Legal Insights *(Cont. from 14)*

Center (EPIC) filed a Freedom of Information Act (FOIA) lawsuit against DHS to make public details about AIT scanners. As a result, DHS and TSA released hundreds of documents, some of which appear to contradict TSA safeguards. One noteworthy revelation is a TSA procurements specifications document that reveals that the AIT scanners have the ability to store, print, and export images.

In response, TSA clarified that the AIT machines have both a screening operation mode and a test mode. The test mode gives TSA the ability to store, print, and export images but the screening mode does not. TSA asserts that all AIT scanners are delivered to airport checkpoints in screening mode and that there is no way for TSOs to place the machines into test mode. However, FOIA released documents identifying an undisclosed number of "superusers" who have the ability to change AIT scanners from screening mode to test mode.

DHS and TSA need to strictly adhere to the safeguard requirements to ensure the privacy of passengers. TSA should provide constant transparency to ensure safeguards are not breached. Violation of these safeguards, whether voluntary or involuntary, should be dealt with quickly and firmly to maintain passengers' safety, privacy, and trust. Furthermore, TSA should more clearly define how and when AIT scanners will be placed in test mode and whether passengers will be made aware that their image could be stored for training purposes.

Legislative Developments

Congressman Jason Chaffetz (R-UT) introduced a bill in the House to amend 49 U.S.C. § 44901 limiting the use of AIT scanners at airports. The bill prohibits using AIT technology as the "sole or primary method of screening a passenger" and only allows for use of the technology once "another method of screening, such as metal detection, demonstrates cause for preventing such passenger from boarding an aircraft."[7] The bill also requires that passengers are provided information about the operation of AIT technology, the image generated, related privacy policies, and the right to request a pat-down search in lieu of the AIT screening.

Additionally, the Chaffetz Amendment prohibits the storing, transferring, sharing, or copying of AIT -produced images after the boarding determination is made. The bill warns that any officer or employee of the United States who knowingly violates these provisions shall be fined or imprisoned not more than three years, or both. On June 4, 2009 the U.S. House of Representatives approved the Chaffetz Amendment by a vote of 310-118.[8] However, with the Christmas Day bombing scare, TSAs renewed interest in AIT technology, and the President's backing, a vote in the Senate now seems unlikely.

Notwithstanding the passing of the Chaffetz Amendment, TSA is currently expanding the AIT system for use as a primary screening measure to replace traditional metal detectors. Currently, there are 40 millimeter wave units in use at 19 airports and four backscatter units in use at two airports. In March 2010, TSA began deploying 150 backscatter AIT scanners and plans to deploy a total of 450 AITs by the end of 2010. TSA plans to acquire and deploy a total 1,800 AITs.[9]

Emerging Technologies

Privacy and security are often thought of as being on opposite ends of a spectrum, where strengthening one necessarily implies weakening the other. But one emerging technology suggests how technology can shift this paradigm and enhance security and privacy concurrently. TSA is currently testing a new imaging technology that uses thermal-boosted infrared detection to create a temperature differential between clothes and any hidden object, thereby revealing the thermal imprint of any material — plastic, wood, metal, or ceramic powder.

(Continued on Page 19)

[7] Transportation Security Administration Authorization Act, H.R. 2200, 111th Cong. § 215 (2009).
[8] Id.
[9] U.S. Gov. Accountability Office, Aviation Security: TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain (Mar. 17, 2010).

Lessons Learned from Cyber ShockWave

by Maeve Dion
CIPHS Program Manager for Education

Earlier this year, the Bipartisan Policy Center staged *Cyber ShockWave* ('CSW'), a simulated meeting of the National Security Council convened to advise the President about an ongoing, significant cyber incident. This simulation was televised, providing a wonderful opportunity to both educate the public and raise awareness of cyber law and policy concerns. As with many exercises, there were flaws in the technical, operational, and legal premises, which unfortunately were not explained to the viewing public. However, this article focuses on four general observations which may provide some recommendations for future simulations or other education and training programs.

