MAY 2003 / VOLUME 1, NUMBER 11

THE CIP REPORT

HOMELAND SECURITY ISSUE

CIP PROJECT STAFF

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Rebecca Luria, *CIP Project Administrator / Executive Assistant*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

George Baker, *Associate Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

Focus on the Department of Homeland Security

On January 24, 2003, the Department of Homeland Security became the 15th executive department of the President's Cabinet. In the biggest reorganization of the Federal government since World War II, Secretary of Homeland Security Tom Ridge took over the leadership of 22 previously disparate agencies, bringing over 170,000 professionals into the umbrella of homeland security. The Department's first priority is to protect the nation against further terrorist attacks-a mission it will undertake by analyzing threats, guarding borders and airports, safeguarding critical infrastructure, and coordinating our national response to future emergencies.

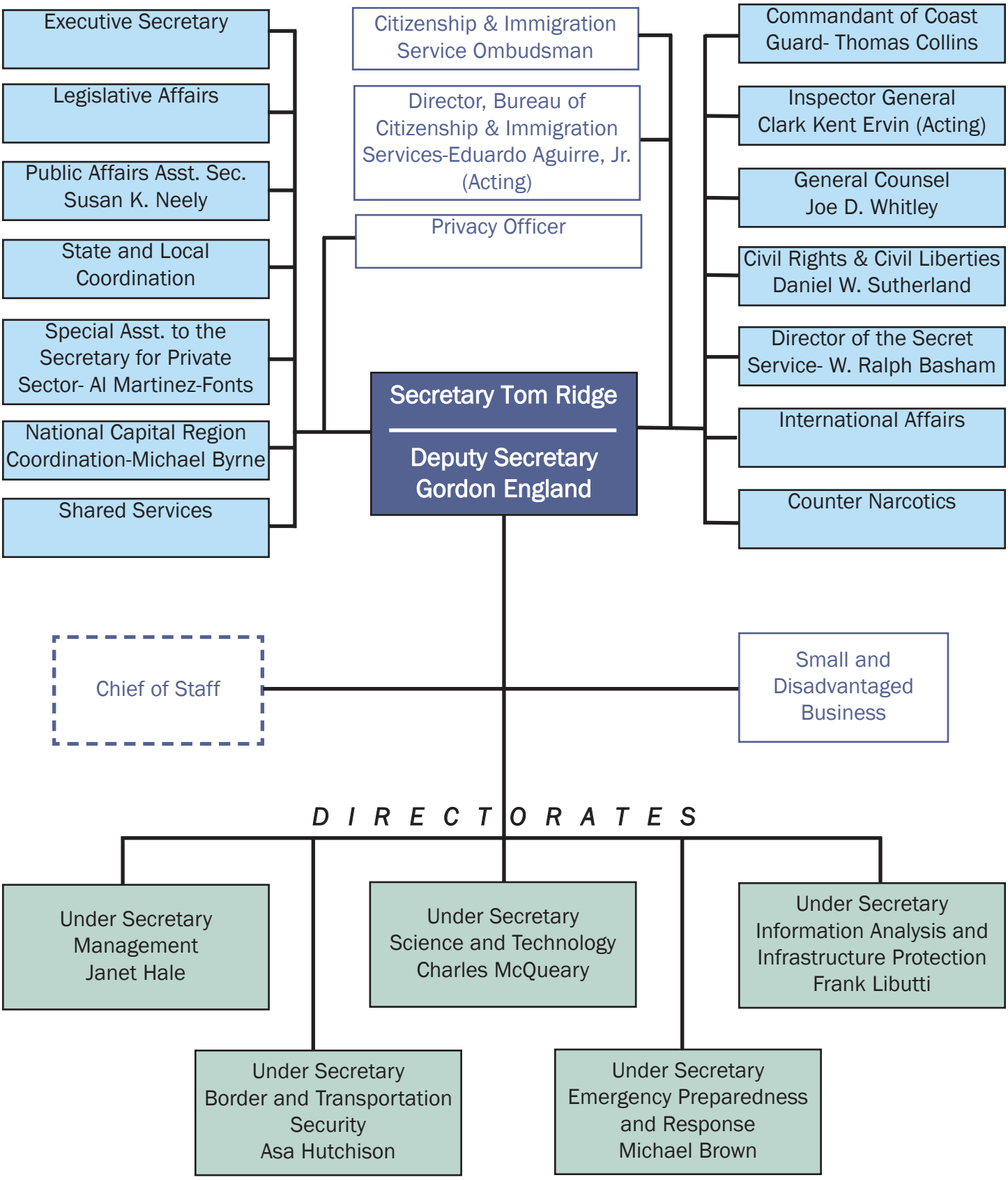
THE TECH CENTER
National Center for Technology & Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

In its first 100 days, the Department has already made significant progress in a number of areas, including:

- Orchestrated and launched Operation Liberty Shield, the first comprehensive, national plan to increase protections of America's citizens and infrastructure;
- Deployed new technologies and tools at land, air and sea borders;
- Stood up the Homeland Security Command Center, a national 24-7 watch operation;
- Launched the Ready campaign, a national multimedia public information program designed to build a citizen preparedness movement by giving Americans the basic tools they need to better prepare themselves and their families and encouraging them to "Be Ready;" and since its launch, Ready.gov has become one of the most visited sites in America;
- Expedited distribution of millions of dollars in grant monies to states and cities with more to come;
- Initiated a comprehensive reorganization of the border agencies as well as other administrative measures to increase departmental services and capabilities;
- Completed transition of majority of component agencies into the Department in the largest federal reorganization since World War II and;
- Conducted a series of listening sessions at strategic ports throughout the U.S. and began development of the vessel, facility and port security plans required by the Maritime Security Act of 2002.

The purpose of this issue of *The CIP Report* is to introduce you to some of the Homeland Security leaders at the Department, the White House, and Congress, and to some of the initiatives underway in this field of securing our nation.

Organization and Leadership of the Department of Homeland Security



DHS Who's Who

Secretary: Tom Ridge

On January 24, 2003, Tom Ridge became the first Secretary of the Department of Homeland Security. Ridge will work with more than 180,000 employees from combined agencies to strengthen our borders, provide for intelligence analysis and infrastructure protection, improve the use of science and technology to counter weapons of mass destruction, and to create a comprehensive response and recovery division.

