THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 4

OCTOBER 2008
COMMUNICATIONS SECTOR

In this issue of *The CIP Report*, we focus on the Communications Sector. This important Sector encompasses many different aspects of our everyday lives, such as business, technology, emergency response, and it includes many different partnerships. It is abundantly evident the essential role that Communications plays.

GEORGE MASON UNIVERSITY
School of Law
CENTER FOR INFRASTRUCTURE PROTECTION

The first three articles featured are the combined efforts of the leadership of the following organizations: the National Security Telecommunications Advisory Committee (NSTAC), the Communications Information Sharing and Analysis Center (C-ISAC), and the Communications Sector Coordinating Council (CSCC). They provide an overview of how their organizations work within the Communications Sector on critical infrastructure protection issues and how they mutually support each other. A brief overview of the Sector-Specific Plan (SSP) is included, outlining the Sector's security goals. There is also a review of the National Emergency Communications Plan (NECP), which was released July 31, 2008.

This month also marks Cyber Security Awareness Month. We present an article from the National Cyber Security Division of the Department of Homeland Security (DHS) on recommendations that everyone can follow to ensure better cyberspace protection. *Legal Insights* touches upon telecommunications and the need for long-term, high-risk research. Finally, a press release covers the Governor's Technology Award recently presented to James Madison University (JMU).

We hope you find this month's issue useful and we appreciate your continued support and feedback. Please let us know if there is a specific area that you would like us to feature. We would also like to know if there are others we should add to our distribution list for this publication. If so, provide an e-mail address or click here to subscribe.

Mick Kicklighter
Director, CIP
George Mason University, School of Law

National Security Telecommunications Advisory Committee (NSTAC)

For more than 25 years, the National Security Telecommunications Advisory Committee (NSTAC) has brought up to 30 industry chief executives together from major telecommunications companies, network service providers, information technology, finance, and aerospace companies. Together, these industry leaders focus on providing industry-based advice and expertise to the President on issues related to implementing national security and emergency preparedness (NS/EP) communications policy and programs. The NSTAC's goal is to collaboratively develop recommendations to the U.S. Government that will assure communications through any event or crisis and maintain a reliable, secure, and resilient national communications posture. Edward Mueller, CEO of Qwest Communications and John Stankey, CEO of AT&T Operations are the current Chair and Vice-Chair, respectively.

Beyond the combined Communications/IT/Finance industry collaboration, the NSTAC serves as a standard for trusted public-private partnerships, which has resulted in the creation of mutually beneficial information sharing mechanisms and other long-standing programs that reinforce that partnership. One of the first NSTAC recommendations led to the creation of the National Coordinating Center (NCC) as an operational arm of the NSTAC. The NCC later became designated as the Information Sharing and Analysis Center (ISAC) for the Communications Sector, where information relevant to the protection and operation of the communications infrastructure is shared between industry and Government. The NSTAC also helped establish the joint Industry/Government Network Security Information Exchanges (NSIE), which allows representatives from the public and private sectors to share sensitive information on threats to operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. The NSTAC has long recognized that information sharing is the foundation in the industry and Government relationship, and underlies all facets of the NSTAC agenda to ensure robust and resilient national telecommunications services.

Since its inception, the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns. In recent years, the Government, with the support of the NSTAC, has addressed new NS/EP challenges caused by several changing factors: the convergence of traditional and broadband networks, the changing global threat environment, and the continuing global expansion of both provider and user communities. As the domestic and global network becomes increasingly complex, the NSTAC's work, more so than ever, is of vital national importance and the committee remains vigilant in aggressively addressing our Nation's highest priority NS/EP communications needs.

The five key themes of major focus continue to be 1) strengthening national security, 2) enhancing cybersecurity, 3) maintaining the global communications infrastructure, 4) assuring communications for disaster response, and 5) addressing critical infrastructure interdependencies and dependencies. Recent work in these five areas has focused on network security, identity management, international incident management, emergency communications interoperability, access and credentialing, financial services and telecommunication, and electric power interdependencies.

NSTAC publications and reports can be found at http://www.ncs.gov/nstac/nstac_publications.html. ❖

Communications Information Sharing and Analysis Center (C-ISAC)

While the NSTAC tends to address long-term, strategic issues, real partnership is manifested at the operational level. The Federal Government and the communications industry have had a long-standing partnership within the NCC since 1984. The mission of the NCC has been focused on ensuring communications for NS/EP. In response to a recommendation of the President's National Security Telecommunications Advisory Committee, the NCC was created and acknowledged by the President as an ISAC for the Communications Sector. The goal of an ISAC, created by Presidential Decision Directive/NSC-63, is to seek the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships.

