The Critical Infrastructure Protection Program August 2005 / Volume 4, No. 2

THE CIP REPORT

Newsletter Editorial Staff

Editors

Jessica Milloy

Jeanne Geers

Staff Writers

Amy Cobb

Randy Jackson

Colleen Hardy

Maeve Dion

JMU Coordinators

John Noftsinger

Ken Newbold

Publishing

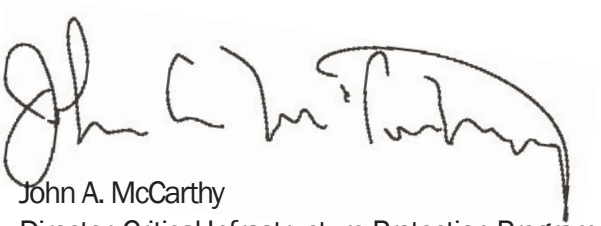
Zeichner Risk Analytics

Contact: cipp01@gmu.edu
703.993.4840

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

This month's edition of *The CIP Report* focuses on the enormous changes ongoing in the homeland security and critical infrastructure protection arenas and the major initiatives outlined by the new Secretary of Homeland Security, Michael Chertoff, following the Department of Homeland Security's (DHS) Second Stage Review. These changes, which stem from a six point agenda covering such topics as preparedness for catastrophic events, transportation security systems, border security, and even internal DHS financial and human resource management processes, represent the Department's recognition that its work must be based upon priorities driven by risk. These announced changes, and the forthcoming policy initiatives, reveal Secretary Chertoff's vision and direction for DHS under his leadership. This topic will be further explored not only in the pages of this issue, but in the upcoming CIP Program event *"Making America Safer Four Years after 9/11; A Conversation with Secretary Michael Chertoff"*, to be held on September 9, 2005 at the National Press Club. This event is the fifth in a series of Critical Conversations moderated by Frank Sesno, a Senior Fellow of the CIP Program, and will provide ample opportunity for Chertoff to further discuss this agenda and his vision for the Department.

In addition to the six point agenda, we have also included the new organization chart released by DHS last month as the proposed end state for the reorganized Department. We are also pleased to include an interview with Dr. John H. Marburger, Director of the Office of Science and Technology Policy. We would also like to welcome Assistant Secretary for Infrastructure Protection Bob Stephan, who we have highlighted in his new position within DHS leadership. We are also pleased to include contributions from the National Biometric Security Project, which focuses on applications of biometric technology in support of homeland security objectives, and a Legal Insights column by Rod Nydam, which describes some of the legal challenges that DHS has faced during the past few years. Finally, we have included project summaries of the work undertaken by CIP Program interns this summer and invitation information on the upcoming Critical Conversation event.



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

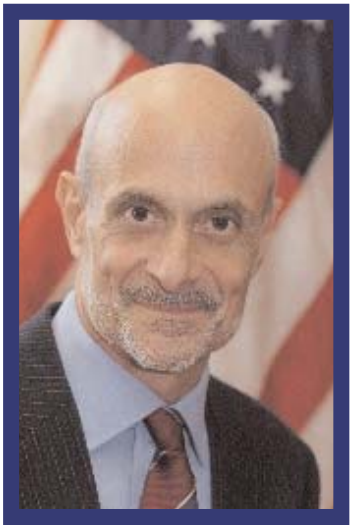
Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security

Secretary Michael Chertoff today announced a six-point agenda for the Department of Homeland Security (DHS) designed to ensure that the Department's policies, operations, and structures are aligned in the best way to address the potential threats - both present and future - that face our nation.

"Our Department must drive improvement with a sense of urgency. Our enemy constantly changes and adapts, so we as a Department must be nimble and decisive," said Secretary Michael Chertoff.

The July 13th announcement reflects conclusions drawn as a result of the Second Stage Review, a careful study of the Department's programs, policies, operations and structure. The Review examined nearly every element of the Department of Homeland Security in order to recommend ways that DHS could better manage risk in terms of threat, vulnerability and consequence; prioritize policies and operational missions according to this risk-based approach; and establish a series of preventive and protective steps that would increase security at multiple levels.

"DHS must base its work on priorities driven by risk," said Secretary Chertoff. "Our goal is to maximize our security, but not security at any price. Our security regime must promote Americans' freedom, prosperity, mobility, and individual privacy."



Secretary Michael Chertoff

The Secretary's six-point agenda will guide DHS in the near term and result in changes that will:

- Increase overall preparedness, particularly for catastrophic events;
- Create better transportation security systems to move people and cargo more securely and efficiently;
- Strengthen border security and interior enforcement and reform immigration processes;
- Enhance information sharing with our partners;
- Improve DHS financial management, human resource development, procurement and information technology; and
- Realign the DHS organization to maximize mission performance.

Secretary Chertoff said that details of new policy initiatives in these six areas will be announced in the coming weeks and months, including:

- A new approach to securing our borders through additional personnel, new technologies, infrastructure investments, and interior enforcement - coupled with efforts to reduce the demand for illegal border migration by channeling migrants seeking work into regulated legal channels;
- Restructuring the current immigration process to enhance security and improve customer service;
- Reaching out to state homeland security officials to improve information exchange protocols, refine the Homeland Security Advisory System, support state and regional data fusion centers, and address other topics of mutual concern; and
- Investing in the Department's most important asset - its people - with top-notch professional career training and development efforts.

