this issue of The CIP Report to publicize the 2004 NCIP R&D Plan, it was a way to reach a large number of relevant people with news that would help build the stakeholder community and provide channels for ongoing communication among those participating in the community.

In coming years, it is hoped that the proliferation of knowledgeable individuals and communities will all coalesce in shared information pools that lead to an ever-better Plan ... and an ever-safer Nation.

The opinions in this article represent those of the author and not those of any governmental entity or representative. ❖

Two New Business Roundtable CEO Guides Offer Strategic Guidance on Risk Management and Crisis Preparedness

Washington, DC - Business Roundtable, an association of 160 CEOs of leading U.S. companies, has developed and released two comprehensive guides to assist CEOs and other corporate managers in strengthening homeland security by improving the private sector's preparedness for infrastructure disruptions, natural disasters and terrorist attacks.

Committed to Protecting America: CEO Guide to Security Challenges is a first-ever compilation of best management practices and key security lessons learned by CEOs who are facing new and evolving security threats. The second document, *Committed to Protecting America: A Private Sector Crisis Preparedness Guide*, offers smart practices and planning checklists essential for crisis management, including employee communication, evacuation and business continuity.

Preparing for threats and attacks at a time of finite resources requires companies to make choices, and the Roundtable's guides can serve as a roadmap for companies to assess risk, evaluate their plans and take appropriate actions. Both documents are available free of charge through the Roundtable's website, www.businessroundtable.org.

In releasing the guides on May 3, the Roundtable urged every CEO to take a lead role in demonstrating the importance of security preparedness within their companies.

"The security challenges in the post-9/11 era require new thinking and new approaches that go far beyond traditional physical security models," said Frederick W. Smith, Chairman, President and Chief Executive Officer of FedEx Corporation and Chairman of the Roundtable's Security Task Force. "Companies need to embed security in all aspects of their business processes and operations.

"Just as the federal government is reforming its procedures and testing its security preparedness through exercises such as TOPOFF 3, businesses must revise corporate governance practices and evaluate their crisis plans to address important security issues in this new world," Smith said. "CEO leadership is critical, because only CEOs can establish the necessary tone and ensure that vital security needs are met across departments and throughout operations over the long term."

Homeland Security Secretary Michael Chertoff, in a comment about the Roundtable security guides, said: "Our recent TOPOFF 3 exercise demonstrated the importance of being prepared and *(Continued, Page 17)*

Committed to Protecting America: A Private Sector Crisis Preparedness Guide *Summary of Key Recommendations*

CEO Role: Critical to Disaster Response and Recovery

- Be involved in crisis preparedness and response processes
- Endorse the importance of preparedness to set expectations and send clear signal to all stakeholders
- Demonstrate readiness to immediately serve as spokesman to public, employees, customers and community in the event of a crisis

Employee Communications: Keep Company and Employees Informed

- Establish an Employee Emergency Communications Task Force
- Train employees on crisis plans and procedures
- Remind employees of the importance of crisis readiness through posters, notices, meetings
- Distribute local and national emergency readiness materials to employees
- Set up a system to locate staff in an emergency, including those traveling internationally
- Disseminate information about a crisis to employees at all company locations

Evacuations and Incident Response: Ensure Employee Safety

- Conduct drills to test evacuation plans, and do post-drill debriefings to assess ways to improve
- Include evacuation and crisis training as part of orientation for new hires
- Account for contractors and visitors in evacuations
- Update plans by applying lessons from government exercises or other crises *(Continued, Page 17)*

Centering the Tornado: Gathering Priorities & Focus from Content Workshops

Kisha D. Salters
Touchstone Consulting Group, Inc.

It is more important than ever that national resources are deployed wisely to protect critical infrastructures. The Critical Infrastructure Protection R&D team at the Department of Homeland Security has worked to understand the ongoing CIP projects and priorities of the federal government, industry, and R&D provider groups (including academe). One of the most effective ways they do this is by convening interactive stakeholder-specific workshops. These workshops have encouraged information sharing across sectors and enabled the federal government to communicate the work that has been done to develop the baseline 2004 National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan.