The Communications ISAC (C-ISAC) consists of industry members of the NCC and receives the support of the NCC Watch, a 24/7 operations center. The NCC, serving as the ISAC for the Communications Sector, facilitates the exchange of vulnerability, threat, intrusion, and anomaly information affecting the communications infrastructure among Government and industry participants. The NCC Watch monitors events, tracks action items, and disseminates alerts and warnings. Regular operations include a weekly meeting with all Government and industry members to share information on threats or incidents and discuss issues. During emergency operations, daily meetings are held with Government and industry members who have a role in the current response effort. Recent events including Hurricanes Dolly, Gustav, and Ike are examples of industry and Government partnering together to obtain situational awareness of communications impacted by the hurricanes and capturing lessons learned to be incorporated into future response efforts. As an extension of these efforts, Communications Sector members' companies are integrated into the National Response Framework through Emergency Support Function 2.

Since September 11, 2001, the NCC has experienced a significant increase in membership, expanding from 16 to 50 private sector companies. The industry presence in the NCC is composed of resident representatives who provide on-site support to the government, as well as the nonresident representatives. Membership includes wireless, wireline, cable and satellite companies, broadcasters, equipment manufacturers, systems integrators, and associations.

For more information on the NCC/C-ISAC, please visit http://www.ncs.gov/ncc/. ❖

Communications Sector Coordinating Council (CSCC)

The Communications Sector Coordinating Council (CSCC) is distinct from the C-ISAC, which is operationally focused, and the NSTAC, which is chartered to provide Presidential-level recommendations on issues pertaining to NS/EP communications, because it works to encompass all aspects of the Sector. These three organizations coordinate closely with each other to avoid duplication of effort and to maximize positive sector outcomes.

The CSCC was created in 2005 and is designed to build upon the Communications Sector's collective strengths and experience in addressing critical infrastructure protection policies. The broad purpose of the CSCC is to foster and facilitate the coordination of sector-wide initiatives designed to strengthen the physical and cyber security of the Sector's critical assets. Additionally, the CSCC serves to enhance information sharing within the Sector, across sectors, and with the Department of Honeland Security (DHS). Through the CSCC framework, private sector owners, operators, and suppliers can engage DHS and other federal agencies to more effectively advance the following:

- Identify, prioritize, and coordinate policy issues related to the protection of critical infrastructure and key resources
- Facilitate the sharing of information related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices
- Address policy issues related to response and recovery activities and communication following an incident or event

The Communications Sector has evolved from a predominantly closed, wireline and microwave telecommunications network focused on providing equipment and voice services, into a diverse, open, highly competitive, and interconnected industry comprised of companies using diverse technologies, services, routes, connectivity, and vendors to provide voice, video, and data services to customers. In addition, private, internal communications systems provide an integral role to critical infrastructure/key resources (CI/KR) functionality. In recognition of the industry changes, the CSCC membership is broadly representative of the Sector and consists of 40 members from the wireline, wireless, broadcast, cable, satellite, equipment, and the system integrator industries.

CSCC officers are elected annually as well as four at-large voting members and two non-voting members. Non-voting members include a representative from the C-ISAC and the Information Technology Sector Coordinating Council (IT-SCC), who serves as liaison to the Communications Sector and a representative of the CSCC who serves as a liaison to the IT-SCC.

Government stakeholders are invited to meet jointly with industry members at the CSCC quarterly membership meetings. In addition, CSCC Committees meet as necessary to advance the organization's work plan. When a policy issue requires examination, the Executive Committee assigns it to one of the CSCC operating committees.

The following are a few of the CSCC's acommplishments:

- Researched and developed critical infrastructure protection priorities,

(Continued on Page 11)

Overview of the Communications Sector-Specific Plan

The Communications Sector released its Sector-Specific Plan (SSP) in May 2007. The SSP includes security goals, a risk assessment framework, and roles and responsibilities within the Sector. It also identifies the Communications Sector's industry and government partnerships, federal relationships and key entities, emergency response organizations that include local and State relationships, as well as international relationships.

The Sector also has many interdependencies with other sectors. Some of these sectors include: Banking and Finance, Chemical, Defense Industrial Base, Emergency Services, Energy, Food and Agriculture, Information Technology, Postal and Shipping, Public Health and Healthcare, Transportation, and Water.