Tom Ridge was sworn in as the first Director of the Office of Homeland Security in October 2001, following the tragic events of September 11. The charge to the nation's new director of homeland defense was to develop and coordinate a comprehensive

Tom Ridge

national strategy to strengthen the United States against terrorist threats or attacks. In the words of President George W. Bush, he had the strength, experience, personal commitment and authority to accomplish this critical mission.

Born Aug. 26, 1945, in Pittsburgh's Steel Valley, Gov. Ridge was raised in a working class family in veterans' public housing in Erie. He earned a scholarship to Harvard, graduating with honors in 1967. After his first year at The Dickinson School of Law, he was drafted into the U.S. Army, where he served as an infantry staff sergeant in Vietnam, earning the Bronze Star for Valor. After returning to Pennsylvania, he earned his law degree and was in private practice before becoming assistant district attorney in Erie County. He was elected to Congress in 1982. He was the first enlisted Vietnam combat veteran elected to the U.S. House, and was overwhelmingly re-elected six times. Governor Ridge and his wife, Michele, the former executive director of the Erie County Library system, have two children, Lesley and Tommy.

Deputy Secretary: Gordon England

Gordon England was confirmed as the first Deputy Secretary in the U.S. Department of Homeland Security on January 30, 2003.

Previously, Secretary England served as the 72nd Secretary of the Navy from May 24, 2001 until confirmation as Deputy Secretary. As Secretary of the Navy, Mr. England was responsible for an annual budget in excess of $110B and over 800,000 personnel.

Mr. England served as executive vice president of General Dynamics Corporation from 1997 until 2001 and was responsible for two major sectors of the corporation: Information Systems and International. Previously, he served as executive vice president of the Combat Systems Group, president of General Dynamics Fort Worth aircraft company (later Lockheed), president of General Dynamics Land Systems company and as the principal of a mergers and acquisition consulting company.

A native of Baltimore, Mr. England graduated from the University of Maryland in 1961 with a bachelor's degree in electrical engineering. In 1975 he earned a master's degree in business administration from the M.J. Neeley School of Business at Texas Christian University and is a member of various honorary societies: Beta Gamma Sigma (business), Omicron Delta Kappa (leadership) and Eta Kappa Nu (engineering).

DHS Who's Who

Under Secretary for Management: Janet Hale

Janet Hale was confirmed on March 6 as Under Secretary for Management.
Prior to her nomination and confirmation as Under Secretary, Ms. Hale served as the Assistant Secretary for Budget, Technology and Finance for the U.S. Department of Health and Human Services (HHS), and as chief financial officer and chief information officer.
Prior to HHS, she was the Associate Administrator for Finance for the House of Representatives and the Associate Director for Economics and Government at the Office of Management and Budget, responsible for budget and policy development, regulatory reform, and financial management for the departments of Treasury, Transportation, Commerce, Justice, and 25 smaller agencies.
Ms. Hale has also served as the Assistant Secretary for Budget and Programs at the Department of Transportation, Acting Assistant Secretary of Housing at the Department of Housing and Urban Development, Vice President with the U.S. Telephone Association, and Executive Vice President for the University of Pennsylvania.

She graduated from Miami University in Oxford, Ohio, with a Bachelor of Science in Education and received a Master in Public Administration from the Harvard University, John F. Kennedy School of Government.

Under Secretary for Science and Technology: Dr. Charles E. McQueary

Dr. Charles E. McQueary is Under Secretary for Science and Technology, Department of Homeland Security. Prior to that, Dr. McQueary served as President, General Dynamics Advanced Technology systems, in Greensboro, N.C., a company that focuses on electro-optic under-sea systems, networking and decision support systems, active control systems, signal processing solutions and software solutions.

Prior to General Dynamics, Dr. McQueary served as President and Vice President of business units for AT&T, Lucent Technologies, and as a Director for AT&T Bell Laboratories.

Dr. McQueary holds both a Ph.D. in Engineering Mechanics and an M.S. in Mechanical Engineering from the University of Texas, Austin. The University of Texas has named McQueary a Distinguished Engineering Graduate.

Under Secretary for Information Analysis and Infrastructure Protection: Frank Libutti

The President announced on March 20 his intention to nominate Frank Libutti of New York, to be Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security. Mr. Libutti currently serves as the New York City Police Department's Deputy Commissioner of Counter Terrorism. He previously served as Special Assistant for Homeland Security at the Department of Defense. A retired Lieutenant General in the United States Marine Corps, he was honored with numerous personal decorations during his 35-year military career, including the Defense Distinguished Service Medal, the Distinguished Service Medal, the Silver Star Medal, the Defense Superior Service Medal, as well as a Purple Heart. Mr. Libutti is a graduate of The Citadel–The Military College of South Carolina.

DHS Who's Who

Assistant Secretary for Infrastructure Protection: Robert P. Liscouski

Mr. Liscouski is the Assistant Secretary of Homeland Security for Infrastructure Protection, having assumed the post in March 2003. He is responsible for the Department's efforts to identify our critical infrastructures and propose protective measures to keep them safe from terrorist attacks.

Prior to returning to government service, he was the Director of Information Assurance for The Coca-Cola Company, responsible for the development and guidance of information security strategies across the enterprise and for conducting research on new business technology vulnerabilities and risk mitigation strategies.

Mr. Liscouski is a member of the Director of Central Intelligence Advanced Technology Panel, a panel comprised of industry representatives providing expert advice, consultation and analysis on scientific, technical and engineering matters to the Director of Central Intelligence (DCI) and to the senior leadership of the Intelligence Community on scientific, technical and engineering matters.

Mr. Liscouski's government experience includes 11 years with the Diplomatic Security Service of the US Department of State and 5 years criminal investigative experience as a homicide and narcotics investigator in Bergen County, NJ.

Mr. Liscouski received his BS degree in Criminal Justice from John Jay College of Criminal Justice in New York, and his Masters of Public Administration from the Kennedy School of Government, Harvard University.

Assistant Secretary for Information Analysis: Paul J. Redmond

Paul J. Redmond is the Assistant Secretary for Information Analysis at the Department of Homeland Security. Mr. Redmond worked 33 years in the CIA's Directorate of Operations serving abroad in East Asia, Eastern Europe, and Europe. At CIA Headquarters he managed operations against the Warsaw Pact. He also served the Director, Central Intelligence (DCI) as his Special Assistant for Counterintelligence and Security.