Four General Observations:

I. Security of the information infrastructure relies on a variety of interrelationships among the private and public sectors. These many actors are connected to each other in both informal and formal structures. An incident such as the CSW fact pattern would likely involve entities such as the:

- National Cyber Response Coordination Group (NCRCG), the federal interagency group that coordinates response to cyber incidents and is jointly chaired by the departments of homeland security, defense, and justice;

- Network Security Information Exchanges (NSIEs), structures which facilitate timely sharing of sensitive information among industry and government, focused on cyber threats and vulnerabilities;

- National Coordinating Center for Telecommunications (a public-private sector collaboration), the telecommunications sector's information sharing and analysis center, and its 24/7 watch and warning center (NCC Watch); and more broadly the National Communications System, established in the 1960s and substantially enhanced by executive order in the early 1980s;

- Government Forum of Incident First Response Teams (GFIRST), the Federal government's core cyber incident responders; and

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which presumably would have provided valuable situational awareness as the CSW simulation evolved and impacted the power grid.

Yet none of these entities were incorporated in the CSW simulation, nor were any of them referenced by the participants (the only cyber-specific organization identified was US-CERT). No one mentioned the nascent National Cyber Incident Response Plan currently under development. The simulation was meant as an educational device, not necessarily a replica of a National Security Council meeting, so there was opportunity to identify these entities, or others. Watching the "realistic" and "believable" CSW simulation on television, the American public would be left ignorant of such entities and mechanisms for managing cyber incidents. As the CSW demonstrated, there is a lot of work to be done to clarify legal and policy gaps and improve coordination of cyber incident response and government decisionmaking, but this country is not starting from scratch. Educating the public involves explaining the quality and responsiveness of the current private and public cyber incident response efforts. A proper depiction of the status quo is a necessary foundation upon which to build better structures and organizations.

II. Policymakers are not experts in technology, telecommunications, or the information infrastructure. Specialists and advisors who have this expertise must convey their knowledge to the government decisionmakers in a manner that permits quick and comprehensive

(Continued on Page 17)

Cyber Shock wave *(Cont. from 16)*

analysis. Any public forum should demonstrate properly how this system works. Yet the CSW exercise minimally integrated these experts: occasional updates were provided from US-CERT, and those updates appeared to be overly-technical for the purposes of the CSW National Security Council.

III. During an actual cyber incident, the private sector industries are the first responders, albeit in communication and coordination with the Federal government. This was not sufficiently portrayed in the CSW simulation. As introduced by Wolf Blitzer, this event simulated a real time response to a cyber attack. The average television viewers would be excused the assumption that the telecommunications companies and ISPs were doing very little in response to the incident. At one point, one participant noted that most of the critical infrastructure is privately owned, and that those businesses were "not waiting for us to tell them what to do; they are moving to protect their assets." This would have been a good opening to educate the audience on the collaborative security efforts between industry and government.

IV. Cyber incidents require government decisionmakers to simultaneously focus on all aspects of response, including defensive issues of technical mitigation and public emergency management, as well as offensive actions for potential retaliation or deterrence of future incidents. When an accident or attack results in traditional, physical consequences, the local government and emergency responders manage the defensive actions (providing medical treatment, managing evacuations, controlling public disorder, etc.), and the Federal government focuses on any offensive responses.[1] However, in a cyber incident significant enough to require government action, the Federal government will likely need to manage both the defensive and offensive decisionmaking. The CSW participants showed that the Federal government may not comfortably balance these two efforts, and may instead focus the weight of its attentions on offensive policy decisions. Initially, much of the CSW participants' debate revolved around the President's wartime powers, whether the incident was an act of war, the identity of the perpetrator(s) and potential sponsoring nation(s), and recommendations of how to show the President in a strong, commanding, and confident posture. In fact, one participant could identify no legal authorities for response "without summoning up all of the authorities of a wartime President." Eventually, someone stated a concern that the simulated incident was like "five Category Five hurricanes coming at the United States and we're looking at how we're going to retaliate against the Gulf of Mexico."

Another participant also questioned the war paradigm, asking whether "public safety" authorities provided a legal basis for some of the desired defensive response actions. For future simulations or other public events, it may be helpful to include experts who can comment comfortably on analogous authorities for defensive responses, such as non-wartime public emergency powers and regulatory authorities.

During the live CSW simulation, the room was filled with invited observers from industry, government, media, and academia. The observers mingled before the event and during the break, holding some very interesting, detailed conversations related to the simulation; they eagerly anticipated the post-simulation hotwash, described as an opportunity for the observers to interact with the participants and sponsors. This hotwash would have been a good opportunity to address these four observations and other outstanding questions and circumstances not fully elucidated during the event. The event instead ended with a few scripted questions from Wolf Blitzer and a short moderated discussion among the event sponsors. Future simulations or other education and training programs would do well to include a hotwash or Q&A, incorporating the "extracurricular" comments and conversations that

(Continued on Page 21)

[1] Of course, the federal government also provides support to local and State governments during major disasters, but the generalization still holds that it is the local governments who manage the immediate defensive actions.