Federal R&D Stakeholders

The first workshop was held on December 16, 2004. The participants were Federal Program Managers. The workshop attendees represented over 110 research leaders from approximately 30 agencies within the federal government. The purpose of the meeting was to align government leaders with a shared understanding of the scope, purpose, approach, and coordinated actions focusing on R&D to secure critical infrastructures. During the meeting, R&D professionals discussed their CIP priorities and how they compared to the ones outlined in the 2004 NCIP R&D plan developed by the National Science and Technology Council (NSTC) Infrastructure Subcommittee. The networking opportunities enabled the individuals to begin valuable conversations that extended far beyond the one-day workshop. The follow up Federal Program Managers workshop was held on May 19, 2005 to resume the work began in December and discuss the progress made over the last five months.

Industry R&D Providers and Users

The CIP R&D Industry workshop was called by the Partnership for Critical Infrastructure Security, Inc. and hosted by George Mason University's Private Sector Programs Division on April 14, 2005. The workshop attendees included 45 industry R&D leaders and users from 11 critical infrastructure sectors. The purpose of the meeting was to discuss current research and development, gaps in R&D, and priorities for R&D in the area of homeland security from the critical infrastructure owner-operator perspective. While all of the critical infrastructure sectors were not represented during the meeting, the workshop was a valuable first step. Interestingly, workshop participants were perhaps most interested in the session that provided information about the 2004 NCIP R&D Plan, as well as what other organizations were doing in the areas of research and development.

Academic and Federal Lab CIP R&D Providers

The third inaugural workshop will be held for Academic and Federal Lab CIP R&D Providers in the near future. During the Academic and Federal Lab R&D Provider workshop, participants will discuss CIP R&D strategies and priorities to protect critical infrastructure. The academic and federal lab researchers will have an opportunity to learn about and critique the Plan. These individuals will also help to shape the government's understanding of ongoing and planned R&D that addresses the needs identified in the Plan. Like the participants from the two previous workshops, it is hoped that the research community will discover that one of the best outcomes is interacting with other people who care about and work on complementary issues.

The workshops are an ongoing effort and commitment by the NSTC Infrastructure Subcommittee to gather feedback from R&D professionals and understand the initiatives that are being developed to protect the nation's critical infrastructures. The Infrastructure Subcommittee will continue to integrate the stakeholder community as it develops the 2005 and 2006 plans because it is dedicated to understanding what the federal government can do to support R&D professionals in their work to protect the nation [See: "Stakeholder Integration & the Future of

(Continued, Page 11)

Cybersecurity R&D Act of 2002

Randy Jackson, CIP Program

Administration budgets have not taken advantage of funding opportunities presented by the Cybersecurity Research and Development Act of 2002 (P.L. 107-305).

The Cybersecurity R&D Act (the Act) became P.L. 107-305 when it was signed by President Bush in November of 2002, authorizing appropriations for the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST). The goal was to facilitate increased R&D for computer network security and to support research fellowships and training. The total funding authorized over a five year period was $902.15 million.

However, in the current FY 2005, although $128.25 million had been allocated to NSF, and $61.4 million was allocated to NIST, the Administration's budget request was for only $76 million for NSF R&D and $18.5 million for NIST. Each of these did constitute an increase over the FY 2004 budget request (19% and 48% respectively); however, such funding is clearly well below the level targeted by P.L. 107-305. The low levels are a continuation of similarly low levels of NSF and NIST R&D budget requests made in FY 2003 and FY 2004.

For FY 2006, funding requests have remained fairly constant, continuing to forego R&D funding opportunities presented by the Cybersecurity R&D Act. The NSF request for FY 2006 is $67.5 million, a 2% increase over FY 2005 for cybersecurity R&D, but shows a 27% decrease to $12 million for education programs. This equates to a total request of $79.5 million out of a possible $134.35 million allocated through the Act. Finally, for NIST in FY 2006, $19 million has been requested, the same as that of FY 2005. This was considerably less than the $61.4 million allocated by the Act for FY 2005 and even further below the $76.6 million allocated for FY 2006.