At the time of his retirement in 1997, Mr. Redmond was the Associate Deputy Director for Operations for Counterintelligence. During retirement, Mr. Redmond was a private security consultant and also served as a consultant to the House Permanent Select Committee on Intelligence. Most recently, Mr. Redmond served as consultant to the DCI as Director of the Intelligence Community Damage Assessment for the Robert Hanssen spy case.

Mr. Redmond graduated from Harvard College, is married to Katharine B. Redmond, and has two grown children.

Under Secretary for Border & Transportation Security: Asa Hutchinson

On January 23, former DEA Administrator Asa Hutchinson was confirmed as Under Secretary for Border and Transportation Security.

As head of the DEA, Hutchinson focused enforcement efforts at top-level drug trafficking organizations, acting at the same time as a national advocate for increased prevention and treatment programs. To that end, he developed the Integrated Drug Enforcement Assistance (IDEA) Program, which combines law enforcement action with community efforts to keep neighborhoods safe and drug-free.

Hutchinson was three times elected to the House of Representatives and, while in Congress, demonstrated strong leadership in the fight against drugs. He served on the Speaker's Task Force for a Drug-Free America, the House Judiciary Committee and the Select Committee on Intelligence.

Prior to his election to the U.S. Congress in 1996, Asa Hutchinson practiced law in Arkansas for 21 years. During that time, he was appointed by President Ronald Reagan as U.S. Attorney for Western Arkansas. Mr. Hutchinson was, at age 31, the youngest U.S. Attorney in the nation.

DHS Who's Who

Under Secretary for Emergency Preparedness & Response: Michael Brown

Michael Brown was confirmed as the first Under Secretary for Emergency Preparedness and Response (EP&R). Mr. Brown will coordinate federal disaster relief activities, including implementation of the Federal Response Plan, which authorizes the response and recovery operations of 26 federal agencies and departments as well as the American Red Cross. He will also oversee the National Flood Insurance Program and the U.S. Fire Administration, and initiate proactive mitigation activities. Additionally, as Under Secretary, Mr. Brown will help the Secretary of Homeland Security ensure the effectiveness of emergency responders, and direct the Strategic National Stockpile, the National Disaster Medical System and the Nuclear Incident Response Team.

Previously, Mr. Brown served as FEMA's Deputy Director and the agency's General Counsel. Shortly after the September 11th terrorist attacks, Mr. Brown served on the President's Consequence Management Principal's Committee, which acted as the White House's policy coordination group for the federal domestic response to the attacks. Later, the President asked him to head the Consequence Management Working Group to identify and resolve key issues regarding the federal response plan. In August 2002, President Bush appointed him to the Transition Planning Office for the new Department of Homeland Security, serving as the transition leader for the EP&R Division. Mr. Brown currently chairs the National Citizen Corps Council, part of the President's USA Freedom Corps volunteer initiative.

A native of Oklahoma, Mr. Brown holds a B.A. in Public Administration/Political Science from Central State University, Oklahoma. He received his J.D. from Oklahoma City University's School of Law. He was an adjunct professor of law for the Oklahoma City University.

Chief Information Officer: Steven I. Cooper

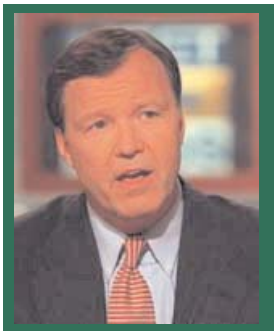
Mr. Cooper was appointed by President Bush to be the first CIO of the Department of Homeland Security in February, 2003. He and his team have responsibility for the information technology assets supporting 190,000 federal employees of the 22 agencies now comprising the new department. They will also continue efforts focused on integrating new and existing sources of essential homeland security information via proven and emerging technologies and in full compliance with our broader values of privacy, civil liberties, and openness.

Mr. Cooper was appointed in March 2002 as a Special Assistant to the President for Homeland Security and served as Senior Director for Information Integration in the White House Office of Homeland Security. In this role, Mr. Cooper launched the development of the National Enterprise Architecture for Homeland Security to address information integration within the federal government and the sharing of homeland security information with state, local, and relevant private sector entities. He fostered partnerships with state and local government and the private sector to assist federal, state, and local initiatives focused on the sharing of law enforcement, public health, and emergency services information. With James Flyzik, Senior Advisor to the Homeland Security Director and former CIO of the Treasury Department, he provided the input for Information Sharing and Systems to the National Strategy for Homeland Security.

Mr. Cooper holds a BA degree from Ohio Wesleyan University, and has held professional certification as a Certified Computer Professional (CCP) from the Institute for the Certification of Computer Professionals (ICCP). He also served in the Naval Air Reserve during the Vietnam conflict. He has been married for thirty years, and his wife, Suzanne, and he have four daughters.

Representative Chris Cox Chairs Select Committee on Homeland Security

On January 9, 2003, Speaker of the House J. Dennis Hastert (R-Il.) selected Rep. Christopher Cox (R-CA) to chair the Select Committee on Homeland Security. Representative Jim Turner (D-TX) is the Ranking Member.



Representative Christopher Cox

"I am honored to serve as the Chairman of the Select Committee on Homeland Security," Rep. Cox said. "In the wake of September 11th, our most important job is protecting American citizens. I will work to make our government more effective in the fight against terrorism. I will ensure that it is done efficiently, and that Congress and the Federal government work together toward this common goal."

The newly-created Select Committee on Homeland Security is designed to coordinate the efforts between Congress and the Federal agencies tasked with protecting our homeland from terrorist attack. The Committee has exclusive legislative jurisdiction over all matters relating to the Homeland Security Act and will be a crucial influence in shaping America's security future.

Chairman Cox brings extensive expertise to bear as Chairman of this Select Committee. He has served as Vice Chairman of the Government Reform Committee, Chairman of the Select Committee on U.S. National Security and Military Commercial Concerns with the Peoples' Republic of China, and Vice Chairman of the Energy and Commerce Oversight and Investigations Subcommittee. For the past eight years, he has also chaired the House Policy Committee, where he also pursued oversight of U.S. policy toward Russia and North Korea.

"Chairman Cox is a superbly qualified leader in the Congress," Speaker Dennis Hastert said. "Overseeing the House implementation of the Homeland Security Department is one of the most important issues before the 108th Congress. I can think of no one better equipped to tackle this challenge."