Secretary Chertoff also announced two common sense changes to improve the way the Department does business.
(Continued, Page 3)

Six Point Agenda *(Cont. from Page 2)*

- **Require 10-Fingerscan Standard for Foreign Visitors.** DHS will strengthen the US-VISIT program to require a one-time 10-fingerscan capture upon enrollment, with continued use of two-print verification during later entries, to ensure the highest levels of accuracy in identifying people entering and exiting our country.

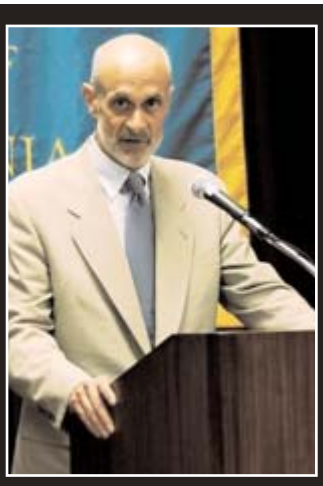
- **Eliminate 30-minute Rule for DCA Flights.** As a result of numerous security measures established to protect passengers and air travel, DHS will eliminate the 30-minute rule preventing passengers from standing up within thirty minutes of takeoff or landing for flights to or from Ronald Reagan National Airport.

Organizational Initiatives: Structural Adjustments to DHS

The Secretary also announced details of his proposal for realigning the Department of Homeland Security to increase its ability to prepare, prevent, and respond to terrorist attacks and other emergencies. These changes will better integrate the Department, giving DHS employees better tools to help them accomplish their mission. These management tools will:

- *Centralize and Improve Policy Development and Coordination*. A new Directorate of Policy, ultimately led by an Under Secretary upon enactment of legislation, will serve as the primary Department-wide coordinator for policies, regulations, and other initiatives. This Directorate will ensure the consistency of policy and regulatory development across various parts of the Department as well as perform long-range strategic policy planning. It will assume the policy coordination functions previously performed by the Border and Transportation Security (BTS) Directorate. It will also create a single point of contact for internal and external stakeholders by consolidating or co-locating similar activities from across the department. This new Directorate will include:
  - *Office of International Affairs;*
  - *Office of Private Sector Liaison;*
  - *Homeland Security Advisory Council;*
  - *Office of Immigration Statistics;*
  - *Senior Asylum Officer.*

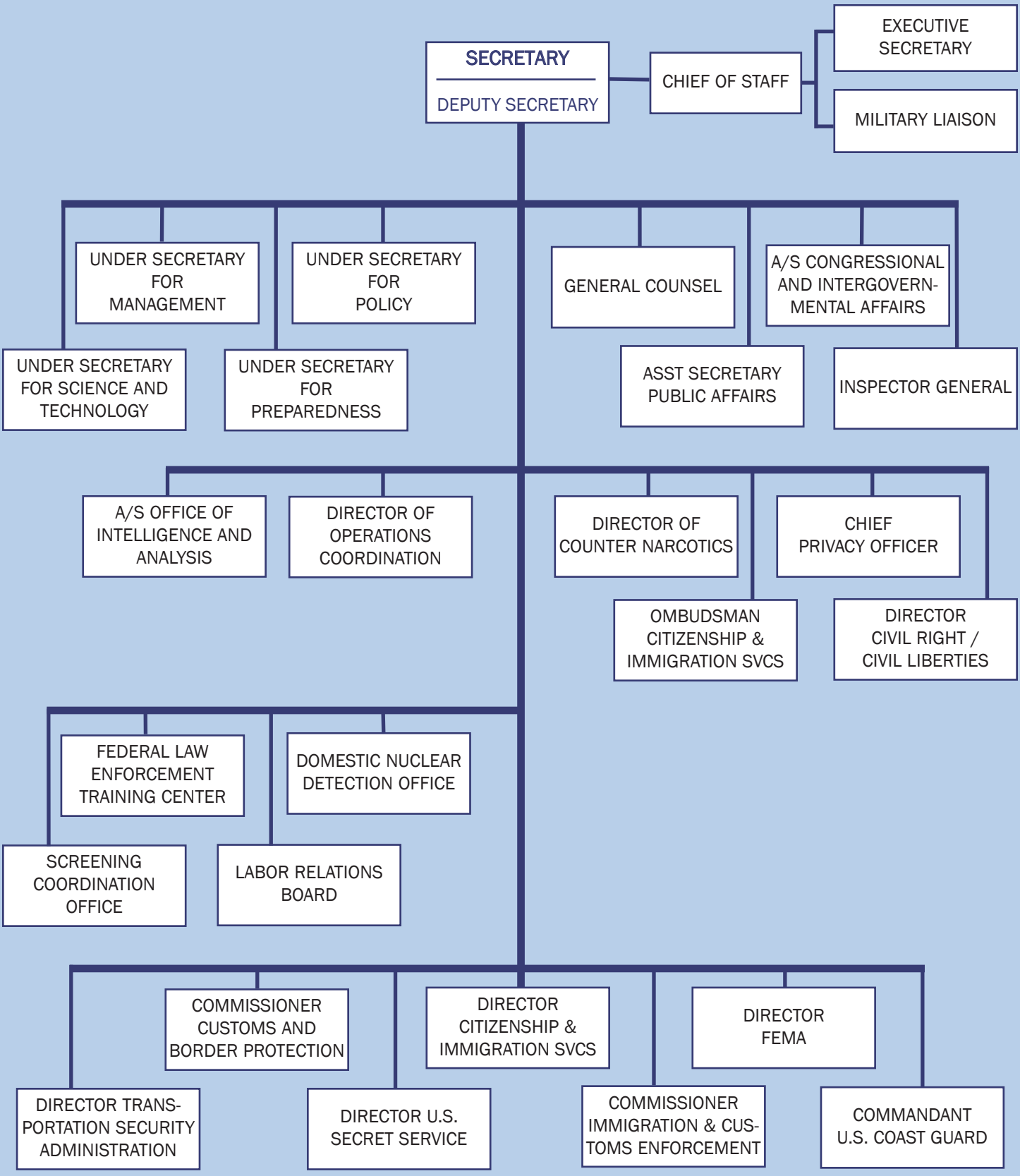
- *Strengthen Intelligence Functions and Information Sharing*. A new Office of Intelligence and Analysis will ensure that information is gathered from all relevant field operations and other parts of the intelligence community; analyzed with a mission-oriented focus; informative to senior decision-makers; and disseminated to the appropriate federal, state, local, and private sector partners. Led by a Chief Intelligence Officer who reports directly to the Secretary, this office will be comprised of analysts within the former Information Analysis directorate and draw on expertise of other DHS components with intelligence *(Continued, Page 5)*