The last year for which P.L. 107-305 targets spending is FY 2007. Levels are $142.25 million for NSF and $91.8 million for NIST. Based on the track record over the life of the Act, it seems unlikely that anything near that level of spending will emerge. Certainly in an age of tight budgets and fiscal worries, spending must be carefully scrutinized and vetted before allocation. However, investment in cybersecurity R&D will play a crucial role in strengthening the US cybersecurity infrastructure thereby supporting the myriad ways in which infrastructure facilitates the functioning of the economy. Furthermore, dollars spent now on R&D will mean even more dollars saved at a later date when cyber incidents and attacks are intercepted and blocked without causing disruption to the system. ❖

Content Workshops *(Cont. from Page 10)* CIP R&D", also in this issue]. The workshops provide an opportunity for individuals from all sectors to initiate conversations with each other to expand their knowledge base and fill data gaps. The goal is for these conversations to develop into meaningful, cross-institutional partnerships that produce valuable critical infrastructure protection strategies. These partnerships will help to maximize CIP resources, build upon existing knowledge, and move the nation forward in the fight against terrorism. ❖

R&D at DHS Centers of Excellence

The Homeland Security Centers of Excellence were established to engage the academic community in efforts to secure the nation. Under the Department of Homeland Security's Science and Technology Directorate, the Centers of Excellence program is launching an integrated network of university-based centers to carry out multi-disciplinary research and establish innovative educational programs for critical Homeland Security missions. The DHS Centers of Excellence research areas that influence the multidisciplinary capabilities of universities. The Department of Homeland Security and these collaborator universities have united the nation's most talented researchers from areas that include agricultural, chemical, biological, nuclear and radiological, explosive and cyber terrorism, as well as terrorism from a social and behavioral perspective. The Centers complement other programs within the Department of Homeland Security, connect with the Department of Energy laboratories and DHS laboratories that contribute to the DHS S&T mission, work with Federal, state and local DHS government partners, and engage private industry in their research and education activities.

Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California is evaluating the risks, costs and consequences of terrorism, to guide economically viable investments in countermeasures that will make our nation safer and more secure. They are focused on developing risk assessment and modeling capabilities that cut across general threats and targets, in application areas such as biological threats, transportation and funding allocation formulas. Additionally, the Center for Risk and Economic Analysis will develop tools for planning responses to emergencies, to minimize the threat to human lives and reduce economic impacts of terrorist attacks. Major partners with USC include the University of Wisconsin at Madison, New York University, and Structured Decisions Corporation (affiliated with MIT).

CREATE was selected to be the first university Center of Excellence for the Department of Homeland Security after a competition among 72 universities.

Dr. Randolph Hall is the Senior Associate Dean for Research, Principal Investigator/co-Director for the Center for Risk and Economic Analysis of Terrorism Events (CREATE).

National Center for Food Protection and Defense (NCFPD) is led by the University of Minnesota in partnership with Michigan State University, North Dakota State University, University (Continued, Page 13)

There are four Centers of Excellence located throughout the United States. Each Center of Excellence is partnered with multiple universities and acts as the unifying point for these institutions. The Centers include:

- Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California
- National Center for Food Protection and Defense at the University of Minnesota
- National Center for Foreign Animal and Zoonotic Disease Defense at Texas A&M University
- National Center for the Study of Terrorism and the Response to Terrorism at the University of Maryland

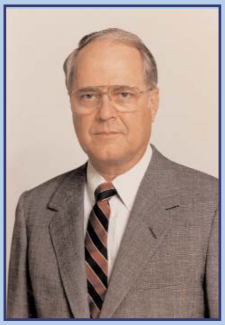
Centers of Excellence *(Cont. from Page 12)* of Wisconsin at Madison, Georgia Institute of Technology and the University of Tennessee at Knoxville, and collaborators from more than 16 other universities. NCFPD identifies vulnerable food products, addresses the vulnerable nodes in the food supply chain from pre-farm inputs through consumption, derives new instrumentation and strategies to meet the needs of rapid and multiple samplings, and assesses the public health impact of new technologies as well as terrorist influences and subsequent economic impacts. This Center addresses the need for continuous communications strategies to responsibly educate the public. Through its research and education programs, NCFPD helps develop food system professionals to protect the food supply.