Representative Jim Turner

Rep. Cox will remain Chairman of the House Policy Committee, a position in the elected leadership of the House he has held since 1994, as well as a senior member of the Energy and Commerce Committee.❖

Rep. Mac Thornberry

The Subcommittee on Cybersecurity, Science, and Research & Development is chaired by Rep. Mac Thornberry (R-TX). Representative Zoe Lofgren (D-CA) is the Ranking Member. The Subcommittee is charged with issues regarding security of computer, telecommunications, information technology, industrial control, electric infrastructure, and data systems, including science, research and development related thereto; protection of government and private networks and computer systems from domestic and foreign attack; prevention of injury to civilian populations and physical infrastructure caused by cyber attack; and relevant oversight.

LEGAL INSIGHTS

by Emily Frye

Cyberspace and the Department of Homeland Security: Goals, Challenges, and What's to Come

Figuring out what's coming down the pike involves no small amount of guesswork - especially in a fast-changing arena like cybersecurity. But the Department of Homeland Security has started to assemble the team of people who will be working on prioritizing and funding these issues, so this is a good time to take a close look at where we are, and where we might be in a few months (or a few years).

To summarize the descriptions that you may find in more complete form throughout this issue of The CIP Report, here's the lay of the land so far: The Science and Technology Directorate within the DHS is headed by Gen. Charles McQueary (Ret.). He is retired from the presidency of General Dynamics Advanced Technology Systems, and has a strong knowledge as well of the telecommunications industry, having served as vice president and president of business units within AT&T and Lucent.

Within DHS, the Information Analysis and Infrastructure Protection (IAIP) section is likely to be most closely involved in setting cybersecurity policy. Frank Libutti is the recently appointed Under Secretary for IAIP. He comes to the DHS from New York City, where he directed counter-terrorism efforts. Prior to working in the counterterrorism field, he had a long and distinguished career in the Marines. Libutti's two deputies are Robert Liscouski and Paul Redmond. Liscouski is in charge of the "IP" component of IAIP. He comes from the private sector, where he was most recently the Director of Information Assurance for Coca-Cola. Redmond had an extended and diverse career in the Central Intelligence Agency.

The mix within the Department will also be flavored by the agencies in its ambit that include cybersecurity research as part of their agendas. Rep. Sherwood Boehlert (R-NY) called a hearing of the Science Committee of the U.S. House of Representatives on May 14, 2003, to evaluate the status of cybersecurity work at the DHS. Boehlert and others in Congress have expressed concern that cybersecurity expenditure and research focus appears to be shrinking rather than increasing, despite growing budget figures for research and development in homeland security.

McQueary's testimony at that hearing indicated that the DHS has begun to confer with the Infosec Research Council (IRC) - a loose affiliation of four other agencies - to help shape and inform its research agenda. The backgrounds of the IRC agency directors provide helpful context in understanding the personalities and politics involved in cybersecurity prioritization.

The IRC's main members are the Defense Advanced Research Projects Agency (DARPA, directed by Dr. Tony Tether), the National Institute for Standards and Technology (NIST, directed by Arden L. Bement), the National Science Foundation (NSF, directed by Dr. Rita Colwell), and the National Security Agency (NSA).

All of these people - McQueary, Libutti, Liscouski, Tether, Bement, and Colwell - are gifted, capable leaders. But they are not cybersecurity professionals.

Identifying Goals and Challenges

To some extent, this experienced management team is not composed of cybersecurity professionals because leadership requires experience, and experience requires time. Achieving senior status in any of these organizations is almost antithetical to the field of cybersecurity: this is a relatively new field with rules that change almost monthly and experts that come and go rapidly. The field has not settled down enough to allow for long-term seniority.

One goal, then, is this: to identify the personnel and proposals that have staying power, and then to incorporate both into the research agendas of the relevant agencies. Not least, those of us interested in the future of cybersecurity must identify which connections and which concepts may be able to bend the ear of leadership.
(Continued, Page 14)

Grants Enable Volunteers to Engage in Homeland Security

Homeland Security Volunteers

Policy makers, state officials, and first responders are not the only ones working on homeland security. Thousands of normal citizens are getting involved through volunteer work to do their part in the war on terror. In July 2002 the Corporation for National and Community Service awarded $10.3 million in competitive grants, funded by Congress, to 43 non-profit and public organizations across 26 states and the District of Columbia. These groups will support more than 37,000 volunteers for local efforts to develop disaster response plans, expand Neighborhood Watch and Community Emergency Response Teams, establish Medical Reserve Corps, train youth to cope with disasters, disseminate information on bioterrorism, and assist ham radio operators and volunteer pilots in responding to disasters.

The Corporation for National and Community Service (CNCS), which is part of USA Freedom Corps, engages more than two million Americans in national service each year through AmeriCorps, Senior Corps, and Learn and Serve America. Homeland security is a new focus for the Corporation, but one that builds on many years of work in public health and safety efforts.

The CNCS encourages relief agencies to organize into "VOADs"-Voluntary Organizations Active in Disaster (for more information on the National VOAD, visit www.nvoad.org). A VOAD is a group of voluntary organizations that collaborate to organize their responses to disaster in order to maximize efficiency and effectiveness and minimize redundancy and confusion. In the hours and days after the attacks of 9/11, thousands of emergent volunteers, people who want to help but don't have prior disaster training or experience, were eager to participate in any way possible. However, many were turned away simply because there were not established plans for coordinating large numbers of volunteers and channeling them into areas of need. Harnessing the resources offered by volunteers is absolutely critical, because a community's many needs during a disaster cannot be fully provided by governmental agencies and established disaster relief organizations. Emergent volunteers can be the "first real responders" for the first few critical hours and maybe even for days along with professional rescue teams and the military.

In the world of citizen action, small things can add up to big things. If you go block by block, eventually you cover a city. If you go city by city, county by county, eventually you cover a state. And if you go state by state, eventually our whole country will be prepared. With our round of homeland security grants, we have the opportunity to refine, speed up, and expand the important work we and you and many others have been doing. If we succeed, we will be doing our part to help win the war against terror.

Leslie Lenkowsky, CEO, Corporation for National and Community Service

Grants in Action

The state of Tennessee's Commission on National and Community Service received one of the grants and awarded a portion of that grant to Volunteer Memphis, an organization that connects people with opportunities to serve those in greatest need. The goal of Volunteer Memphis' grant is to create and implement a disaster response plan which recruits and places emergent volunteers in appropriate tasks or organizations, provides information and assistance to area agencies in need of volunteers and coordinates recovery efforts with other voluntary disaster relief agencies.

