NOVEMBER / DECEMBER 2004
VOLUME 3, NUMBER 5

THE CIP REPORT

Public Outreach and Education

CIP Program Staff

John McCarthy, *Director / Principal Investigator*

Jerry Brashear, *Associate Director, National Capitol Region Project*

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

Rod Nydam, *Associate Director, Private Sector Programs*

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

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

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.

Director's Message

On a daily basis our colleagues and partners deal with a variety of issues related to critical infrastructure protection, ranging the gamut from cyber security to physical security. While our field has developed vast expertise and ongoing methods of communication and collaboration, we have a monumental task ahead of us in terms of educating the public regarding these same issues.

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Our critical infrastructures maintain our quality and way of life, yet rarely do we as citizens stop to contemplate our reliance upon these complex and fragile systems–until a major event causes a disruption of service and our communities experience an unwanted jolt of reality. While the impact of Hurricane Isabel is slowly fading away, with its many lessons of interdependencies and cascading failures, the planning and lessons learned in our professional community have resulted in improved systems and a greater awareness of providing the public with accurate, timely and potentially life-saving information.

Whether we are facing a single event or a series of disasters, the likes from which Florida is still recovering, or preparing for the possibility of a terrorist attack of an unspecified nature, a prepared, educated and empowered public is our best asset. In this issue of *The CIP Report*, we try to highlight some of those vital efforts to engage and prepare citizens in times of emergency and present some of the strategies and tactics used. Linwood Rose, President of James Madison University, our partner in the CIP Program, submitted an article on higher eduction's role in cyber security awareness. This article was recently published in the *Educause Review*. JMU also recently released their "Education, Planning and Preparedness: A Citizen's Guide," which provides high level information to individuals to better inform them on issues related to cyber security and related crimes, critical infrastructures, planning for disasters and the effectiveness of our national security efforts.

In addition to this piece, we also have portions of testimony that Frank Sesno, Senior CIPP Fellow and Professor of Public Policy at GMU, gave to the House Select Committee on Homeland Security regarding the role of media in providing clear, accurate and responsible coverage in the face of complicated terrorist threats. We include an update on CIPP funded research in GMU's School of Public Policy addressing communications needs during a disaster. We are also pleased to include information on two Federal initiatives. First, the Protected Critical Infrastructure Information (PCII) Program Office is tasked with accepting information from owners or operators of critical infrastructure and distributing this information to appropriate federal, state, and local government entities. Second, we highlight the contributions made to engage and educate the public during the second year of the Ready.Gov campaign by the Department of Homeland Security.

We hope you enjoy this edition of *The CIP Report* and we look forward to continued initiatives of this nature as our field continues to engage the public in efforts to further strengthen the services that our critical infrastructures provide.

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

Covering Terrorism: New Challenges in a New Era

Frank Sesno

Presented before the House Select Committee on Homeland Security

September 15, 2004

Mr. Chairman, I want to thank you and the committee for inviting me here today, and for this discussion about one of the most important challenges relating to the terrorism threat in America: the need for clear, accurate, fast and responsible information. The landscape has changed fundamentally in our post 9/11 world. As we have seen here and around the globe, events can take any number of sinister forms: planes flying into buildings; bombs set off in trains; anthrax sent through the mail; children taken hostage and brutally killed. Weapons of mass destruction take the menace to an almost unthinkable place. Getting information out - communicating clearly with the public - assumes a new and even unprecedented urgency. It is a challenge that confronts all of us: the media, certainly because they will be the conduit for information; the public because citizens must take responsibility to be well informed; government officials and first responders because they will decide what information to release and when, how forthcoming they will be, how much faith they will place in the media and the public to handle that information.

Some say that this 'new normal' requires a new arrangement. They say the news media and government should pursue a 'partnership' to get the job done. That is neither practical nor wise. And it won't happen. The news media have a job to do that requires them to stand aside. They should inform. They should investigate. They should hold responsible officials to account. To do this they must remain independent from those they cover, even against the grim backdrop of terrorism.

It is a challenge that confronts all of us: the media, certainly because they will be the conduit for information; the public, because citizens must take responsibility to be well informed; government officials and first responders because they will decide what information to release and when, how forthcoming they will be, how much faith they will place in the media and the public to handle that information.