The SSP outlines the benefits of the plan. It also describes the need for both private and public sector participation in order to achieve the goals set out by the plan. Ultimately, the goal is to better protect the Nation from any event that could damage, disrupt, or destroy the systems, networks, and functions of the Communications Sector.

For more information and to view a copy of the Communications SSP, please visit http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf. ❖

Vision Statement

The Communications Sector acknowledges the Nation's critical reliance on assured communications. The Communications Sector will strive to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster.

Security Goals

1. Protect the overall health of the national communications backbone.
2. Rapidly reconstitute critical communications services after national and regional emergencies.
3. Plan for emergencies and crises by participating in exercises and updating response and continuity of operations plans.
4. Develop protocols to manage the exponential surge in utilization during an emergency situation and ensure the integrity of sector networks during and after an emergency event.
5. Educate stakeholders on communications infrastructure resiliency and risk management practices in the Communications Sector.
6. Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decision-makers in the sector.
7. Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness, and cross-sector incident management.

National Emergency Communications Plan

The failure of communications equipment and systems during major emergencies, particularly events like 9/11, has been widely accepted as a critical flaw in our Nation's defense and response infrastructure that needs to be remedied. A great deal of policy papers have been written and funds have been expended to try and resolve the problems with the current emergency communications systems. Toward remedying this issue, DHS has released the National Emergency Communications Plan (NECP).

The NECP represents an overarching strategy to coordinate and guide efforts to improve the communications systems used by emergency responders at all levels of government. The ultimate goal is for 75 percent of all jurisdictions to demonstrate response-level emergency communications within three hours of a significant incident. The NECP contains a roadmap delineating the route from today to the goals in the next five years. It focuses resources on creating formal governance structures and clear leadership roles, on coordinating federal activities, on drafting common planning and operational goals, on setting standards for emerging technologies, on improving emergency responder skills and capabilities, on planning for a communication system's lifecycle, and on the bottom line, which is an improved disaster communications capability.

These goals will help guide, though not control, the distribution of homeland security funds towards communication. The idea is to create operable communications systems and gradually link them together into a larger system. Two systems are considered fully interoperable when they have shared forms of: governance, standard operating procedures, technology, training and exercises, and are used in the same basic fashion. A series of reports will be issued over the coming years to indicate progress towards these goals and to see if established milestones are being met.

This process does not lack challenges. The Plan indicates the following as obstacles that need to be overcome for truly effective interoperable emergency communications to exist:

- In many cases, emergency response agencies are unaware of (or have yet to adopt and integrate) national-level policies that define roles, responsibilities, and coordinating structures for emergency communications.

- State Interoperability Executive Committees (SIEC) or their equivalents do not have uniform structures, they typically act in an ad hoc capacity, and they often lack inclusive membership.

- The Nation does not have an objective, standardized framework to identify and assess emergency communications capabilities nationwide. Thus, it is difficult for jurisdictions to invest in building and maintaining appropriate levels of operability, interoperability, and continuity of communications.

- Emergency communications strategic planning efforts vary in scope and often do not address the operability and interoperability concerns of all stakeholders.

- Many agencies often do not consider communications planning to be a priority and therefore do not allocate resources for participation in planning activities.

- There is a need for greater Federal department and agency participation in State, regional, and local governance and planning processes.

- Many States do not have full-time statewide interoperability coordinators, or equivalent positions, to focus on the activities needed to drive change.

This work is just one of many steps in a larger journey. Laying out a series of goals and a rough framework for meeting those goals, as well as some attempts to measure progress, is an encouraging sign. It remains to be seen if this will actually take place, as the vagaries of policy-

(Continued on Page 11)

Cyber Security is Our Shared Responsibility

by the National Cyber Security Division, Department of Homeland Security

The term "personal computer" just doesn't mean what it used to a few years ago. Wireless and high-speed broadband Internet access has turned once isolated "personal" desktop machines into networking dynamos. Everything from globe-trotting laptops to home servers are now connected to far more sources of input then just one person. Today's computers crunch zeros and ones that grow and process food, purify and supply water, produce energy, balance checkbooks, connect the phone lines, bring news and information to the public, and dispatch emergency services. Tomorrow the very same laptops and computers could easily turn over the shop keys to some anonymous hacker, criminal, or terrorist who gains access from around the block or across an ocean. That is, if they haven't already.

This October marks the fifth annual National Cyber Security Awareness Month, another milestone in the U.S. Department of Homeland Security's effort to raise awareness about cyber risks to our security and economic prosperity. October is the time of the year when we look to focus educational efforts on improving Americans' understanding about the consequences of unsafe computing practices, and the importance of protecting computers at home and at work.