Shannon Dixon serves as the Disaster Preparedness Coordinator responsible for carrying out this goal. In collaboration with local disaster relief agencies, Ms. Dixon worked to establish the Memphis Shelby County VOAD in February of this year, and has created a Disaster Response Plan for Volunteer

(Continued, Page 10)

Grants *(Cont. from Page 9)*
Memphis. Part of this plan includes an agreement with the local public television station to act as the Volunteer Reception Center location during a major disaster. Emergent volunteers would be asked to report to this center, where their skills would be quickly assessed and matched to the disaster relief agency in need of those skills. Ms. Dixon is also working with the Mid-South Chapter of the American Red Cross to educate and recruit volunteers prior to a disaster, and to build a database of skills. In addition, Ms. Dixon is collaborating with the Memphis / Shelby

Shannon Dixon is the Disaster Preparedness Coordinator for Volunteer Memphis

County Emergency Management Agency to establish a local council of the Citizen Corps, a FEMA-coordinated program for disaster preparedness and response.

At a fall conference for grantees, Leslie Lenkowsky, CEO of the Corporation for National and Community Service, spoke about the responsibilities of American citizenship: "While we cannot all participate in the fighting, we can all support the cause-not to the same degree as our young men and women in uniform, but with the same intent: to honor the ideals of freedom by becoming better citizens. This is why engaging volunteers in homeland security is so valuable." ❖

THE HOMELAND SECURITY ACT OF 2002

by Robert Almosd, Second-Year Student, George Mason University School of Law

In the immediate aftermath of the 9/11 terrorist attacks, President George W. Bush signed the Homeland Security Act of 2002, consolidating 22 Federal agencies into one Department. The new Department of Homeland Security is intended to protect the homeland from acts of terrorism. The organic act creating the new department was the Homeland Security Act of 2002 (H.R. 5005). Congressman Richard K. Armey introduced the bill on June 24, 2002 on behalf of 118 other Representatives cosponsoring the legislation. Because of the importance of the establishment of the new Department, Congress worked hard to pass the legislation quickly. The Act, on fast track, was adopted by both the House of Representatives and the Senate in five months. The President signed the bill into law on November 25, 2002.

Titles of the Homeland Security Act of 2002

I Department of Homeland Security
II Information Analysis and Infrastructure Protection
III Science and Technology In Support Of Homeland Security
IV Directorate of Border and Transportation Security
V Emergency Preparedness and Response
VII Management
VIII Coordination with Non-Federal Entities; Inspector General; United States Secret Service; Coast Guard; General Provisions
IX National Homeland Security Council
X Information Security
XI Department Of Justice Divisions
XII Airline War Risk Insurance Legislation
XIII Federal Workforce Improvement
XIV Arming Pilots against Terrorism
XV Transition
XVI Corrections to Existing Law Relating To Airline Transportation Security
XVII Conforming and Technical Amendments

The primary purpose of the Homeland Security Act is the establishment of the Department of Homeland Security. The Department is headed by the Secretary of Homeland Security who is appointed by the President. The Act sets up five DHS Directorates and establishes other critical agencies, or transfers entire existing agencies or agency functions into DHS. The Act also creates Under Secretaries to head the Directorates and other leadership positions to oversee the agencies. The Act describes the authorities and responsibilities of these officers.
(Continued, Page 11)

HSA *(Cont. from Page 10)*

Interaction with Nonfederal Entities

Recognizing that information sharing is important not only horizontally within the Federal government, but also vertically between the Federal government and State & local agencies, the Act creates a process for DHS to interact with nonfederal entities. The SAFETY Act, which is integrated into Title VIII of the Homeland Security Act as Subtitle G, is a good example to demonstrate how the Homeland Security Act coordinates anti-terrorism related interaction between the Federal government and private entities.

National Homeland Security Council

An additional achievement of the Homeland Security Act is the creation of the National Homeland Security Council within the executive Office of the President. The primary function of the Council is to advise the President on homeland security matters. The Council consists of the President, the Vice President, and cabinet level officials such as the Secretary of Homeland Security, the Attorney General, and the Secretary of Defense. The President may appoint other officials to the Council.

Information Security

Information security is an important aspect of the legislation. The Department's success depends on the quality and the proper dissemination of the information. To ensure the security of information transferred from one component of the Agency to an internal or external organization, the Act establishes a procedure for sharing information. The procedure includes mechanisms to protect the privacy of personal information. To emphasize the importance of privacy protection, the Act establishes the Privacy Officer, which is the first statutorily defined Federal privacy position in US history.

Department of Justice

Certain provisions of the Act affect divisions of the Department of Justice. For example, the Act renders the Executive Office for Immigration Review under the supervision of the Attorney General. Also, the Act establishes the Bureau of Alcohol, Tobacco, Firearms, and Explosives within the Department of Justice. The Bureau is respon-

(Continued, Page 15)

Supporting Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act)

The purpose of the SAFETY Act is to encourage industry participation in the fight against terrorism by limiting liability of private companies providing the Federal government and other entities with anti-terrorism technology.

Limitations on qualified anti-terrorism technology provider liability include the following:

- Tort claims may not be filed in State courts; lawsuits must be brought under Federal law in an appropriate Federal district court;
- Plaintiffs cannot claim prejudgment interest or punitive damages;
- Plaintiffs seeking pain and suffering damages must prove physical harm;
- If the court finds liability on the part of the technology provider, the damages awarded have to be in proportion with the extent of fault and cannot be more than the liability insurance coverage required by the Act.

To be eligible for SAFETY Act protection, (1) the qualified anti-terrorism technology provider must maintain a liability insurance, (2) the provider must enter into reciprocal waiver of claims with its contractors, subcontractors, suppliers, etc, and (3) the anti-terrorism technology have to be designated as qualified anti-terrorism technology by the Secretary of Homeland Security. To be eligible for the Secretary's approved product list, the technology must meet certain criteria, including:

- Previous use by the Federal government and proof of substantial utility and effectiveness;
- Availability for immediate deployment by both public and private entities;
- Existence of extraordinarily large possibility or risk of third party lawsuits if the product is deployed;
- Possibility that the technology will not be used because of risk of lawsuits;
- Risk to the public if the technology is not used;
- Scientific studies proving the effectiveness of the product;
- The product is able to prevent and respond to terrorist acts.