That is not to say, however, that there are not common interests and even common responsibilities. Journalists and government officials both serve the public. Both need to be sure the information they disseminate is accurate, credible, timely and relevant. Both must know that they will pay a price if they fail to do their jobs well.

New Responsibility

The news media in this country face a new responsibility and public service prompted by the threats we face. It is a big challenge. And while many news organizations have taken steps to meet the challenge, many have not. News organizations - especially in broadcasting - need to do more before an incident takes place. They need coverage plans so they'll get the story right; they need emergency plans to look after their own personnel; they need contingency plans to continue operating if their broadcasting, publishing or server capacities are damaged or destroyed. And, they need ready access to expertise, critical in the event of an attack. This is particularly true for local television and radio since this is where most people will turn to get practical information and instructions.

How many news organizations have personnel who are knowledgeable about homeland security and can explain what to do in the event of a bio attack - plague, anthrax, tularemia? How many news departments have people who understand the dangers and behavior of *(Continued, Page 3)*

Protected Critical Infrastructure Information Program Facilitates Information Sharing

Protecting critical infrastructure requires timely and useful information. Much of this information is held by private hands and is normally not shared with government entities. Congress enacted the Critical Infrastructure Information Act of 2002 to allow private companies to voluntarily share sensitive or proprietary information, while providing the assurance that it will be protected from public disclosure under the Freedom of Information Act, state and local sunshine laws, and from use in civil law suits.

The Protected Critical Infrastructure Information (PCII) Program Office was created to accept information from owners or operators of critical infrastructure and distribute this information to appropriate federal, state, and local government entities. The PCII Program Office validates submissions to assure the information meets pre-defined criteria for critical infrastructure. This office also assures that any users follow procedures for proper use and safeguarding.

With access to more critical infrastructure information, homeland security and intelligence communities are better prepared to assess vulnerabilities, identify threats, and issue advisories and warnings, thereby preventing disruptions to the nation's economy and citizens' everyday lives. Federal agencies and information sharing organizations are starting to understand the value the PCII Program offers to expand their data gathering and information sharing efforts.

For additional information on the PCII Program visit the Website at: www.dhs.gov/pcii

Sesno *(Cont. from Page 2)* a radiological device - a dirty bomb - and could convey nuanced information to the public? How many newsrooms have a comprehensive, current list of experts who could address the crucial specifics of biological weapons?

Public Expectations

The public expects us to deliver the goods - correctly and swiftly. Yet while citizens say they want more information, they remain largely uninformed about preparations close to home. According to a Hart Teeter poll conducted for the Council for Excellence in Government for a project called We the People: Homeland Security from the Citizens' Perspective, "Despite publicity about new or improved preparedness plans, Americans largely are in the dark about plans for terrorist attacks or other emergencies." Just one in five (19%) Americans say that they are aware of and familiar with their city or town's preparedness plans, and likewise, just one in five (18%) are familiar with their state's plans. Mr. Chairman, the challenge of informing the public is ongoing. If there is terrorism, the news media will be a lifeline: what happened; what is the danger and the risk; where should I go; what routes should I take; will I need medicine; what about my kids; my school; my elderly parents?

This underscores the responsibility that the news media have - a life or death *(Continued, Page 9)*

Frank Sesno is a CIP Program Senior Fellow and a Professor of Public Policy and Communication at George Mason University. He is a former anchor, Senior Vice President, and Washington bureau chief for CNN. He has recently moderated town meetings across the country on citizen engagement in Homeland Security.

Department of Homeland Security Citizen Preparedness Campaign

READY: make a kit, make a plan, and be informed

In early 2003, the Department of Homeland Security, in partnership with The Advertising Council and the Sloan Foundation, launched a national public service advertising (PSA) campaign to educate and empower American citizens to prepare for and respond to potential future terrorist attacks.

READYAmerica
U.S. Department of Homeland Security

The PSAs offer practical suggestions to increase preparedness, including learning about serious threats, making emergency supply kits, creating a family communication plan and keeping emergency phone numbers near the phone. The ads direct Americans to call 1-800-BE-READY to access a free brochure or visit www.ready.gov where they can learn the best ways to protect themselves and their families against terrorism. Every American has a role in strengthening the nation's preparedness.

The campaign seeks to reduce fears and provide information by providing individuals specific actions they can take to protect themselves, their families and their communities in the wake of an attack, or another emergency situation.