Cyber security has become serious business in the increasingly networked world. These interconnections today mean that cyber security is a shared responsibility for all Americans. Just as the opportunity of living in a democracy carries with it the responsibilities of citizenship, so does being a part of the on-line world require commitment to responsible use. Democracies fail without the active participation of their citizenry. Cyberspace fails when hackers and criminals are allowed to navigate our systems with impunity. The government can't secure cyberspace alone. Neither can banks, schools, favorite social networking sites, or utility companies. And individuals can't secure their cyberspace alone either.

No one is powerless, however. What people can do is recognize their role in cyberspace protection, and take action in securing their own computer. And they can be confident that the effects of their actions will spillover to their friends and co-workers. Following some basic rules is important because most successful cyber attacks aimed at organizations large and small are the result of errors, many of them careless, by well-intentioned employees. In order to protect both information and critical infrastructure the following is a recommended comprehensive, multi-step approach:

1. **Be on the lookout for "phishing" scams.** Never open unsolicited or unknown email messages. Never reply to or click on links in messages asking for personal information, especially social security numbers.

2. **Be an ambassador for cyber security.** Educate yourself with tips and advice from www.StaySafeOnline.org. Print cyber security posters from www.OnGuardOnline.gov and post them in workrooms, hallways, bathrooms and other employee gathering places. Print and post cyber security tips near your computer in a prominent location.

(Continued on Page 12)

Legal Insights

Telecommunications Infrastructure R&D: U.S. Remains World Leader But Further Erosion Threatens National Security

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

The United States remains the world leader in telecommunications infrastructure development and deployment. Telecom deregulation has unleashed a strong current of innovation with new technologies and new companies rapidly bringing products to the market. This has created wealth and spawned new global industries in wireless, broadband, and satellite communications. The Communications Sector is extremely dynamic and robust with small, medium and large companies competing globally in both manufacturing and services. This competitive environment has had tremendous benefits for consumers, lowering prices and increasing choices.

A major concern in the Communications Sector however is the need for more long-term, high-risk research in the United States. Among all the CI/KR sectors, the Communications Sector is R&D intensive — dependent on continual technical innovation and advanced research for growth. Relative to other critical infrastructure sectors such as energy, transportation, agriculture or health care, federal investments in telecom research and development (R&D) have been modest. This is due primarily to the telecom industry's history as a largely vertically integrated, regulated monopoly where industry basic R&D was subsidized. Traditionally there was less need for major federal long-term basic research spending in this Sector. As a result U.S. academic research programs in telecommunications — the primary performers of U.S. basic research — are relatively small compared with energy or agriculture, for example.

Many experts in the information and communication technology (ICT) field have been sounding the alarm bells for U.S. industry ICT research since the demise of Bell Labs in the mid-1990s. Prior to telecom restructuring in 1984, U.S. industry sectors invested strongly in R&D across all areas of technology, especially high-risk basic research. Post-restructuring, industrial support for such research has declined, become more short-term in scope, and become less stable. This decline in long-term, high-risk R&D is borne out of data from the Organisation for Economic Co-operation and Development (OECD) which shows that U.S. R&D investment in ICT manufacturing dropped substantially from 1997 to 2005 as a share of gross domestic product (GDP).

In the current highly competitive marketplace, most companies are focused on short-term product development. Mergers and acquisitions in the Communications Sector also contribute to this short-term focus as companies simply use acquisitions to obtain technologies rather than investing in research. Telecommunications products and services are now a commodity business and with lower labor costs and reduced technical barriers to entry, foreign competition is strong within the Sector. Adoption of next-generation wireless technologies in many emerging countries have given European wireless giants Nokia, Vodafone, and Eriksson strong competitive advantages over U.S. providers and manufacturers.

This competitive environment has spurred other nations in Europe and Asia to invest heavily in ICT research. Nations such as Korea, Finland, Sweden, and Japan substantially increased their R&D spending in the Communications Sector. Europe is planning major investments in ICT R&D — ICT is one of the key themes of the E.U.'s Seventh Framework Programme (FP7) for Research and Technological Development, with plans to fund over €9 billion euros in research across the E.U. from 2007-2013. Also, according to the Telecommunications Industry Association (TIA), many other OECD countries now offer much more generous tax incentives than

(Continued on Page 9)

Legal Insights *(Cont. from 8)*

the U.S. for both basic and applied research.