Dr. Francis Busta is Principal Investigator of the National Center for Food Protection and Defense.

National Center for Foreign Animal and Zoonotic Disease Defense (FAZD) is led by Texas A&M University, in partnership with the University of Texas Medical Branch, University of California at Davis, and University of Southern California. FAZD projects embrace vaccine development, new and faster diagnostics, recovery strategies, gap analyses using models, model development, and integrating existing databases. This program is defined by five areas of work over the next three years:

- Biological Systems
- Models and Model Integration
- Information Management
- Risk Communications
- Education

In addition to direct collaboration with the Plum Island Animal Disease Center, FAZD will work closely with academia, industry and government to address potential threats to animal agriculture, including Foot and Mouth Disease, Rift Valley Fever, Avian Influenza and Brucellosis. In support of the Integrated Network concept of the DHS Centers, FAZD is also working with CREATE at the University of Southern California to develop and apply risk assessment and risk communication methods to foreign animal and zoonotic disease defense.



The principal investigator for the National Center for Zoonotic and Foreign Animal Disease Defense is **Dr. Neville Clark.**

National Center for the Study of Terrorism and the Response to Terrorism (START) is led by the University of Maryland in partnership with the University of California at Los Angeles, University of Colorado, Monterey Institute of International Studies, University of Pennsylvania, and the University of South Carolina. START will address a set of broad, challenging questions including: What moves individuals, small groups and social movements to undertake terrorism as a strategy? What are the social and psychological dynamics of terrorist groups and how are they affected by in-group competition for leadership and inter-group competition for support of terrorist sympathizers? And how can we respond more effectively to terrorist threats and increase the resiliency of our citizens to attack? Studying the phenomenon of terrorism from a social and behavioral perspective will help us interpret fragments of intelligence information and broaden our understanding of the actions taken by terrorists and terrorists groups. The behavioral and social sciences can also provide knowledge of and insights into the responses of individuals and organizations to the threat of terrorism and to terrorist events. ❖

Dr. Gary LaFree is the Director of the new National Center for the Study of Terrorism and Responses to Terrorism.

Cyber Security Research Priorities

The President's Information Technology Advisory Committee spent a year studying the IT infrastructure of the United States, and subsequently published a report to the President entitled, *Cyber Security: A Crisis of Prioritization*. As part of its findings and recommendations, the committee identified ten priority areas of paramount importance. Without significant advances in research in these areas, the Nation will not be able to secure its IT infrastructure.

Authentication Technologies. Authentication schemes for networked entities such as hardware, software, data, and users are needed for a variety of purposes, including identification, authorization, and integrity checking. These schemes must be provably secure, easy to verify, supportable for use with billions of components, and rapidly executable. Methods in traditional cryptography have focused on security but may not be efficient enough for widespread use in environments where, for example, millions of data packets per second must be authenticated by a single network router. Much useful work has been done on cryptographic protocols. But the requirement that the protocols be usable in an environment such as the Internet demands the development of new protocols.

Secure Fundamental Protocols. Few of the protocols governing the Internet's operation have adequate security. For example, to misdirect traffic to an alternate site, an attacker can easily fool (or "spoof") protocols such as the Border Gateway Protocol (BGP) (which controls the paths taken by packets as they move through the Internet); and services such as the Domain Name System (DNS) (which controls the destinations of packets). Such attackers can intercept, monitor, alter, or otherwise manipulate Internet traffic, often without detection. Secure versions of the basic protocols that address threats such as denial of service, corruption, and spoofing, must be developed if the Internet is to become a reliable medium for communication. Moreover, we need to secure basic protocols against incapacitating attacks that exploit weaknesses in the protocols themselves.