Created *pro bono* by The Martin Agency, a Virginia-based advertising agency, the campaign includes television, radio, print, outdoor and Internet advertising. The Ad Council and the U.S. Department of Homeland Security have partnered with various organizations to extend the reach of these critical messages. One key partnership with The Yellow Pages Integrated Media Association provides information about what to do in an emergency in each of its 550 million Yellow Pages directories. Another vital partner, The U.S. Postal Service, distributes preparedness brochures to consumers via their 35,000 post offices nationwide.

Additionally, the Salvation Army distributes preparedness information from their 9,000 retail locations and the American Red Cross provides terrorism preparedness training from their local Red Cross

(Continued, Page 11)

The Ready Campaign's Emergency Preparedness Advice

Emergency Supply Kit:
Start with three days worth of non-perishable food and water. Remember, even if your community is not directly affected by an attack, your life and daily routine may be disrupted. You may need to shelter at home for a couple of days. Roads and stores may be closed - electricity may be turned off - your water supply might be interrupted.

Add flashlights and a battery-powered radio to hear the latest instructions from local authorities. Don't forget extra batteries, a blanket, a first aid kit and medicines, and a manual can opener. Stash away duct tape and pre-measured plastic sheeting for future use. Experts tell us that a safe room inside your house or apartment can help protect you from airborne contaminants for approximately five hours - that could be just enough time for a chemical agent to blow away.

Family Communication Plan:
Make certain that everyone knows how to get in touch, and knows what the emergency plan is for different types of attacks. Every state, every community, every school and every workplace should have an emergency plan. Find out what that plan is and who is in charge. If your school or employer does not have a plan, volunteer to be part of a group to create one. Choose a meeting place, maybe a friend or relative's house, that's well away from your neighborhood. Keep your gas tank half-full. And always make sure you have a set of emergency and contact numbers posted by the phone.

Be Informed and Aware:
Log onto www.ready.gov or call 1-800-BE-READY. In the event of an emergency, listen to local authorities for instructions.

Information Security: A Difficult Balance

Linwood H. Rose, President, James Madison University

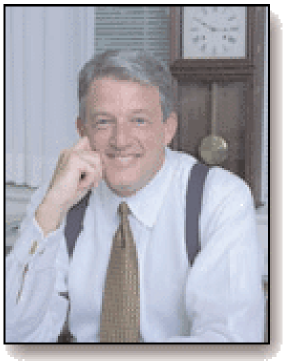
Dr. Linwood H. Rose serves on the President's National Infrastructure Advisory Committee.

Protecting the critical infrastructure of our country is essential to the preservation of our lives as we now live them. My personal interest in this area began somewhat serendipitously, following a meeting with one of our faculty members at James Madison University (JMU). I was intrigued with the work he was conducting on information security. The subject seemed like a natural fit for our new College of Integrated Science and Technology.

Clearly, as scholars, researchers, and educators, those of us in higher education have a key role to play in helping to promote a secure environment for our businesses, our government, our public institutions, and our families.

So I became a "champion" for our efforts in information assurance. I learned what I could, but perhaps most important, I provided encouragement, some additional resources, and visibility for the program. I began to envision that JMU might play a significant role in the nation's efforts against cyber-terrorism when, in January 2000, I stood in the White House Rose Garden as President Bill Clinton signed the "National Plan for Information Systems Protection: An Invitation to Dialogue." Then came the tragic events of September 11, which still haunt us all. JMU lost several talented alumni on that day, and I know the same can be said for many other institutions. Though the 9/11 attack was a physical assault, it was at least partially attributable to imperfections in security systems. In addition, cyber-attacks occur every day. These attacks, not necessarily from terrorists, are designed to detect system vulnerabilities, to acquire or destroy information, and to delay access. Clearly, as scholars, researchers, and educators, those of us in higher education have a key role to play in helping to promote a secure environment for our businesses, our government, our public institutions, and our families.

As a university president, I have awakened to a new reality. The time has come for leaders in higher education to recognize and creatively respond to the opportunity and realities of protecting the national critical infrastructure. To do this effectively, the academy must embrace and implement a vision that is truly interdisciplinary in program development and deployment, balances basic research with applied research and integrates this vision into the curriculum, facilitates technology transfer, is engaged through strategic alliances and collaborative efforts, and balances public interest/national security with individual rights.