"[A]mong the imperatives in setting our agenda in the next six months were the need to increase our focus on preparedness at all levels of government and private life; the obligation that we have to finally gain control of our borders and to do so in a way that is consistent with our traditional value of welcoming visitors and also fostering immigration that strengthens our country; protecting our transportation, which is what binds us together; further promoting information and intelligence sharing; building upon the management of the individual components to finally create a unified management that covers such important considerations as procurement policy that is efficient and has integrity; properly managed finances; and, of course, a fully integrated state-of-the-art information technology system."
Secretary Michael Chertoff, addressing the Council of Excellence in Government

Department of Homeland Security Organization Chart

(proposed end state)



Six Point Agenda *(Cont. from Page 3)* collection and analysis operations.

- *Improve Coordination and Efficiency of Operations*. A new Director of Operations Coordination will enable DHS to more effectively conduct joint operations across all organizational elements; coordinate incident management activities; and utilize all resources within the Department to translate intelligence and policy into immediate action. The Homeland Security Operations Center, which serves as the nation's nerve center for information sharing and domestic incident management on a 24/7/365 basis, will be a critical part of this new office.

- *Enhance Coordination and Deployment of Preparedness Assets*. The Information Analysis and Infrastructure Protection Directorate will be renamed the Directorate for Preparedness and consolidate preparedness assets from across the Department. The Directorate for Preparedness will facilitate grants and oversee nationwide preparedness efforts supporting first responder training, citizen awareness, public health, infrastructure and cyber security and ensure proper steps are taken to protect high-risk targets. The directorate will be managed by an Under Secretary and include:

  - A new Assistant Secretary for Cyber Security and Telecommunications, responsible for identifying and assessing the vulnerability of critical telecommunications infrastructure and assets; providing timely, actionable and valuable threat information; and leading the national response to cyber and telecommunications attacks;
  - A new Chief Medical Officer, responsible for carrying out the Department's responsibilities to coordinate the response to biological attacks - and to serve as a principal liaison between DHS and the Department of Health and Human Services, the Centers for Disease Control, the National Institutes of Health, and other key parts of the biomedical and public health communities;
  - Assistant Secretary for Infrastructure Protection;
  - Assets of the Office of State and Local Government Coordination and Preparedness responsible for grants, training and exercises;
  - U.S. Fire Administration; and
  - Office of National Capitol Region Coordination.

Other Department Realignments

- *Improve National Response and Recovery Efforts by Focusing FEMA on Its Core Functions.* FEMA will report directly to the Secretary of Homeland Security. In order to strengthen and enhance our Nation's ability to respond to and recover from manmade or natural disasters, FEMA will now focus on its historic and vital mission of response and recovery.
- *Integrate Federal Air Marshal Service (FAMS) into Broader Aviation Security Efforts*. The Federal Air Marshal Service will be moved from the Immigration *(Continued, Page 6)*

Secretary of Homeland Security Michael Chertoff

On February 15, 2005, Judge Michael Chertoff was sworn in as the second Secretary of Homeland Security. Chosen by President George W. Bush, Senator Charles Schumer (D-NY) praised that "Judge [Michael] Chertoff has the résumé to be an excellent homeland security secretary, given his law enforcement background and understanding of New York and America's neglected homeland security needs." Chertoff's bipartisan support extends back to 1993 when then President Bill Clinton replaced all except one U.S. attorney across the country with his own nominees - the exception was New Jersey U.S. Attorney Michael Chertoff who was ask to remain and to continue serving the American people.