VTTI *(Cont. from 6)*

program is:

To address the role of driver performance and behavior in traffic safety. This includes developing an understanding of how the driver interacts with and adapts to the vehicle, traffic environment, roadway characteristics, traffic control devices and the environment. It also includes assessing the changes in collision risk associated with each of these factors and interactions. This information will support the development of new and improved countermeasures with greater effectiveness.

It is estimated that this project will ultimately produce more than 2.5 million hours of driving data as well as very specific crash data. With a wider range of data from the driving population in terms of age, vehicle type, and geographic location, VTTI will be able to explore many unexamined and yet to be determined transportation safety questions.

The CTD also provides management and technical development for vehicle infrastructure wireless communications, fatigue monitoring systems, and enhanced computer vision/imaging systems for VTTI's continuing research efforts.

The CTD continues to develop, test, implement, and maintain multiple state-of-the-art vehicle and infrastructure-based systems to support the research efforts of VTTI. In addition, the world-class wireless communications research conducted at Virginia Tech enables the CTD to uniquely identify and apply emerging technologies to meet the safety, mobility, and operational needs of the U.S. Department of Transportation (USDOT) as well as many states' departments of transportation.

The VTTI is the largest university-level research center at Virginia Tech. The Institute employs more than 225 faculty, staff, and students working on more than 100 projects and is the largest supporter of graduate and undergraduate students at Virginia Tech.

In 1996, the Institute was designated as one of three Federal Highway Administration/Federal Transit Administration Intelligent Transportation Systems (FHWA/FTA ITS) Research Centers of Excellence. Since then, VTTI has grown tremendously and has garnered a reputation as one of the leading transportation research institutions in the nation. In 2005, because of its continued research leadership, VTTI was designated to house the National Surface Transportation Safety Center for Excellence (NSTSCE).

VTTI's cutting-edge research is effecting significant change in public policies in the transportation domain on both the state and national levels. The Institute is dedicated to conducting research to save lives, save time, and save money in the transportation field by developing and using state-of-the-art tools, techniques, and technologies to solve transportation challenges. With invaluable contributions from CTD and its other nine centers, VTTI has earned its unique standing in the transportation research field as a "one-stop-shop" for transportation research, evaluation, analysis, and development. ❖

For more information about VTTI's Center for Technology Development, contact Andy Petersen at apetersen@vtti.vt.edu.

ACAMS *(Cont. from 8)*

Conference, to be held on June 23rd and 24th in Orlando, FL, is an event hosted by the DHS's Office of Infrastructure Protection. This conference helps meet the needs of Federal and State CAPTAP training teams, State Critical Infrastructure Protection (CIP) Coordinators, State Homeland Security Advisors, and other State and local personnel utilizing ACAMS to support their regional infrastructure protection roles and responsibilities. If interested in attending, please contact IICD-Training@dhs.gov for more information.

Legal Insights *(Cont. from 15)*

Most importantly, the imaging system reveals the hidden objects (Figure 3) while eliminating the safety and privacy concerns of other AIT scanners. The Iscon imager uses infrared technology rather than radiation, and images of passengers reveal hidden objects on top off their clothes rather than beneath them. The imaging system is available as both a whole-body scanner portal and as a hand-held portable device.[10]

Figure 3: Iscon

TSA has not yet released any results on the testing of the Iscon system. For the time being, TSA will mostly deploy backscatter AITs and some millimeter wave scanners. This move has been met with opposition from privacy groups and Congress. After the Christmas Day bombing, the deployment of AITs as primary screening devices at airports now seems inevitable. While security and privacy safeguards must be developed and maintained for existing AITs, emerging technologies suggest hope for changing the AIT debate altogether by concurrently strengthening security, safety, and privacy. ❖

---

[10] http://www.isconimaging.com/.

Sensory Technology *(Cont. from 12)*

investment, the long-term maintenance costs associated with batteries makes this initial investment competitive in terms of total costs. However, even if owners become more comfortable with the idea of receiving and using this more constant data stream, there is an additional issue about standards. Adopters were initially reluctant to deploy sensors and generators more widely because they were not sure the technology would continue to be compatible with newer devices or with sensors they might choose to deploy elsewhere. The stakeholders had to come together and agree on a set of universal standards, which lowered the barrier to new customers and gave them a sense that their investment in the technology could be long-term.