Secure Software Engineering and Software Assurance. Commercial software engineering today lacks the scientific underpinnings and rigorous controls needed to produce high-quality, secure products at acceptable cost. Commonly used software engineering practices permit dangerous errors, such as improper handling of buffer overflows, which enable hundreds of attack programs to compromise millions of computers every year. In the future, the Nation may face even more challenging problems as adversaries - both foreign and domestic - become increasingly sophisticated in their ability to insert malicious code into critical software. From avoiding basic programming errors to developing massive systems that remain secure even if portions of the system software are compromised, significant new research on secure software engineering is needed.

Holistic System Security. Effective security in a complex, many-layered, global infrastructure such as the Internet and its nodes requires more than the security of its component parts. Establishing sound methods for authentication, secure protocols for basic Web operations, and improved software engineering will undoubtedly become part of an evolving solution to this problem. But most importantly, researchers must recognize from the outset that an end-to-end architectural approach to the security of the whole necessarily transcends the security of the individual parts. For example, customers assume that their online banking transactions, based on secure socket layer (SSL), are indeed secure. But by spoofing the associated underlying protocols or end-user software, a malicious party can make a user's transaction appear secured by SSL while allowing the theft of confidential data. It is also possible to compromise the security of the end computing systems, obtaining the data even though it was secure in transit. Software usability itself is a legitimate and important research topic in cyber security. Incorrectly used software or hostile or confusing user interfaces can lead to user frustration and unauthorized workarounds that can compromise even the most robust security schemes. Research is also needed on how to make large and complex systems, where components can interact in unexpected ways, secure as a whole. Ultimately, fundamental research should address the development of entirely new, holistic security architectures including hardware, operating systems, networks, and applications.

(Continued, Page 15)

Cyber Security Research Priorities *(Cont. from Page 14)*

Monitoring and Detection. Regardless of progress made in the preceding research areas, unanticipated events will still occur. When they do, tools to monitor and understand what is happening are needed to enable the proper deployment of appropriate defensive measures. The ability of current tools that monitor irregular network activity to rapidly identify the underlying cause is primitive. The current advantage that adversaries enjoy will increase as they become more knowledgeable and as the Internet becomes larger and more complex.

Mitigation and Recovery Methodologies. Secure systems must be designed to rapidly respond to unforeseen events and attacks, and recover from any resultant damage - a particularly challenging task in a system as large and complex as the Internet and its nodes. This issue has been addressed in other systems of extraordinary complexity such as the space shuttle, where a substantial investment has been made to build in maximal reliability and redundancy. No comparable effort has been invested in developing methods to make the Internet and critical computer systems reliable in the face of attacks.

Cyber Forensics: Catching Criminals and Deterring Criminal Activities. The rapid arrest and conviction of criminals is a primary goal of law enforcement and also serves as a deterrent. When potential criminals believe there is a strong chance that they will be caught and convicted, they are more reluctant to commit crimes. Current capabilities to investigate cyber crime, identify perpetrators, gather and present evidence, and convict criminals are woefully inadequate. Compounding the problem, we do not really know how to deter cyber crime. Very few of the thousands of cyber criminals active today are being caught. There is a pressing need to develop new tools and techniques to investigate cyber crimes and prosecute criminals. Robust cyber forensic methods are also needed that will prove capable of withstanding the burden of proof in court, whether employed to prosecute criminals or exonerate the innocent.

Modeling and Testbeds for New Technologies. One of the barriers to the rapid development of new cyber security products is the paucity of realistic models and testbeds available for exercising the latest technologies in a real-world environment. Some Internet modeling research has been conducted, but it has been rudimentary and has had little impact in practice. The problem is challenging because of the Internet's scale and complexity. Additionally, existing data on the Internet's workings are limited and typically confidential. Some Federal programs have been established recently, but a significantly larger and more sophisticated effort is needed if useful models and testbeds are ever to become a reality.