I come to this responsibility therefore with the conviction that, as a nation, we have every reason to be resolute about our fight against terror; every reason to be optimistic about our ability to enhance our security while preserving our liberties; and every reason to act urgently in doing both. (Secretary Chertoff, George Washington University, Homeland Security Policy Institute remarks, March 16, 2005)

In addition to his service as the New Jersey U.S. Attorney, Secretary Chertoff served as a clerk to Supreme Court Justice William Brennan, Jr., was a Partner in the law firm of Latham & Watkins, served as Special Counsel for the U.S. Senate Whitewater Committee, and was previously confirmed by the Senate to serve in the Bush Administration as Assistant Attorney General for the Criminal Division at the Department of Justice. Chertoff graduated magna cum laude from Harvard College in 1975 and *(Continued, Page 14)*

Leadership Highlight

Robert B. Stephan

Acting Under Secretary for Information Analysis and Infrastructure Protection
Assistant Secretary for Infrastructure Protection

The CIP Program would like to express its gratitude for being invited into a series of conversations between the public and private sectors and academe regarding feedback of where we have been vis-à-vis Robert Stephan's priorities within his portfolio. This was an open and welcome exchange that was extremely informative and will help shape the role that the CIP Program plays in this ongoing discussion.

Colonel Bob Stephan was appointed to serve as the Assistant Secretary of Homeland Security for Infrastructure Protection in April 2005. In this capacity, he is responsible for the Department's efforts to catalog our critical infrastructures and key resources and coordinate risk-based strategies and protective measures to secure them from terrorist attack.

His prior experience as Senior Director for Critical Infrastructure Protection in the Executive Office of the President (EOP) makes him a well qualified choice for the Assistant Secretary position. During his tenure with EOP, his duties included developing and coordinating interagency policy and strategic initiatives to protect the United States against terrorist attack across 13 critical infrastructure sectors.

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

Colonel Stephan held a variety of key operational and command positions in the joint special operations community during a 24-year Air Force career. During Operation Desert Storm, he deployed to Saudi Arabia as a joint battle staff planner and mission commander supporting Joint Special Operations Task Force strategic interdiction operations in Iraq. As a commander of two Air Force Special Tactics Squadrons, Colonel Stephan organized, trained, and equipped forces for contingency operations in Somalia, Haiti, Bosnia, Croatia, Liberia, Colombia, and Kosovo.

Robert Stephan

Colonel Stephan is a distinguished graduate of the USAF Academy, and holds a bachelor's degree in Political Science. He is an Olmsted Scholar, and has earned master's degrees in International Relations from the University of Belgrano, Buenos Aires, Argentina, and The Johns Hopkins University. ❖

Six Point Agenda *(Cont. from Page 5)* and Customs Enforcement (ICE) bureau to the Transportation Security Administration to increase operational coordination and strengthen efforts to meet this common goal of aviation security.

- *Merge Legislative and Intergovernmental Affairs.* This new Office of Legislative and Intergovernmental Affairs will merge certain functions among the Office of Legislative Affairs and the Office of State and Local Government Coordination in order to streamline intergovernmental relations efforts and better share homeland security information with members of Congress as *(Continued, Page 8)*

Legal Insights

DHS and the Private Sector: Addressing Hurdles to Information Sharing

Rod Nydam
Associate Director, Private Sector Programs
CIP Program

Relations with the private sector have always been a key factor in DHS's evolution. The Department has recognized that the private sector plays a key role in efforts to protect the country's critical infrastructure and has begun many programs to integrate private sector information into their programs. From the beginning, the private sector identified many legal issues which complicate the relationship with the government and present hurdles to sharing the type of information needed to develop effective programs. This article highlights just two of the current legal research projects underway at the CIP Program related to some of the most important legal hurdles to public-private information sharing.

I. Protected Critical Infrastructure Information (PCII)

In order to develop plans to protect the nation's infrastructure, DHS and other government agencies have been requesting large amounts of data from the private sector. Obviously, many private companies are concerned that these disclosures might become subject to the Freedom of Information Act (FOIA) and be disclosed to the public and their competitors. In addition, there is a concern that the information might fall into the wrong hands and defeat the purpose for gathering the information.

In order to address these concerns, the Homeland Security Act contained a provision which allowed private entities to submit information to DHS and have that information be exempted from FOIA. While there were already national security exemptions for voluntarily submitted information, PCII allowed private entities to receive confirmation before a FOIA request that the information would be protected from disclosure. This article will not go into the detailed workings of PCII and readers can find a good summary of the program at http://www.dhs.gov/dhspublic/display?theme=52&content=3455.