THE INFORMATION SECURITY WORK FORCE: The New Millennium

by Allan Berg

(This is the final installment of a three part series)

The International Need for IS Workers

Some employers of IT workers are looking to workers from other countries to meet their skill needs. Whether or not to allow larger numbers of skilled foreign workers to enter a country in order to meet employers' demands for more IT and IS workers can be a contentious issue. Throughout the technologically emerging and industrialized nations the IT and IS industry requires more skilled foreign workers to help meet skill shortages. The inability to find workers has limited growth, or in some cases, curtailed growth in the IT and IS industry as well as other parts of the economy that need IS workers. This insatiable need helps drive international work force requirements to meet the needs of international markets. The IS industry needs to be able to attract the best and brightest workers from around the world, and by definition the skilled IS worker will gravitate to market demands, worldwide. The alternative is to move the work to other countries capable of sustaining IT growth and IS at the expense of other nations.

Mid-Career Technical Workers

In the midst of a tight IS labor market worldwide, there are numerous anecdotes of middle-age technical workers having difficulty finding IS jobs. Data from the U.S. National Science Foundation indicate, however, that the employment profile for computer and math scientists closely parallels that of the overall science and engineering work force. It is important to recognize that the IS industry is young and fast growing compared to many other industries and, thus, has a younger worker demographic profile which may contribute to the perception that it is not a hospitable environment for mid-career workers to change careers.

The IS industry is populated by many younger workers. Approximately 75 percent are under the age of 45. Many managers in the IS industry are in their 20s and 30s, and may be uncomfortable hiring or managing older and more experienced workers. Many IT companies having the need for experienced IS workers have operating modes that require long and intense work hours, and mid-career workers, for example those with family obligations, may be assumed to be unwilling to work these long hours (although they may in fact be willing). Some employers may hold the perception that mid-career workers expect higher pay for doing the same work that younger workers do. There is a perception that mid-career workers may not be current with the latest skills, may not be as flexible in doing different kinds of work, and may be less innovative, compared to younger workers. Some employers may have concerns that mid-career workers will cost the company more in insurance premiums, due to age and higher likelihood of having covered family members. On the other hand, many mid-career workers have kept up with the latest skills (or could easily obtain them), are innovative, and are willing to work long hours for market pay rates. Many mid-career workers have a breadth of experience that could benefit many young IT companies. Some mid-career unemployed and underemployed engineers may find difficulty in obtaining employment because they expect higher wages or, while they may be highly skilled and experienced, they may not have the specific technical skills that employers want. On the other hand, it is likely that some mid-career engineers who have appropriate skills and are willing to work at market wages are overlooked because of the perception-not the reality-that older workers cannot do the job. This group must be identified and marketed for training, or retraining in information security.

Temporary and Contract Employees

In an uncertain IT business environment, faced with rapid tech-

(Continued, Page 13)

Work Force *(Cont. from Page 12)*
nological change, many employers seek flexible means of staffing their projects. Employers use independent contractors or temporary workers employed by staffing companies as a mechanism to meet their need for IT and IS workers in this dynamic environment. In the case of contract workers, the workers are not considered to be employees and are responsible, in many cases, for paying their own payroll taxes and unemployment insurance. In the case of temporary workers, the staffing companies are responsible for their employees' wages and legally required payroll deductions, and may provide some benefits as well.

Using either independent contractors or temporary workers has advantages for the employer. Employers can get the specific skills they need for a temporary project without hiring people that might need to be laid off later. Employers can also check out people on a trial basis before deciding whether or not to hire them. And companies do not have to pay (at least not directly) for expensive benefit packages.

Contract or temporary work can also be advantageous to some IS employees. Independent IS contractors with skills in high demand can get paid at a higher rate than most employees, and some workers desire the greater flexibility and variety that can come from temporary or contract work. Temporary work may let IS employees gain invaluable IS work experience that may make them even more marketable in this highly competitive market. On the other hand, many IS employees who accept such arrangements may prefer to have permanent employment. Today, the IT and IS industry has been expanding its use of various types of temporary workers.

The increasing use of temporary workers has implications for the training of IS workers. When a company uses temporary or contract workers, it is generally purchasing skills for immediate use, and has little or no motivation for investing in training for that worker. The incentive and responsibility for investing in training lies clearly with the individual worker, and, to some extent with the organization that manages this temporary worker.

Rapid, Steady Long-term Growth
There can be no disagreement that the numbers of core IT and IS workers in the industrialized nations have grown rapidly and steadily during the past fifteen years. In the United States the numbers of core IT and IS workers are projected to grow dramatically between 1996 and 2006. The Office of Technology Policy's analysis of the Bureau of Labor Statistics' growth projections for this period shows that the number of core IS and IT workers-computer scientists, computer engineers, systems analysts and computer programmers-will grow from 1.5 million in 1996 to 2.6 million in 2006, an increase of 1.1 million. In addition, another 244,000 workers will be needed to replace those exiting these professions. The insatiable appetite and worldwide competition for the skilled IT and IS worker is and will continue to outstrip the worlds' supply.

The Supply of Core IS Workers
What is the composition of the IS work force? What are the primary educational and training pipelines that bring people into the core IS occupations? What is the demographic profile of these occupations? Who is likely to pursue these career fields in the future? Where are the untapped labor pools from which to draw IS workers? What are the educational and training pathways for people seeking to become IS workers? How do we better prepare students moving through various educational pipelines to engage in IS education and training for careers in industry and government? How do we improve existing pathways to better prepare students for an IS career? Where do we find the "right" people to train and to educate? How do we identify and "entice" people who have some or all or the requisite skills to consider retooling of a career in IS? How do we engage older members of the work force in bringing them into the IS work force? How do governments collaboratively engage in developing the new millennium IS worker without jeopardizing their national interests? How can academic institutions and corporate training programs work in a symbiotic fashion, both nationally and internationally, to leverage IS education and training for the IS work force? How do we prepare for tomorrow when we can barely prepare for today? ❖

Insights *(Cont. from Page 8)*
While other agencies and experts certainly offer valuable connections and concepts, DARPA explicitly addressed cybersecurity at the May 14 hearing. Dr. Tony Tether addressed Rep. Boehlert's concern about dwindling investment by noting that, increasingly, cybersecurity-related projects are cloaked in classified garb. Once classified, they are handled through a different budget process; they do not show up as identifiable line items in the same way that unclassified projects do. Dr. Tether's explanation makes it clear that we have a challenge to address here: as more and more projects move into the classified realm, how can the research agencies that are diligently working on cybersecurity challenges assure Congress and the public that progress is being made?