Leaders model the way. When my father, a bogey golfer, taught me to play the game, he often said: "Do as I say, not as I do." That won't work in information security. Leaders must have credibility, and that comes from first taking care of business at home. We must all become much more vigilant in the provision of secure systems, in intrusion detection, in rapid response, and especially in education. We must practice, teach, and infuse all aspects of security into our campus lives. The goal is to go beyond reasonable policy and precaution and to assist students and others in the development of what are now essential life skills. We must challenge faculty to move from gaining simple literacy about information assurance to understanding and communicating the necessity and use of information assurance in students' personal and professional

(Continued, Page 6)

Rose *(Cont. from Page 5)* lives.

Information security is no longer a field of study isolated to the computer science department. The need for the understanding and study of information security is pervasive across all academic fields. Political science students need to study the power and influence of information dominance in today's political environments. Business students must study and learn how to treat information security as an integral part of, indeed even a new line of, business.

In addition, college faculty members working in information assurance have a new task in their already overburdened lives: informing and educating administrators and other faculty about the need for fundamental precautions as well as new institutional policies and practices. For example, at JMU a universal information security awareness program has been put in place. Students, staff, and faculty must proceed through a tutorial/quiz to obtain or change a password. The experience is totally online; it is not onerous, but it does require that attention be devoted to information ownership, management, and protection issues. How many colleges and universities have something similar in place?

Achieving a balanced, university-wide approach to solving the information assurance challenge is critical when some researchers are conducting only basic research and others are linked to the private sector through applied research. Too much isolationism or too much commercialism will doom information security efforts. This is not to say that the results of research and development are misguided; it simply underlines the need for a balanced approach to the information assurance challenge for the academy. Some researchers should be encouraged to link up with the private sector-but not all of them.

We also need to admit that this three-legged stool of government, higher education, and business is a bit wobbly.

In addition to the dilemma of balancing basic and applied research, there is the question of the structure of academic programs and the focus on pedagogy in the academy. These factors have a direct effect on information security through the quality of the labor pool working on the problem and the related research activities of institutions. But without leadership-particularly presidential leadership-there will be no reconceptualization of how academic curricula and programs need to be developed. The traditional organizational structure and approach of higher education encourage small-scale, programmatic innovation along the fringes, such as incremental modifications of existing major programs. We are doing better, but if the academy is to make a difference in the information assurance arena, it must bring about systems-level, paradigm-shifting curricular reforms. We must focus on programs, not academic units, and on pedagogy driven by solving problems through research.

Task forces and interdisciplinary teams designed to collaboratively examine threats and opportunities should be used creatively and strategically. Any opportunity that facilitates interaction between people who do not traditionally communicate should be pursued. In their well-intended zeal to establish an information security profession or discipline, colleges should not close the door to political scientists, lawyers, mathematicians, psychologists, and business faculty, who have so much to offer.

Carefully crafted and flexible employment contracts and faculty activity plans that focus energies on mission-supporting activities can also be useful in achieving an effective systems-level intervention. Senior administrators may need to step in when the traditional reward structures leading to promotion, tenure, and improved compensation do not function effectively in today's environment. Within higher education, we must stop talking about collaboration and start practicing it. Collaboration is hard and often inconvenient. It requires give as well as take.

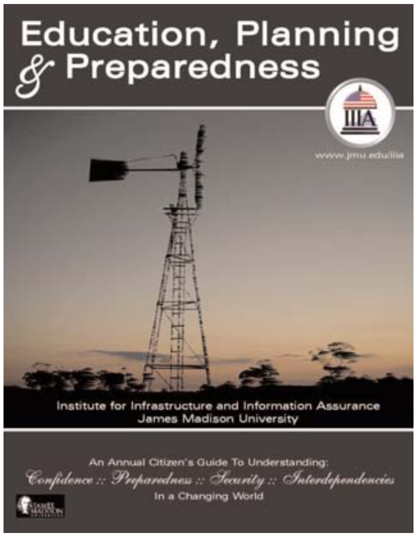
Higher education must also do a better job of setting strategic priorities and must, through negotiation, *(Continued, Page 11)*

James Madison University's *Education, Planning and Preparedness*

A Guide to Understanding: Confidence, Preparedness, Security and Interdependencies

John Noftsinger
Ken Newbold

Our purpose in creating this Guide is to provide information of a practical and digestible nature to citizens, business leaders and decision makers within our nation and state. We endeavor to take complex issues that affect consumer financial stability, personal well-being and quality of life, and present them in a meaningful manner to aid citizens in improving their security and planning. Innate to universities are the research and capabilities that shed valuable light to the issues that threaten the safety and security of the nation. As we, and partner universities, government agencies, and businesses, engage in this research, we recognized the need to provide a public service through the publication of an annual guide which will capture the most emergent and relevant issues within the homeland security arena.