While the private sector sees PCII as a first step in encouraging information submissions, many private companies still are concerned that the Act needs to offer more protections for the information submitted before it will produce the desired level of information sharing. In upcoming white papers and research papers, we will be discussing ways that the Act may be modified to address private sector concerns including the following topics:

- *Originator Control.* Under the current PCII act, once a private entity submits information, that entity loses control over how the information is disseminated or used within the government. While building trusting relations is important, many private entities are not comfortable knowing that sensitive information submitted to one agency for a limited purpose may find its way to several other agencies. This results in a great deal of hesitancy to submit the information. Originator control is one way to address this concern. For example, assume a pipeline company has information about critical nodes in its pipeline and wants to share that information with the government in order to make the government aware of a particular vulnerability. That company would be more comfortable submitting the information under conditions it establishes knowing that information will only be used and disseminated in the manner it directs. Originator control would allow the company to submit the information to DHS with explicit instructions on how the information can be used. While PCII has some provisions addressing dissemination of submitted information, those decisions currently lie with the government, not the submitter.

(Continued, Page 8)

Legal Insights *(Cont. from Page 7)*

- *Time Limitation.* Another private sector concern is the fact that submitted information may become out of date or that, if the information stays within the government for extended periods of time, the risk of inadvertent disclosure or improper use of the information increases. One possible solution for this problem is putting a limit on the amount of time the government holds the information. This limit could be established two ways. The submitting entity could be allowed to submit the information but place a limit on its use requiring, for example, that all information must be destroyed or returned within a year after submitting. Second, the Act could set a statutory time limit for information retention stating that all information (except for the end products produced from the information) must be destroyed or returned within a given amount of time.

- *Limitations of Liability.* PCII does provide some protection with respect to the use of submitted information in litigation. The information is not discoverable from the government. However, many private sector participants raise concerns about whether information produced could be discovered by private litigants in a lawsuit. For example, in an industrial accident, could a private litigant obtain information prepared by a company for the government during the discovery process? Furthermore, could a company be held liable for not acting on a vulnerability discovered during the process of collecting data that it intended to submit voluntarily to the government for critical infrastructure protection purposes?

II. FACA and Sunshine Laws

The Federal Advisory Committee Act presents another challenge to DHS's efforts to integrate the private sector into homeland security processes. The government needs to interact with the private sector. However, current FACA regulations often put undue burdens and bureaucracy in the dealings between the public and private sector. CIP Program research is addressing various ways to have an effective public-private partnership within the requirements of FACA. In addition, this research is evaluating the power of the Secretary to exempt certain organizations from FACA requirements when national security issues are at stake.

In addition to FACA, states and localities often have Sunshine Laws that require open meetings when the private sector meets with government officials. These laws complicate the private sector's ability to share sensitive information with state and local officials. This is particularly complicated with state and municipal utilities, as well as with private companies trying to work with state and local agencies and first responders. As part of the FACA research, the CIP Program will be evaluating methods to address CIP within the framework of state Sunshine Laws.

FOIA and FACA are just two examples of some of the legal hurdles facing DHS and the private sector. Those laws were passed long before the extensive post 9-11 efforts to protect critical infrastructure. In order to ensure an effective public-private partnership, the participants will need to establish creative solutions to work within current law. In addition, current law is probably not adequate to produce a completely effective relationship and we should expect that these laws will change and evolve to meet the new challenges facing us. ❖

Six Point Agenda *(Cont. from Page 6)* well as state and local officials.

- *Assign Office of Security to Management Directorate.* The Office of Security will be moved to return oversight of that office to the Under Secretary for Management in order to better manage information systems, contractual activities, security accreditation, training and resources.

The Homeland Security Act of 2002 (HSA) provides certain flexibility for the Secretary of Homeland Security to establish, consolidate, alter or discontinue organizational units within the Department. The mechanism for implementing these changes is a notification to Congress, required under section 872 of the HSA, allowing for the changes to take effect after 60 days. Other proposed changes *(Continued, Page 14)*

An Interview with Dr. John H. Marburger, III Science Advisor to the President Director, Office of Science and Technology Policy

After 9/11, the United States became more aware of possible outside threats and had to examine its critical infrastructure vulnerabilities. What impact do you feel the 2004 National Plan for Research and Development (R&D) in Support of Critical Infrastructure Protection will have on improving national security?

The 2004 plan outlines a vision for future CIP-related research and development (R&D) and provides a baseline so that we can better understand what our current status, capabilities and resources are. This thorough assessment will enable the U.S. to leverage existing assets and operations and "jump start" R&D in this area. It also forms the basis for a broader plan that incorporates R&D efforts conducted by industry and academia.

What impact will the Plan have on CIP R&D initiatives?

The Plan is a clear statement of how the collective resources of government can be brought to bear on the complex, multi-faceted set of issues related to infrastructure protection. It will enable us to build a cohesive set of activities that will contribute to the achievement of the Plan's strategic goals. Its first impact is to facilitate discussion with industry and academia and inform agencies as they plan their future efforts.

Who were the key players involved in the development of the 2004 Plan that involves the protection of all the critical infrastructures and key assets?

In coordination with OSTP, DHS led the effort through the agency's CIP R&D portfolio manager, Dr. John Cummings. A number of Federal agencies, working together, developed and reviewed the plan, seeking guidance from other user and stakeholder communities in order to ensure broad coverage and an integrated picture.