DARPA, as well as the NSA, is focused on defense needs and defense networks. Classifying projects is standard in much of the defense world. This fact highlights another challenge for Critical Infrastructure Protection: protecting defense networks does not protect the 80-90 percent of CIP that resides in the private sector.

What can happen - and is most useful - is that technologies developed first for defense use may be de-classified and commercialized for broad deployment. Firewalls, for instance, originated in the DARPA environment. The NSA has placed a pronounced value on technology transfer to the private sector, as well. These initiatives are essential to disseminating a higher standard of security across the affected networks.
Dr. Tony Tether testified on May 14 that DARPA continues to be acutely aware of cybersecurity needs and includes them under one of its eight strategic thrusts: "Robust, Self-Forming Networks." A related thrust is "Cognitive Computing," which can have an impact on cybersecurity in the long run if computers develop the ability to understand what is happening to them and to operate around detected limitations. Moving these bodies of knowledge into the private sector would help private network operators incorporate a layer of reassurance that is desperately needed.

NIST, also, has been a natural leader in cybersecurity research. Its Computer Security Resource Center has focused on, and made significant strides in, several areas of research seen as key by a broad consensus of knowledgeable experts; it has a well-regarded and productive computer security division. It will probably continue in this capacity. Its Advisory Board has brought both fresh ideas and experienced views to NIST's leadership. Hopefully, DHS will come to a close relationship with the valuable distillation process that NIST has put in place.

What's Next?
As these players continue their work, the plot has thickened: following the departure of Richard Clarke and Howard Schmidt from the White House, cybersecurity as a named interest has suffered from the absence of a focal point. On May 27, 2003, The Washington Post announced that the White House plans to create a new position dedicated to cybersecurity within the DHS, as "an effort to appease frustrated technology executives over what they consider a lack of White House attention to hackers, cyberterror and other Internet threats."

This is an important, although not unexpected, development. At press time for The CIP Report, no candidates had been named. The cybersecurity official is likely to influence policy direction for the rest of the Bush Administration, and - because the DHS itself is so new - may well leave an imprint well into another Administration, regardless of whether it is Republican or Democrat.

The big questions looming over cybersecurity's next steps are: How high a priority? What standards? And who pays? These questions dominate almost all CIP discussions, but they are especially complex in the cyber arena. So far, government has resisted imposing burdensome and expensive regulation on cyber operations. Defining a style that enhances the effectiveness of the private sector's own activities, while refraining from imposing a heavy-handed and inefficient regulatory regime, is a delicate task. A list of ingredients does not a recipe make, but it's a good start. Name this key ingredient - and we'll be able to figure out what we're cooking. ❖

[1]In this context, it is only fair to note that the CIP Project benefits from NIST's funding foresight.

HSA *(Cont. from Page 11)*

sible not only for investigating alcohol, tobacco, firearms, and explosives related violations, but also for instances of violent crimes and domestic terrorism.

Federal Workforce Improvement
The Homeland Security Act creates agency Chief Human Capital Officers and the Chief Human Capital Officers Council to improve the quality of the Federal workforce. These entities are charged with the improvement of agency human resources activities and development of a workforce improvement strategy based on the assessment of the future needs of agencies.

Air Transportation Security
Three provisions of the Act focus on the improvement of air transportation security. First, the Airline War Risk Insurance Legislation amends Section 44302 of title 49 of the US Code extending the termination of certain insurance policies issued by the Department of Transportation to air carriers. Second, the Arming Pilots Against Terrorism Act requires that the Undersecretary for Transportation Security establish a program to train volunteering pilots to become armed Federal flight deck officers to protect passengers and crew in cases of terrorist incidents. Finally, the Act provides for corrections to existing law relating to airline transportation security authorizing the Department of Transportation to retain security related information, increasing civil penalties for security violations, and allowing not only US citizens but also US nationals to become security screeners.

Other Provisions
Other provisions of the Act provide for technical amendments of existing law relating to, for example, the US Secret Service, the US Coast Guard, development of smallpox vaccine stockpile, transferring of certain law enforcement functions, transportation security regulations, biological weapons defense, and railroad and hazmat safety. ❖

Department of Homeland Security Funding for States and Cities

Since Congress passed the FY '03 Budget in February and the FY '03 Supplemental Budget in April, the Department of Homeland Security's Office for Domestic Preparedness has made a significant amount of money available to states and cities to prevent, prepare and respond to terrorism. Nearly $4 billion has been made available to state and local governments to help first responders and offset costs associated with extra security measures.

Grants for States, Cities, Urban Areas and First Responders

- March 7, 2003 - $566 million was made available to the states and cities from the FY '03 budget to assist first responders in the form of funding for equipment, training, planning and exercises.
- March 10, 2003 - $750 million was made available for firefighter assistance grants from the FY '03 Budget to help rural, urban and suburban fire departments better train, prepare and equip themselves.
- April 8, 2003 - $100 million was made available to certain cities as part of the urban area security initiative from the FY '03 Budget to help enhance the local government's ability to secure large population areas and critical infrastructure.
- April 16, 2003 - $165 million was made available from the FY '03 budget to help state and local governments better prepare for all hazards preparedness activities and emergency management.
- April 30, 2003 - $1.5 billion was made available to the states and localities from the FY '03 Supplemental Budget to help state and local law enforcement personnel pay for equipment, planning, training and exercises and to offset costs associated with enhanced security measures deployed during heightened threat periods.
- May 14, 2003 - $700 million was made available from the FY '03 Supplemental Budget as part of the urban area security initiative for 30 cities and their contiguous counties and mutual aid partners to enhance the security of urban areas with high density populations and critical infrastructure, ports and mass transit systems. ❖