Marzano offers some predictions about the future of vibration energy harvesting technology. He thinks the technology is still at the beginning of deployment and could become much more widely used in the next five to ten years. The past five years marked their first breakthrough into the mainstream. Prior to the last five years, there was not as much of a market for remotely powered sensors. Marzano can imagine larger networks of hundreds or even thousands of sensors being deployed in the future over a broader range of infrastructure. The increased amount of data being collected has also led for a need to determine how to manage this data stream and point customers towards only the most important pieces of information, which has spurred new developments in data management and interface technology. These kinds of developments work in tandem to create entirely new systems that can change the face of infrastructure protection as we know it. ❖

Mobile Data *(Cont. from 11)*

being gathered and analysed as part of a new research agenda initiated by the Malaria Atlas Project to quantify human movement patterns in relation to assessment of malaria elimination feasibility.

Malaria elimination requires a significant investment of resources and capacity and, as has been demonstrated twice before on Zanzibar, failure to achieve this ambitious target can lead to fatigue among donors and policymakers and subsequent devastating resurgence of malaria. As more countries across the world make progress toward malaria elimination, there is a need for evidence based and locally-tailored assessments of the feasibility of making the final step in initiating an elimination campaign. With mobile phone uptake continuing to grow around the world, this novel data source has the potential to play a key role in providing such valuable evidence. While 'vulnerability' has been discussed in relation to malaria elimination for decades, the approaches outlined here represent a first step towards finally quantifying it. Replicating and refining these approaches in other areas will enable the development of a standardized methodology for malaria importation risk assessment to aid countries that are considering and planning elimination. ❖

Cyber Shock Wave *(Cont. from 17)*

can only enhance such events. ❖

Articles and Op-Eds on Cyber ShockWave

The Cyber ShockWave event and its aftermath
The Tech Herald

War game reveals U.S. lacks cyber-crisis skills
The Washington Post

Security experts wrestle with cyber-attack scenario
PC World

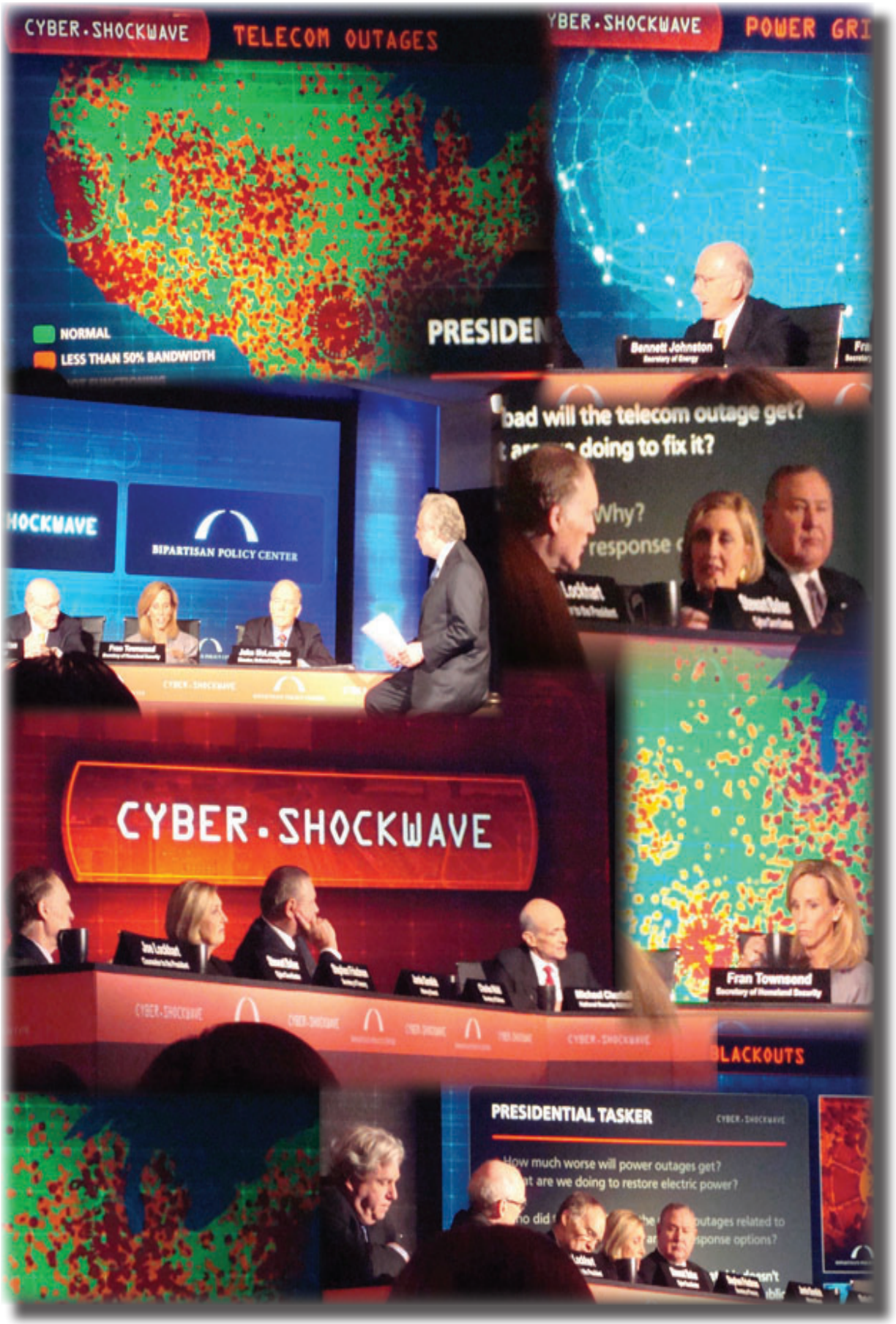
Cyber ShockWave
Marcus Sachs, Director, SANS Internet Storm Center