The 2004 Plan identifies R&D gaps and needs based on known threats. What is the most effective way to address future-identified and unknown threats in a timely fashion?

The plan addresses the development of new technology and processes that are designed to perform environmental scans, mine information, perform alternative scenario analysis and use other means to help discover emerging threats or those conditions that could ferment them. These efforts will be instrumental in identifying and addressing future threats in a timely manner.

The 2004 Plan provides a baseline of R&D gaps and will be updated annually. Will the R&D priorities change as the Plan is modified? If so, how will this constant change impact R&D efforts and the ability of researchers to follow through on their work?

Future research and development achievements will offer new opportunities and new research directions, which future versions of the Plan can encompass. However, the three *(Continued, Page 14)*

My Summer as a CIP Program Intern

Each summer the CIP Program chooses highly qualified students to work on a variety of projects. CIP Program internships attempt to match students with internal projects related to their academic interests or place students in agencies and offices of partner organizations. In the section below, our interns describe their summer projects and future plans.

Timothy Goobic is in his final year as a graduate student at the University of Kentucky's Martin School for Public Administration. In 2004 he graduated from Brown University with degrees in History and Political Science and desires to one day become involved with national security policy. Over a 10-week period at the CIP Program, Tim has been involved in a number of areas of the program which have exposed him to a wide range of issues. His first project involved gathering data from previously completed CIPP research projects and cataloguing them by genres for use in an internal database. Throughout this process he also produced four written works which were published in *The CIP Report* and assisted in various event preparations. However, the most fascinating aspect of the internship came through assisting Rebecca Luria with the CIP Oral History Project where he conducted background research on various terrorism commissions and was given the opportunity to sit in on multiple interviews with high ranking federal officials.

During the summer of 2005, Jeremy Kidd had the opportunity to examine in detail the implications of the Protection of Critical Infrastructure Information Act of 2002 (PCII). He investigated its impacts on the application of Exemption 4 of the Freedom of Information Act (FOIA), as well as PCII's ability to achieve its stated goals. Exhaustive searches of law reviews, case law, and media outlets were used to develop the premises of the research, and then those same sources, along with economic intuition and theory, were used to evaluate proposed changes to PCII. The application of economic principles to the law is particularly of interest to Jeremy because he completed a bachelor's degree in economics and political science and a Ph.D. in economics at Utah State University, and is a rising second year student in law at George Mason University School of Law.

Kristen DiGirolamo is working in Governor Warner's Office of Commonwealth Preparedness. In relation to CIP, Kristen has gone on Site Assist Visits (SAVs) in order to write Buffer Zone Protection Plans. During the SAVs, Kristen assisted a team from VDOT and local law enforcement in assessing site vulnerabilities. She also helped to do the preliminary infrastructure prioritization list. Also relating to CIP, Kristen attended the NCR CIP Working Group meetings, as well as Virginia's CIP Working Group meetings. In addition, she is assisting her office in coming up with ways to shift the focus from protection to resiliency of critical infrastructure. Kristen is a junior at the University of Richmond and is majoring in Political Science with a minor in Leadership Studies.

Brett A. Callahan is currently working toward her J.D. from George Mason University School of Law in the Intellectual Property Law Track. She expects to graduate in May of 2007. She received a B.S. in Nutrition, Food, and Agriculture from Cornell University. This summer she interned for the CIP Program's Private Sector Programs group where she conducted legal research on several topics. Brett researched the legislative history of a provision of the Homeland Security Act of 2002. She also examined theories of potential civil liability and defenses. Additionally, Brett studied an issue relating to the open government laws.

Sachin Kandhari started his JD program at the George Mason University School of Law in Fall 2004, and expects to graduate in 2007. Being a graduate of the University of Virginia with a BS degree in Physics and having a strong interest in cyberspace and technology, Sachin is focusing his legal education on Intellectual Property Law. He spent the summer of 2005 working for the National Capital Region project, which focuses on developing methods to inform public and private decision-makers on the benefits and costs of initiatives to enhance the security of the region. Sachin was involved in the more technical aspects of the NCR. His duties included helping to design regional public/private governance and resource allocation systems for risk management, and coordinating and editing risk management reports for the Phase One project. Sachin also designed a document and report catalog website for the NCR, and helped compile an analytic database of regional public-private partnerships to improve infrastructure resiliency.

Greg Clinton spent this summer working with the Department of Energy on a cross-border mutual aid program for the electricity and natural gas industries. During emergencies, electric companies in the United States often request aid from their Canadian counterparts. In the past, these Canadian workers have encountered difficulty crossing the border. Greg's project seeks to find ways to facilitate this process. This fall Greg will be starting his third year at George Mason Law School. Prior to this he graduated with a degree in computer science from Cornell University.