State Homeland Security Contacts			
Alabama	James Walker	Homeland Security Director	334-353-0242
Alaska	BG Craig Campbell		907-428-6003
Arizona	Chuck Blanchard	Director of Homeland Security	
Arkansas	Bud Harper	Director, Emergency Management	501-730-9750
California	George Vinson	Special Advisor on State Security	916-324-8908
Colorado	Sue Mencer	Executive Director, CO Dept of Public Safety	303-273-1770
Connecticut	Vincent DeRosa	Dep Commissioner, Division of Protective Services	203-805-6600
Delaware	Phil Cabaud	Homeland Security Director	302-744-4242
District of Columbia	Margret Nedelkoff Kellems	Deputy Mayor for Public Safety and Justice	202-727-4036
Florida	Tim Moore	Commissioner, Florida Dept. of Law Enforcement	850-410-7233
Georgia	Bill Hitchens	Director of Homeland Security	404-624-7030
Hawaii	BG Robert Lee	Adjutant General	808-733-4246
Idaho	MG Jack Kane	Adjutant General	208-422-5242
Illinois	Carl Hawkinson	Homeland Security Advisor	217-524-1486
Indiana	Clifford Ong	Director, Counter-Terrorism and Security Council	317-232-8303
Iowa	Ellen Gordon	Administrator, Emergency Management	515-281-3231
Kansas	MG Gregory Gardner	Adjutant General	785-274-1121/1109
Kentucky	BG D. Allen Youngman	Adjutant General	502-607-1257
Louisiana	MG Bennett C. Landreneau	Adjutant General	225-925-7333
Maine	MG Joseph Tinkham, II	Adjutant General	207-626-4440
Maryland	Thomas J. Lockwood	Homeland Security Director	410-974-3901
Massachusetts	Richard Swensen	Office of Commonwealth Security	617-727-3600x556
Michigan	COL Tadarial Sturdivant	Director of State Police	517-336-6198
Minnesota	Rich Stanek	Cmsnr of Public Safety and Homeland Security	
Mississippi	Robert Latham	Executive Director, Emergency Mgmt Agency	601-960-9999
Missouri	Col. Tim Daniel	Special Adviser for Homeland Security	573-522-3007
Montana	Jim Greene	Administrator, Disaster and Emergency Services	406-841-3911
Nebraska	Lieutenant Governor Dave		402-471-2256
Nevada	Jerry Bussell	Homeland Security Director	775-687-7320
New Hampshire	Donald Bliss	Director, Emergency Mgmt and State Fire Marshal	603-271-3294
New Jersey	Sidney Caspersen, Director	N.J. Office of Counter-Terrorism	609-341-3434
New Mexico	R.L. Stockard	Homeland Security Director	505-827-3370
New York	John Scanlon	Director, Office of Public Security	212-867-7060
North Carolina	Bryan Beatty	Secretary, Dept of Crime Control and Public Safety	919-733-2126
North Dakota	Doug Friez	Homeland Security Coord/Emergency Mgmt Dir	701-328-8100
Ohio	Kenneth L. Morckel	Director of Public Safety	614-466-4344
Oklahoma	Bob A. Ricks	Director, Oklahoma Office of Homeland Security	405-425-2001
Oregon	Ronald C. Ruecker	Superintendent of Oregon State Police	503-378-3725
Pennsylvania	Keith Martin	Director, Pennsylvania Office of Homeland Security	717-651-2715
Puerto Rico	Annabelle Rodriguez	Attorney General	787-721-7700
Rhode Island	MG Reginald Centracchio	Adjutant General	401-275-4102
South Carolina	Robert M. Stewart	Chief, S.C. Law Enforcement Division (SLED)	803-737-9000
South Dakota	Deb Bowman	Chief of Homeland Security	1-866-homland
Tennessee	MG (Ret.) Jerry Humble		615-532-7825
Texas	Jay Kimbrough	Deputy Attorney General for Criminal Justice	512-936-1882
Utah	Scott Behunin	Div Dir, Comprehensive Emergency Mgmt	801-538-3400
Vermont	Kerry Sleeper	Commissioner, VT State Police	802-244-8775
Virginia	John Hager	Asst to the Gov for Commonwealth Preparedness	804-225-3826
Washington	MG Timothy J. Lowenberg	Adjutant General	253-512-8201
West Virginia	Joe Martin	Secretary, Dept. of Mil Affairs and Public Safety	304-558-2930

State Homeland Security Contacts (cont.)			
Wisconsin	Ed Gleason	Administrator, Emergency Management	608-242-3210
Wyoming	MG Ed Boenisch	Adjutant General	307-772-5234
Guam	Frank Blas	Homeland Security Advisor	671-475-9600 / 9602
Northern Mariana Islands	Jerry Crisostomo	Special Advisor for Homeland Security	670-664-2280
Virgin Islands	MG Cleave A. McBean	Adjutant General	340-712-7711
American Samoa	Leiataua Birdsall V. Ala'ilima	Special Assistant to the Governor	011-684-633-4116

CIP PROJECT TO SPONSOR PUBLIC-PRIVATE SECTOR DIALOGUE

The CIP Project is pleased to announce that we are furthering the national agenda of homeland security by leading a high-level discussion this June in Washington. Members of Congress and representatives from DHS and the private sector will participate in a CIP Project-sponsored discussion of priorities, cost, accountability and the roles of government and industry in homeland security. Panelists will include:

* The Honorable Robert Liscouski, Assistant Secretary for Infrastruture Protection, Department of Homeland Security

* The Honorable Christopher Cox (R-CA), Chairman, House Select Committee on Homeland Security

* The Honorable Jane Harman (D-CA), Ranking Member, House Permanent Select Committee on Intelligence

* The Honorable John Hager, Assistant to the Governor for Commonwealth Preparedness (Virginia)

* Mr. John Derrick, Jr., Chairman and Chief Executive Officer, Pepco Holdings, Inc.

* Ms. Catherine A. Allen, Chief Executive Officer, BITS, The Technology Group for The Financial Services Roundatable

* Moderator: Frank Sesno, University Professor of Public Policy and Communication; Senior Fellow, Critical Infrastructure Protection Project

Watch our website, http://techcenter.gmu.edu/programs/cipp.html, in late June for a transcript of this discussion.

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

The CIP Report is published by LegalNet Works, Inc. on behalf of the CIP Project. Formed in 1996, LegalNet Works Incorporated focuses on the development of information security laws and regulations with an emphasis on liability, risk management, national security, regulatory compliance, and privacy. LegalNet consults both government and industry officials on legal and policy reform in these complex areas.

If you would like to be added to the distribution list for The CIP Report, please send an e-mail to cipp01@gmu.edu.