Today, major ICT industry-government cooperative research centers and partnerships have been established in India, China and across Europe. The world-wide R&D environment has lowered innovation costs and enabled more robust innovation across the industry. However, this global shift away from the United States to Europe and Asia has serious implications for U.S. national security and homeland security. The U.S. telecommunications industry faces major security pressures while operating in the highly competitive global commercial marketplace. Industry must maintain network security and robustness despite demands countervailing consumer demands for better performance and new features. Use of foreign-produced communications infrastructure or commercial-off-the-shelf (COTS) products has risen, significantly increasing security risks for the U.S. military and critical infrastructure owners and operators. At the same time, the frequency, sophistication, and severity of cyber-attacks are rising dramatically.

A 2006 report by the National Academy of Sciences (NAS) asserts that a decline in U.S. long-term research in ICT has become a threat to national and homeland security. According to the NAS, loss of U.S. technical leadership in the ICT sector poses major security risks including: 1) U.S. dependence on foreign sources of technology to meet critical defense needs; 2) loss of exclusive or early access to state-of-the-art communications technology; 3) loss of know-how to employ state-of-the-art technology; 4) opportunities for other nations to introduce security holes into equipment and networks; and 5) loss of technical capability for cyberdefense.

Congress has sought to increase investments in basic ICT research primarily through the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA). The America COMPETES Act (P.L. 110-69) sponsored by Congressman Bart Gordon (D-TN) was passed into law in 2007. The legislation included a $200 million authorization over three years for a program of basic research in advanced information and communications technologies at the NSF. Areas of research under the program include: affordable broadband access; wireless technologies; network security and reliability; communications interoperability; networking protocols and architectures, including resilience to outages or attacks; trusted software; privacy; nanoelectronics for communications applications; low-power communications electronics; and implementation of equitable access to national advanced fiber optic research and educational networks in noncontiguous states.

Advanced telecommunications infrastructure — made possible by research performed over the last several decades — is an essential element of the U.S. economy and society. According to the NAS, it takes nearly ten years on average for new ICT basic research concepts to come to market. This long time horizon, combined with a decade of decline in telecommunications basic research makes the possibility of "eating the seed corn" very real for the Communications Sector. This puts future U.S. leadership in telecommunications technology and by extension, U.S. national security at risk.

References:

National Science Board, Science and Engineering Indicators 2008, "*R&D in the ICT Sector*" Chapter 4, http://www.nsf.gov/statistics/seind08/c4/c4s.htm#c4sb12.

OECD Science, Technology and Industry Scoreboard, "*R&D in selected ICT industries*" E-14, 2007, http://caliban.sourceoecd.org/vl=1568477/cl=23/nw=1/rpsv/sti2007/e-14.htm.

Report of the National Academy of Sciences, *Renewing U.S. Telecommunications Research*, http://www.nap.edu/catalog/11711.html.

Statement of Jack Keil Wolf, Stephen O. Rice Professor, University of California at San Diego; Vice President, Technology, QUALCOMM Inc. before the Committee on Commerce, Science and Transportation, U.S. Senate, April 24, 2007, http://www.commerce.senate.gov/public/_files/testimonyofJackKeilWolf24April2007SenateCommerce.pdf.

(Continued on Page 11)

JMU Presented the Governor's Technology Award

Below is a copy of the James Madison University Institute for Infrastructure and Information Assurance press release "JMU Institute and Partners Win Governor's Technology Award," dated September 9, 2008.

HARRISONBURG — A computer program that can help hospital administrators manage the level of patient care during flu pandemics and other health crises has received a governor's award for innovation.

John Noftsinger being presented the award by Governor Tim Kaine

Developed by the Institute for Infrastructure and Information Assurance (IIIA) at James Madison University (JMU) and the Augusta Medical Center, the program received the Governor's Innovative Use of Technology in Higher Education Award. Gov. Tim Kaine presented the award Monday, September 8, at the Commonwealth of Virginia Information Technology Symposium in Williamsburg.

"It is an honor to receive the Governor's Technology Award. This recognition is a testament to the true partnership between James Madison University, Augusta Medical Center and the Virginia Department of Health to address planning and preparedness issues impacting the Shenandoah Valley. The innovative work of our faculty and student team has provided a model for future collaborative opportunities," said John Noftsinger, Vice Provost for Research and Public Service at JMU and Executive Director of IIIA.

The software enables hospital management to understand the ramifications of a patient surge. Hospitals can use the model to explore different patient surge scenarios and the impact a surge can exert on the standard level of care. For example, when do caregivers reduce the number of hours of care per patient in order to provide coverage to a larger population of sick?