Nancy Morrison is an incoming PhD student at George Mason University's Institute for Conflict Analysis and Resolution program, where she is currently completing her master's thesis. She received her M.A. in English Literature from Virginia Tech in 1994. She received a B.S. in Clinical Psychology in 1988. Nancy's work at the CIP Program involves the development of the Homeland Security Capabilities Database (HSCD). This project originated during a meeting of the Terrorist Working Group, and the goal is to develop a database by which industry, private individuals, and government can investigate the university's homeland security capabilities (individual research projects, programs/centers, researchers, and course offerings). The HSCD will not duplicate current university "expert databases" through which GMU researchers could look for grant opportunities. The initial prototype will include a select sampling of GMU's homeland security capabilities from each school.

Identity Assurance and the Protection of the Civil Infrastructure

National Biometric Security Project

Unlike other personal identification techniques that rely on something you own, such as a photo ID, driver's license, etc., or something you know, such as a pin or password, biometrics is an automated method of identifying or verifying the identity of a living human being based on a physiological or behavioral characteristic unique to that individual. The most common biometrics in use today include:

- Fingerprint verification
- Iris recognition
- Hand geometry
- Voice verification
- Signature verification
- Facial recognition

Next generation or "bleeding edge biometrics" such as gait, odor, ear, hand vein and thermography are currently under development or have been available for some time with various capabilities for deployment.

Biometrics are most often utilized in four general classes of security applications including: access [logical and physical]; transaction authentication and logging; surveillance; and forensics.

Formed as a not-for-profit private organization after the attacks of September 11, 2001, the mission of the National Biometric Security Project is to assist government and private sector organizations in deterring terrorist attacks on the civil infrastructure by enhancing effective, automated human identification through the application of proven biometric technologies. Threats to the civil infrastructure span both the civil and private sectors and include:

The Transportation System With the recent broadening of the US-VISIT program, aviation transportation has embraced the application of biometric technologies to verify and authenticate the identities of both passengers and personnel.

Maritime transportation has received a great deal of attention from a security perspective in large part due to the realization that only 3% - 10% of all container traffic entering the United States through its ports and waterways is ever inspected. The opportunity for exploitation of our maritime system led to the Maritime Transportation Security Act (MTSA) mandate for implementation of strict security plans by all operators and owners of US-based maritime facilities and ports and all vessel operators who seek to unload cargo in the US. Since the average container entering the U.S. is handled on 17 different occasions before it reaches its final destination, biometrics can be an effective identity authentication method, helping to assure the identity of personnel involved in the transfer of container cargo.

The Economic System One of the most organized sectors in terms of addressing its security concerns is banking and finance, due not only to the extensive human and financial losses suffered by the industry on 9/11 but also to earlier preparations in anticipation of Y2K. Banking and finance is actively applying biometrics in the conduct of its business, due in part to the profound and growing concern with identity theft shared by both corporate and consumer clients. ID theft is at the heart of significantly broader economic vulnerabilities and national security concerns. Using biometrics to develop ID theft countermeasures has direct impact on civil infrastructure protection.

The Energy System represents the one commodity on which all productive economic activity is dependent, the sector most vulnerable to outages, and the one most likely to initiate cascading disruptions. The fragility of critical infrastructure associated with the production of electric power is particularly acute in light of its highly complex delivery systems. It appears that the application of biometrics technology could have significant impact in a limited ingress/egress basis, for controlling access by authorized personnel to sensitive locations.

As in the case of electric power, the opportunity for application of biometrics technologies in the oil and natural *(Continued, Page 13)*

Biometrics *(Cont. from Page 12)*
gas sector appears to be more narrowly defined in terms of verifying/authenticating the access of key personnel to sensitive facilities, both in the US and abroad. Biometrics might also be applied in a cyber-security scenario, for authorizing access to key energy management systems whose functioning is crucial to the industry's data collection processes.

The Communications System The application of biometrics technology in the complex world of IT and telecom requires a focus on points within the sector's critical physical infrastructure whose destruction and/or damage would seriously impair data and voice transmissions. This means key network servers, routers, and switches. (Circuit integrity is also of extreme importance, as the 9/11 tragedy revealed, but circuits are not physically housed in any one specific location; however, the Network Operations Centers that manage them are.) Controlling access to these critical network components in both physical and virtual form can be achieved through a layered combination of biometric technologies that validate, on an incremental basis, a user's right to proceed through increasingly sensitive levels of information.

Each sector has a particular set of unique characteristics and vulnerabilities, yet also has much in common due to their interdependencies. All are struggling to answer complex questions: What impact will outage duration, frequency and other factors have on my ability to operate? How can back-up systems and mechanisms mitigate or reduce the impact of key asset loss? All are concerned with establishing business continuity practices. All worry about the escalating cost of security measures to protect critical infrastructure assets and are concerned with funding and operational interruptions in light of competitive pressures to contain costs and improve efficiency. All worry about public outcry should the measures implemented be perceived as excessive, overly invasive or causing undue inconvenience.

In order for biometrics to address these questions certain prerequisites must be resolved. These include: (1) articulation of application requirements and faster adoption of standards for performance and integration; (2) objective testing and validation; (3) training and education that is pertinent to the end-users and kept current on both technology and sources, and (4) improved tools for use and operation based on focused applied research programs. Additionally, cultural and societal issues such as impact on privacy must be resolved.