Metrics, Benchmarks, and Best Practices. Some scientific fields have established universally acknowledged metrics and benchmarks to help evaluate new technologies or products. However, there has been relatively little research focused on developing metrics, benchmarks, and best practices for cyber security. Where benchmarks or certification criteria exist, they are typically antiquated, expensive, and even counter-productive to improving security. Without universally accepted cyber security metrics, separating promising developments from dead-end approaches will prove difficult. This, in turn, will significantly increase costs and delay time to market when transferring such technologies into the product cycle.

Non-Technology Issues That Can Compromise Cyber Security. A number of non-technological factors - psychological, societal, institutional, legal, and economic - can compromise cyber security in ways that network and software engineering alone cannot address. Technology deployments that fail to address these factors can aggravate problems they are intended to solve. Cyber security research that reaches beyond technology and into these other realms is needed. Research on human and organizational aspects of IT infrastructures can be used to explore solutions that factor in human behavior. ❖

For more information, visit the the National Coordination Office for Information Technology R&D (NITRD) at http://www.hpcc.gov/.

National Science Foundation's Cyber Trust Program

The National Science Foundation (NSF) has a $30 million Cyber Trust program, which includes two cybersecurity research centers that will focus on eliminating plagues of Internet worms and viruses and on building better security defenses through a deeper understanding of Internet "ecology."

"The Cyber Trust program – the centerpiece of NSF's leadership of cybersecurity research and development -- promotes research into more dependable, accountable and secure computer and network systems," said Peter Freeman, NSF assistant director for computer and information science and engineering. "We are very pleased to be able to add these activities to our growing portfolio of work in this critical area."

Mike Reiter
Director
STIM Center

The first center, led by Mike Reiter of Carnegie Mellon University will focus on "Security Through Interaction Modeling" (STIM). In the same way that ecology studies the web of life, the STIM Center will pursue fundamental understanding of the networks of interactions among humans, computers, and even cyberattacks.

The STIM Center, with anticipated funding of $6.4 million over five years, will explore ways to create more effective and usable defenses by modeling these networks of interactions and making the models an integral part of the defenses. Among its activities, the center will study healthy network interactions to see what distinguishes them from attacks; examine the network interactions of particular "species" of applications, such as e-mail or peer-to-peer networks, for clues to limiting successful attacks; and, to develop better defenses, study how cyber-attackers can combine attacks to reach their goals.

The Center for Internet Epidemiology and Defenses will be led by Stefan Savage of the University of California, San Diego (UCSD), and Vern Paxson of the International Computer Science Institute (ICSI), affiliated with UC Berkeley. The center, with expected five-year funding of $6.2 million, will be dedicated to wiping out those plagues of the Internet, worms and viruses that infect thousands upon thousands of computers and cause billions of dollars in down time, network congestion and potentially lost data.

Taking cues from the field of epidemiology, the center will work to understand how the Internet's open communications and software vulnerabilities permit worms to propagate, to devise a global-scale early warning system to detect epidemics in their early stages, to develop forensics capabilities for analyzing wide-ranging infections, and to develop techniques and devices that can suppress outbreaks before they reach pandemic proportions. "These centers, as well as our other funded activities, are looking not only for new ways to cope with imperfections in today's systems, but also for the knowledge and techniques to build better systems in the future," said Carl Landwehr, program director for Cyber Trust. "We had a number of strong proposals, indicating the depth of interest in this area by the academic research community."

Stefan Savage
Co-Director

Vern Paxson
Co-Director

Center for Internet Epidemiology

Both centers will also initiate significant efforts in education and workforce development and coordinate with ongoing outreach activities on their campuses. The centers' results will be incorporated into undergraduate and graduate courses, K-12 and college-level curricula and training programs for high-school students and faculty at traditionally minority-serving institutions.

In addition to the two centers, the Cyber Trust program will support 12 new team projects and 19 individual or small-group projects, out of nearly 400 projects proposed. ❖

BRT Security Guides *(Cont. from Page 9)* undertaking drills to test those preparations. In today's environment, active security measures are critical to businesses themselves because the cost of an attack often outweighs the cost of protection."