Education, Planning & Preparedness
IIIA
www.jmu.edu/iiia
Institute for Infrastructure and Information Assurance
James Madison University
An Annual Citizen's Guide To Understanding:
Confidence :: Preparedness :: Security :: Interdependencies
In a Changing World

Our goal is to provide a product that educates citizens on issues that, while complex, have direct ties to daily life. In addition to education, our Guide will also serve as a resource to help citizens engage and prepare for situations and events of small and catastrophic disaster. To this goal, the Guide has and will be written with practical purposes, information and resources to help citizens take responsibility for the safety of themselves and their family.

We envision the end user of our Guide to be citizens; however, we realize that we can impact and improve the lives of more citizens by working through established, representative groups. Some of these groups are Congressional and State delegations, local chambers of commerce, citizen's groups, professional organizations and government agencies related to these fields and other established and relevant social networks within the state and community. ❖

The 2004 Annual Citizen's Guide covers the following categories:

Confidence:
- Consumer Financial Information
- Identity Theft
- Spyware/Keylogger programs
- Peer to Peer file sharing
- Solutions to each of these concerns

Preparedness:
- Community Shielding
- Evacuation Planning
- Creating your Preparedness Plan

Security:
- Port Security
- Border Security

Interdependencies:
- Critical Infrastructures and the types of failures they experience
- Interdependencies between infrastructures
- SCADA as it relates to infrastructure reliability

For more information or a for a copy of the guide, please contact Ken Newbold at newbolkf@jmu.edu.

Employing Available Technology to Enhance Communication During Disasters

Roger Stough
Director, Mason Enterprise Center
Associate Dean for Academic Affairs and Professor, School of Public Policy, GMU

There has been a heightened awareness of vulnerability of the U.S. population and its public and private sector organizations following increased terrorist actions over the past several years. Events such as those of September 11, 2001 were shocking to the American public and although vulnerability was perceived as a problem before that event, it had not been held as a critical top priority. In short, the perceived threat of terrorist inspired events dramatically increased, public policy changed and changed quite significantly.

A GMU School of Public Policy research project has shown that the more traditional approach to threat and disaster management, called the institutional approach, has been strengthened and yet at the same time this more top down oriented approach is still not connected in a predictable and meaningful way to the "down" part, i.e., the community and individuals at the community level in roles ranging from resident-citizen to employee, boss and leader.

Our analysis has shown that technology such as ReadyLinks erected on an Internet platform like StargazerNet holds significant potential for improving overall communication among first responders, agencies and citizens in the event of a disaster. The ReadyLinks system is a tool for supporting virtual collaboration and joint information sharing within the first-responder communities and directly and indirectly impacted individuals and organizations. It is a free web-based portal that enables individuals, families, businesses, schools and communities to stay in touch and maintain access to critical news, health and safety information before, during and after an emergency. The technology is simple to use and accessible via any web browser, including public access points in libraries. The platform provides access to vital media and government information all from one convenient location. In addition, users can simply log onto the ReadyLinks website and automatically gain access to a secure message board and conference room, where group members can communicate online to inform each other of their status in the aftermath of any incident.

The ReadyLinks system has been primarily introduced in the Washington Metropolitan area and its usage has been growing steadily. Over the last year and a half, ReadyLinks experienced a significant growth in interest as measured by the number of visits and number of pages visited. This base of interest is expected to grow considerably once new services, such as alert notices, document sharing, publishing, improved security, live news and crucial information streams are added to the existing system. ❖

Sesno *(Cont. from Page 3)*

responsibility. And it underscores the need for elected leaders, government officials, first responders and spokespeople to understand how the media operate and why. This is the era of the never-ending news cycle. We exist in an always-on, real-time world where news is delivered in many ways: on television and radio, in newspapers and magazines, on cell phones and wireless devices, in blast emails and over the Internet.