Cyber ShockWave exposed missing links in U.S. security
Michael Chertoff, former Secretary, DHS

(Continued on Page 22)

Participants	Cyber ShockWave Role
Michael Chertoff Former Secretary of Homeland Security	National Security Advisor
Fran Townsend Former White House Homeland Security Advisor	Secretary of Homeland Security
J. Bennett Johnston Former Senator (D-LA)	Secretary of Energy
John Negroponte Former Director of National Intelligence	Secretary of State
Jamie Gorelick Former Deputy Attorney General	Attorney General
Joe Lockhart Former White House Press Secretary	Counselor to the President
John McLaughlin Former Acting Director of Central Intelligence	Director of National Intelligence
Stephen Friedman Former Director of the National Economic Council	Secretary of Treasury
Stewart Baker Former National Security Agency General Counsel	Cyber Coordinator
Charles Wald Former Deputy Commander of U.S. European Command	Secretary of Defense

Cyber Shock Wave *(Cont. from 21)*



Virtual USA *(Cont. from 4)*

key respects — including in what it is not. It is *not* a Federal mandate that DHS is attempting to impose upon the nearly 60,000 emergency preparedness and response agencies in the United States. Programs which attempt to mandate participation are an anathema to State and local governments and are pretty much a guarantee that a program will fail. Virtual USA is a breath of fresh air in that it is a totally voluntary "opt-in" program in which a jurisdiction makes the decision on whether to participate.

Taking it a step further, Virtual USA, first and foremost, is a practitioner driven program. That is, it is being planned, tested, evaluated, and implemented with State and local agencies as full partners. It is following the very successful model that was used in developing all aspects of the DHS run SAFECOM program for communications interoperability. In that program, all key decisions were made with full participation of the State and local agencies that it was designed to serve. In this case, DHS is working with its pilot states as well as a Strategic Resource Group, which is made up of over 150 State and local practitioners who are subject matter experts and represent every discipline.

Another key part of the Virtual USA program is that it does not require the data owner to give up its data. Instead the data owner totally controls its own data and they decide when they release it and to whom. Moreover, none of the data that is provided is stored anywhere — it is only available for as long as the data owner makes it available.

As a result of all of these key precepts, Virtual USA is having the effect of breaking down the stovepipes that have previously impeded information sharing and is causing a profound cultural and operational shift in how the emergency preparedness and response community does its work. Many of us believe that the impact of this program will be incalculable with the real results being the improved safety and security of our nation. ❖

TCIP *(Cont. from 9)*

attendees to discuss best practices and engage in open dialogue regarding innovative prevention, preparedness, response, and recovery related to a variety of emergency response fields. All participants were encouraged to discuss protocols and solutions to inspire cohesive operations and interoperable communities. Emergency responders were also encouraged to leverage their own experiences in order to develop innovative tools and techniques that will help to secure the homeland.

Planning for the 2011 TCIP Conference is already under way. Please visit www.tcipexpo.com for updates. ❖

The Center for Infrastructure Protection works in conjunction with James Madison Univerity 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 Center is funded by a grant from the National Institute of Standards and Technology (NIST).

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