IIIA developed the model based on extensive research into flu pandemics of the past. The model incorporates statistical information that includes trends over time. Four scenarios were created to aid with hospital decision making. Three of the scenarios are grounded in historic data: the 1918 Spanish flu, the 1957-58 Asian flu, and the seasonal flu. The fourth scenario is a hypothetical pandemic flu scenario based on the Centers for Disease Control and Prevention flu severity index.

Following a successful demonstration of the modeling tool's capabilities and methodology, the IIIA-AMC partnership expanded to include the Virginia Department of Health.

CSCC *(Cont. from 4)*

- Created a Communications Sector-Specific Plan which describes a colloborative effort among the private sector, Federal Government, and State governments to protect the Nation's communciations infrastructure,
- Completed a National Communications Sector risk assessment which aids the identification of critical assets against specifc threats,
- Developed a Communcations Pandemic Influenza Planning Guideline for owners and operators throughout the Sector, and
- Hosted a Pandemic Influenza planning Webinar with the IT-SCC.

The Communications Sector understands the degree to which the Nation relies upon its infrastructure and services, and has a long history of developing the processes and implementing the protocols and best practices which have led to the robust services we enjoy. The NSTAC, NCC/C-ISAC, and CSCC are the three foundational organizations which best allow this Sector to advise the Government on NS/EP issues, collaborate with DHS and other CI/KR sectors on issues to further assure our infrastructure's physical and cyber security, and to respond operationally when the need arises to ensure that the services the Nation relies upon are restored most efficiently. These mechanisms have evolved, matured, and improved over the past 25 years and there is no doubt they will continue to evolve as we deepen the partnerships between the Government and our fellow CI/KR sectors.

For more information on the CSCC, please visit http://www.commscc.org or correspondence may be submitted to commsc-ec@tiacomm.org. ❖

NECP *(Cont. from 6)*

making are bound to affect a goal set for the first year of the Presidential term following the next one. As the NECP states, "Ultimately, the NECP's goals cannot be achieved without the support, dedication, and commitment of the stakeholders who have been involved in developing this plan."

A copy of the NECP is available at, http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf. ❖

Legal Insights *(Cont. from 9)*

Telecommunications Industry Association, *Investing in Communications for Tomorrow's Innovations: the Case for Increased Communications Research Funding*, http://www.tiaonline.org/gov_affairs/issues/research_competitiveness/documents/TIAComResearchFunding-Final.pdf.

The America COMPETES Act (P.L. 110-69), http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR02272. ❖

Cyber Security *(Cont. from 7)*

3. **Keep your computer protections up to date.** Install anti-virus software that removes or quarantines viruses, and anti-spyware software that can undo changes spyware makes to your system. Make sure your firewall is on and set up properly. Update these monthly if they do not update automatically.

4. **Get to know your IT department.** Ask IT security specialists at your work to report any potential cyber incident, threat, or attack to the United States Computer Emergency Readiness Team (US-CERT) at 1-888-282-0870 or US-CERT.gov.

5. **Back up important files.** If you have valuable files stored on your computer, copy them onto a removable disc, and store it in a safe place.

6. **Use strong passwords.** The strongest passwords are complex ones that combine numbers, upper and lower case letters, and symbols. A good trick is to turn a favorite phrase into an acronym. Something like Wdmpn2btc? — **W**hy **d**oes **m**y **p**assword **n**eed **t**o **b**e **t**his **c**omplicated? — works fine. Change your passwords monthly. If you write them down, keep them somewhere far away from your computer. If you are a supervisor, email employees reminders to change their passwords.

7. **Subscribe to the National Cyber Alert System from US-CERT.** Through the Alert System, you can receive timely information about current cyber security problems to protect computers. This information includes weekly bulletins with summaries of new vulnerabilities, patch information when available, and tips on common security topics, such as privacy, email spam, and wireless protection. Sign up at www.us-cert.gov.

Awareness Month is a signature event for the Department, one we plan and look forward to all year long. Working with our partners in both the public and private sectors, we organize events, speak to audiences, and disseminate materials. We recognize that securing your part of cyberspace isn't going to happen overnight. The seven preventative steps above will be a good start, though. While they can seem like an inconvenience, they are far easier than what will be required of you (and us) if your computer is compromised. Even the best information technology staffs cannot make every computer safe without your help. Do your part and make your computer personal again. ❖

The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The CIP Program is funded by a grant from the National Institute of Standards and Technology (NIST).

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

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1