Just one in five (19%) Americans say that they are aware of and familiar with their city or town's preparedness plans, and likewise, just one in five (18%) are familiar with their state's plans.

In the event of terrorism, officials will have to take this into account, and provide fast and reliable information for a variety of 'platforms' and audiences down the street and around the world. They will not be able to wait to hold news conferences at convenient, pre-determined times. They will have to respond instantly to what is happening on the ground, or quickly knock down the bad information that sprouts like an unwelcome weed.

Learning the Language of Live

Mr. Chairman, in this environment events and information play out live and 24/7. As a result, we get news by increment. Each little development becomes the latest 'breaking news' piece set into the mosaic of the larger story. This can be helpful or it can be a terrible distraction. One of the challenges for news organizations is to make sure incremental news is proportional and provides context.

The advent of incremental news brings with it the danger of 'information lag.' That is the time between when the media ask a question and a responsible official can answer it. That time lag can be minutes or it can be hours. In some cases - such as with certain types of bioterrorism - it may even be days. This truly is the most precarious time in the story process, when uninformed speculation and rumor can fill the information void. This can be a very dangerous thing. We saw this play out during the anthrax attacks of 2001.

It is why news organizations and public officials alike need to learn and appreciate what I call the "language of live.' The "language of live" recognizes the realities of the 24/7 world. It is a transparent language that is deliberate and clear. It explicitly states

(Continued, Page 10)

The Language of Live: What is it and will it help in an emergency?

Bryan Day
Faculty Research Associate, School of Public Policy

When senior fellow Frank Sesno testified before the House Select Committee on Homeland Security in September 2004, he briefly spoke about a concept he calls, the "*language of live*." As Mr. Sesno explained it, this concept describes our new media cycle - one that plays out in real-time, 24/7 - and its new responsibilities.

Understanding the *language of live* can be helpful to those in immediate need of information in the most dire of emergencies. For example, because the horrid events of 9/11 played out live for all the world to witness, the passengers of United Flight 93 were armed with valuable information that caused them to decide to overtake the hijackers. Because the plane subsequently crashed in a field in Pennsylvania, we will never know what additional damage Al-Qaeda might have inflicted upon Americans if these passengers did not have access to the immediate information. However, the *language of live*, if not fully understood, can create danger due to the natural delay of information in today's non-stop media cycle. Mr. Sesno termed this as *information lag*: the time between a journalist’s question and a responsible official’s answer. There are many current examples of this phenomenon. There is the 1996 Richard Jewell incident - the security guard who spent "88 days in hell" as the media all but presumed him guilty of bombing Atlanta's Olympic Park, as well as the 2001 Anthrax incidents of Capitol Hill where the information lag lead to "speculation and rumor to fill the information void." This was neither helpful nor necessary.

The public understands the realities of an always-on media world. The *language of live* does too. The *language* provides a source for all "factual" information. Mr. Sesno sees a media responsibility for "labeling speculation as such and quickly doubling back on bad information to correct the record."

The language of live requires the media to know their "new" responsibility to the public. Today's media - like our government - is a public good. Americans look to the media to provide accurate and timely information and to give direction for their safety during an emergency. While some have suggested that the media and the government form a partnership, "this is neither practical nor wise," according to Mr. Sesno. It is the media's public role to be informative; to examine issues; and to hold accountable those with authority.

Sesno *(Cont. from Page 9)* what is and what is not known, confirmed or corroborated. It directly attributes sources of information. It labels speculation as such. It quickly doubles back on bad information to correct the record. The "language of live" is a language that many journalists employed fluently in the days after 9/11. Mayor Giuliani spoke it as well.

Throughout his many public comments, he sought to avoid offering more information than he had; he did not over-promise; he made it clear when he was answering a question based on incomplete information - or when he couldn't answer at all. He displayed emotion without being emotional. He responded to facts and 'reports' as they developed.

Similarly, news organizations were broadly praised after 9/11 for their measured and purposeful work. There was a responsible attitude, humanity but also professionalism. Questions were asked and answered in a measured way. The information and the tone were straightforward and sober. Most sought to keep speculation to a minimum.

There are some things the "language of live" should not be - especially when we're talking about the coverage of terrorism. It should not be breathless. It should not be hyped. It does not need to be accompanied by sensational graphics or ominous music. The facts will be ominous enough.