Ambitious goals such as these cannot be achieved overnight. Work in key areas such as standards, testing, applied research and training has languished for nearly a decade, and it will take an integrated industry effort to make quick, significant and continuously expanding progress in all of the important sectors described above. ❖

About the National Biometric Security Project

Supported by Congress, the first Biometrics for National Security (BiNS) contract was awarded to NBSP in August 2003, under administration by the NSA. The Congress supported two additional earmarks for the NBSP in FY 04 and FY 05, also through the intelligence community. NBSP currently supports government and private sector efforts to evaluate, acquire and deploy biometric technology. Key NBSP initiatives include: requirements and standards development; testing and evaluation; applied research and engineering; training; and minimizing the societal impact of deployment.

Marburger *(Cont. from Page 9)* strategic goals identified in the Plan represent enormously challenging research objectives that will most likely require a long term research effort.

What mechanisms are being used to disseminate the 2004 Plan to the relevant communities so as to engage additional researchers in improving national security and decreasing critical infrastructure recovery time in the event of an attack?

Originally released at the first annual Industry Workshop on CIP R&D in April 2005, the Plan is available on the web at http://www.dhs.gov/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf . Also, a website is being developed to gather feedback and promote discussion. Additional workshops engaging a wide variety of researchers from all sectors are planned through the year. We are also working with the Private Sector Programs group at George Mason University's CIP Program that acts as convener for the ISACs as well as the government coordinating councils. ❖

Six Point Agenda *(Cont. from Page 8)* will require Congressional action. The Department will work with Congress to accomplish these shared goals.

Background: The Second Stage Review (2SR) Process

The Second Stage Review included 18 action teams composed of 10-12 members with appropriate expertise dealing with certain subject matter. More than 250 participants within the Department of Homeland Security, representing a comprehensive cross-section, contributed to the Second Stage Review process.

Final issue papers from the action teams were completed and given to the Secretary by May 31, 2005. The Secretary met with all 18 action teams to discuss their findings in detail, and their work served as an important basis for the July 13th announcement - as well as a number of new initiatives yet to be announced.

Action teams examined a wide range of issues, including:

- Risk/Readiness
- Information and Intelligence Sharing
- Performance Metrics
- Law Enforcement Activities
- Listening to External Partners
- Supply Chain Security
- Internal Communications and DHS Culture
- Research, Technology & Detection ❖

Chertoff *(Cont. from Page 5)* magna cum laude from Harvard Law School in 1978.

Chertoff has maintained a low profile since taking over the helm of DHS. After six-months as DHS's top man, in a speech delivered on July 13, 2005 at the Ronald Reagan Building, he stepped forth to share with the Congress and the American people his plan to reorganize the department. Chertoff's "Second Stage Review", or 2SR as he refers to it, started immediately. This systematic evaluation of the Department's operations, policies, and structures was supported by the Homeland Security Act of 2002 (HSA), the law which created the massive department and provides flexibility for the Secretary "to establish, consolidate, alter or discontinue organizational units within the department." The CIP Program is pleased to host the fifth in a series of Critical Conversations on September 9th, 2005 at the National Press Club. This event will feature Secretary Chertoff and moderator Frank Sesno, Senior CIP Program Fellow and a Special Correspondent for CNN. During the morning discussion, Secretary Chertoff will discuss in greater detail his plans following the completion of the 2SR and the challenges that lie ahead for his Department and our nation. ❖

GEORGE MASON UNIVERSITY | School of Law

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

SAVE THE DATE...

For the Fifth in a Series of Critical Conversations on Infrastructure Protection

Sponsored by the Critical Infrastructure Protection Program at
George Mason University School of Law

A Conversation with Secretary Michael Chertoff
Department of Homeland Security

Making America Safer Four Years after 9/11

Friday, September 9, 2005
Breakfast: 9 a.m.
Newsmaker Discussion: 9:30 - 10:30 a.m.

The National Press Club
The Ballroom
529 14th Street, N.W.
Washington, D.C.

R.S.V.P. (703) 993-4722
Please note that seating is limited.

Moderated by
Frank Sesno
Senior Fellow, Critical Infrastructure Protection Program

The CIP Program, a joint effort between George Mason University School of Law and James Madison University 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 infrastructures. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

More information on the CIP Program can be found at http://cipp.gmu.edu.

Rebecca Luria has been with the CIP Program since Day One, when it was just the Executive Director, John McCarthy, and herself. She assisted John in growing the CIP Program into a $20 million research center before she was assigned to her position as Research Associate for the Critical Infrastructure Protection Oral History Project. In this capacity she conducts interviews with high-level industry leaders and government policy makers who have been influential in shaping our current CIP policy. The data collected has been used for a publication on the evolution of CIP policy as well as a digital archive. Rebecca holds a M.A. in International Policy from George Mason University and a B.A. in Anthropology from Guilford College. Rebecca served in the U.S. Peace Corps in rural Honduras and speaks Spanish fluently.

Rebecca is leaving the CIP Program this month to prepare for her upcoming wedding and will be relocating to Colorado. We wish her luck in all of her future endeavors and will miss her greatly!

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.