Businesses have an important part in preparedness and responding to a disaster, as the private sector controls 85% of the critical infrastructure in the United States - including power plants, transportation and computer networks.

The importance of enhancing private sector security preparedness was one of the 9/11 Commission's principal recommendations. The Roundtable's CEO guide compiles security lessons learned across a variety of industries - not only from the 9/11 attacks, but also from major infrastructure disruptions and natural disasters - and assembles them into the first-of-its-kind, comprehensive guide for chief executives.

"The ongoing war on terrorism requires an unprecedented and sustained commitment from the private sector, and the Roundtable is leading the way for improved business preparedness," said John J. Castellani, President of the Roundtable. "While we can never completely eliminate risk from attack or protect against every conceivable threat, we must work each day to keep our employees and our communities safe and secure." ❖

CIP R&D Plan *(Cont. from Page 2)* in the concerns of infrastructure owners, operators, industry representatives, and government officials. It was the process of recording the same themes across all infrastructure stakeholders and sectors that helped to reinforce the validity of this approach for identifying and coordinating necessary CIP R&D.

Along with developing annual Critical Infrastructure Protection Research and Development plans, the Department of Homeland Security is taking a proactive role in building relationships across federal agencies and industry sectors. The NCIP R&D Plan, for example, is explicitly intended to compliment the National Infrastructure Protection Plan rather than to forge a separate set of initiatives. This type of relationship building and integration will result in a safer nation as R&D professionals collaborate and communicate with each other to optimize CIP-related results across multiple initiatives.

To access a copy of the 2004 National Critical Infrastructure Protection plan, click **here.** ❖

BRT Private Sector Guide *(Cont. from Page 9)*

- Create an inventory of employee special skills, such as CPR, first aid or volunteer firefighting
- Encourage employees to take part in training programs for first responders
- Provide employees with "GO" bags containing flashlights and other essentials
- Prepare for shelter-in-place situations
- Discuss disaster response and evacuation plans with local governments for coordination

Business Continuity: Getting Up and Running Again

- Create a business continuity plan covering physical space, phone systems and computer systems
- Designate a business continuity coordinator
- Inform employees about business continuity plans before a crisis
- Plan for alternate locations
- Have low-tech alternatives available in the event that high-tech communications are unavailable
- Work with local communities to register in advance for access to affected sites after a crisis
- Prepare for supply chain needs
- Establish ways to communicate with a dispersed staff following a disaster or incident

Working with the Department of Homeland Security: All-Hazards, Not Just Terrorism

- Prepare a checklist to determine appropriate security actions as the threat increases, even if the color-coded threat level is not changed

For more information, visit http://www.businessroundtable.org. ❖

Cyber Security and the Law: Addressing Compliance, Complexity, and Confusion

The Cyber Security Industry Alliance and The Critical Infrastructure Protection Program at George Mason University School of Law present a three-part symposium on the emerging landscape of cyber security legislation and compliance. The frequency and complexity of legislation surrounding cyber security has exploded in the past two years. As our lives and commerce become increasingly dependent on IT systems, the interaction of existing laws and proposed legislation becomes more and more complex. This symposium series explores the complex emerging framework of multi-level legal and technology compliance requirements.

International-Level Cyber Security Compliance
Thursday, May 26, 6:15-8:00 pm

Holland & Knight, 2099 Pennsylvania Ave. NW Metro-Foggy Bottom, Orange and Blue Line

If state and federal law appear inconsistent, federal and international law are even more so. This last session will set forth the existing pieces of the international cyber security puzzle, identifying places where diplomacy and concerted effort may be able to harmonize legal issues across borders.

Invited speakers include...

Jody Westby, Chair of the ABA's International Cybercrime Project
Drew Arena, Verizon Communications
Richard Beaird, Department of State
Jonathan Winer, Alston and Bird, LLP
Betty Shave, Department of Justice

Space is limited
RSVP now to Amy Cobb, 703-993-8193 or acobb1@gmu.edu

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

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

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://techcenter.gmu.edu/programs/cipp/cip_report.html.