Generalist vs. Specialist

News organizations need expertise. Communities will be terribly served by news organizations that 'wing it.' No community in the country - no matter how remote - should consider itself off the hook. A biological attack on the east coast can spread to virtually any town or village because of the way people travel. A cyber attack can affect any home or business in any place. All news organizations should be familiar with and have ready access to appropriate websites, publications, contacts and phone numbers. Smaller news organizations in more remote communities may not be able to afford a homeland security beat, but preparation must be part of their plan.

Call to Action

Mr. Chairman, few people realize how much thought and debate news professionals put into coverage decisions such as these. Most journalists are acutely aware of their responsibilities. They want to do the right thing.

But it's not easy. Many news organizations have experienced deep budget cuts. In a lot of communities, radio stations no longer have any news department at all. Television has too few experienced beat reporters. Local newspapers have been bought up and pared down. The homeland security beat is not one that can be learned in a day.

There are steps that can be taken. News organizations should:

- Be sure they have assembled, are familiar with and can access relevant information from professional organizations, public health, academic and government sources and websites.

- Know the emergency plans and the responsible officials in their community.

- Develop and keep current before an incident a list of sources and experts who can provide accurate and responsible information and/or advise the news organization about facts relating to it.

- Impress upon sources, especially public officials, the need for rapid information in the event of a terrorist incident and why that will benefit the public.

- Understand the "language of live" so that information relating to an unfolding and confusing situation can be conveyed clearly and calmly.

- Train reporters, photographers and staff in matters of personal and family safety; in the event of terrorism, they will be first responders, too, facing all the risks and personal pressures that that implies.

- Consider conducting exercises to simulate a terrorist attack to test the readiness of staff, the editorial vetting process, the reach and redundancy of communications equipment, the coverage plan that would be implemented in the event of the real-thing.

The public will be well served - and the media will be rewarded - by doing it right. ❖

Rose *(Cont. from Page 6)* establish an improved plan for who will do what. College presidents and faculty may have to surrender some of their traditional freedom to pursue research and instruction as they like and instead consider who will contribute the individual components of an integrated solution to information assurance.

We also need to admit that this three-legged stool of government, higher education, and business is a bit wobbly. Examples of higher education and business working together do come to mind frequently. Likewise, government and the private sector have come together, especially after September 11, in discussing the need for a commitment to security in technology products. But there are few examples of the three sectors joining to provide solutions to information assurance needs. That can-and must-happen.

Finally, we have an obligation to consider the balance of public interests and security with privacy and individual rights. When feeling threatened, Americans have been willing to give up some personal freedoms over the past half-century. For example, my parents grew up in a rural society in which doors to homes were locked only when residents were away for summer vacation. Keys were left in auto ignitions overnight, and no one gave a thought to walking alone. But times and conditions change, and now my parents' grandchildren always secure the home and the car and would never think about being out alone late at night. Similarly, in an earlier time, information security precautions might have been thought of as intrusions into personal freedoms, but in today's environment of terrorist threats, they are as sensible as locking the door at night. Opinion polls after the 9/11 attacks have suggested that the public is willing to trade some civic liberties for more personal security.

This willingness must be approached cautiously, however. As the president of an institution named for one of our Founding Fathers, I believe the words of James Madison are instructive: "As a man is said to have right to his property, he may be equally said to have a property in his rights. Where an excess of power prevails, property of no sort is duly respected. No man is safe in his opinions, his person, his faculties, or his possessions." We need all of the resources of the higher education academy to achieve this difficult legal, technological, and policy balance. ❖

Comments on this article can be sent to the author at <roselh@jmu.edu>.

Ready Campaign *(Cont. from Page 4)* chapters. The OAAA (Outdoor Advertising Association of America) and the NAB (National Association of Broadcasters) offered to provide their support by helping to extend the reach of the messages.

Secretary Ridge appears in the PSAs, as do several New York City firefighters, Office of Emergency Management personnel, Port Authority officers and police officers. In the ads, these spokespeople tell Americans that they should not feel helpless or fear terrorism, but instead take simple steps to prepare for possible attacks, just as they do for other potential emergencies. The ads stress the need to "Arm Yourself with Information," which is meant to empower Americans by helping to see that they can take simple steps to protect themselves. ❖

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

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

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