AUGUST 2004 / VOLUME 3, NUMBER 2

THE CIP REPORT

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.

Secretary Ridge talks to CIP Program about Progress, Challenges in National Security

The launching of National Preparedness Month by the Department of Homeland Security in September 2004 represents an opportunity to take stock of the significant changes and efforts underway to improve our national security. Here at the CIP Program, we have been heavily engaged in many of the same issues that DHS will be highlighting during the month's events, such as citizen education, public-private information sharing and cyber-security.

These issues were also paramount in a recent interview of Homeland Security Secretary Tom Ridge by Senior CIPP Fellow and GMU Professor Frank Sesno. Frank's interview provides an opportunity to reflect upon the progress of and lessons learned by a young department, while exploring some of its biggest challenges and future initiatives. The topic sections of this exclusive interview are organized and expanded upon within this month's CIP Report, providing a variety of perspectives and opinions on the issues that arose during their discussion.

Frank Sesno interviews Secretary Ridge

National Preparedness Month is the launch-pad for a second year of citizen education and outreach efforts. These efforts, already in place at many of the fifty organizations participating and supporting the events, include developing educational materials such as the American Red Cross's Guide on Terrorism, the Department of Homeland Security's Ready.Gov website, and media outlets such as the Washington Post's Personal Preparedness Guide. While these materials exist in a variety of formats and cover a broad spectrum of topics, more outreach is needed to a larger percentage of the citizen population to further educate, prepare and engage our citizens.

GEORGE MASON UNIVERSITY | School of Law

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

These efforts to enhance and enable communication, planning and preparedness echo some of the major challenges facing critical infrastructure protection. Communication between public and private sector entities has received a great deal of critical attention and scrutiny during the past year; the successes of these efforts, which make major contributions towards securing our critical infrastructures, often go unnoticed. However, as articulated by Secretary Ridge, the value of this communication and cooperation cannot be overestimated.

We are very pleased to have the opportunity to publish Frank Sesno's interview with Secretary Ridge and share with you the highlights from that important conversation. Included in this issue are also accompanying articles that expand upon the topics discussed within the interview and that relate to National Preparedness Month.

A Discussion with Secretary of Homeland Security Tom Ridge
by Frank Sesno
July 19, 2004

Introduction by Frank Sesno

Homeland Security has become a national preoccupation. In the three years since the attacks of 9/11, we know this: we have entered an era when our geography no longer protects or isolates us from distant enemies who seek the technology and the weaponry capable of inflicting terrible human suffering and vast economic damage.

For the past year and a half, Tom Ridge, the nation's first Secretary of Homeland Security, has had the unenviable task of forging the vast federal agency meant to respond to this new era. He has overseen a government merger of monumental proportions. But he must reach far beyond Washington-to state and local governments, first responders and public health officials, the private sector and university researchers-because thwarting terrorism requires a resilient multi-disciplinary and multi-layered web of coordination and cooperation.

Tom Ridge exudes a quiet concern but a determined confidence that the American people and its government are up to the challenge they now face. Progress has been made, he asserts, though there is much to be done. He is quick to remind people that no open society, no country as big and diverse as this one will ever be 100% secure. There will be more terrorism, he suggests. It is our new reality.

I sat down with Secretary Ridge when we were in Seattle in July at the National Governors Association meeting, where homeland security was one of the principal agenda items. We spoke at length about threats, progress and the importance of research and public communication.

Critical Infrastructure Protection Progress Report

SESNO: You have been in this job since the department was created in March of last year. How would you grade efforts to improve the nation's critical infrastructure?

RIDGE: Generally, I'm very reluctant to grade myself or the department, but I would give us very high marks for moving aggressively in creating a national critical infrastructure list; and [for] taking a multi-dimensional approach for dealing with critical infrastructure to include physical assets, cyber assets that need to be connected to operational assets, in addition to the men and women who work at those particular venues.

SESNO: Where do you think the most progress has been made?

RIDGE: Clearly transportation heads the list because of the extraordinary support of the Congress. Particularly dealing with aviation and the considerable improvements with regard to port security, rail and mass transit. I think air, land and sea transportation are far better positioned [and are] far safer than they were a year and a half ago. *(Continued, Page 4)*

Reaching Millions During National Preparedness Month

Throughout the month of September, hundreds of activities are planned across the country to highlight the importance of individual emergency preparedness. The National Preparedness Month coalition, which includes the U.S. Department of Homeland Security, more than 80 organizations and all 56 states and territories, will encourage Americans to take simple steps to prepare themselves and their families for any possible emergencies.

"National Preparedness Month will give everyone an opportunity to work toward a better prepared America," said Homeland Security Secretary Tom Ridge. "This broad coalition and vast number of activities and events will allow us to reach millions of individuals and inform them about ways they can prepare for emergencies in their homes, businesses and schools."

The more than 80 National Preparedness Month partner organizations will help reach millions of Americans by communicating the simple ways that individuals can prepare for emergencies. Partner activities include:

- The American Red Cross will organize *Together We Prepare* Saturday, September 18 with its chapters nationwide. Chapters are encouraged to sponsor events in their communities such as first aid trainings and preparedness fairs. The organization's website, RedCross.org will also launch an online store in September with new pre-packaged products to compliment the wide range of preparedness resources.

- The America Prepared Campaign has galvanized the private sector in support of National Preparedness Month by providing preparedness information and tools at some of the nation's largest retailers, including Home Depot, Starbucks, Wal-Mart, Costco and Sam's Club. The campaign has also developed public service announcements, which seek to raise awareness about the importance of preparedness and will distribute these starting in September through broadcast, print and outdoor vehicles.

- The U.S. Chamber of Commerce, the world's largest business federation, is participating in National Preparedness Month to help get the business community prepared. The Chamber will distribute emergency preparedness information to its employees nationwide and encourage its members, which include businesses, state and local chambers of commerce, and trade and professional associations, to do the same.

- The National Association of Broadcasters has partnered with the Department of Homeland Security to create *Are You Ready?*, a step-by-step emergency preparedness guidebook for local broadcasters. The guide provides detailed instructions about how broadcasters can prepare their stations for emergencies and get involved in promoting preparedness in their communities. The NAB will make this valuable resource available to all television and radio broadcast stations during September.

- The Department of Homeland Security's National Preparedness Month activities will include initiatives related to the Ready campaign as well as events hosted by Citizen Corps. In September, DHS will build on its Ready campaign, a national public education effort launched in 2003 in partnership with the Ad Council designed to educate and empower individuals to prepare for emergencies by getting a kit, making a family communications plan and being informed about potential threats. *Ready for Business* will be launched to educate small and medium-sized businesses about safeguarding their employees and assets while preparing for business continuity in the event of a disaster. In addition, Citizen Corps, the Department's community-based organization that encourages Americans to volunteer to make their communities safer and better prepared for emergencies, will organize events through its 1,400 state and local Councils across the country.

Events will be held across the country throughout the month. National Preparedness Month partner organizations joined together for a launch on Capitol Hill on September 9 in Washington, DC. ❖

Discussion *(Cont. from Page 2)*
Clearly, in each and every one, there are still additional adjustments to be made, and initiatives and technology to be applied.

Enormous progress has been made in the chemical sector, as well. Most of the major players have started security, vulnerability and liability assessments and have increased investments in protective measures to around three quarters of a billion dollars.

At the end of the day, the challenges for the department, whether it's transportation, the chemical sector or any of the 13 sectors into which we have segmented this $11 trillion economy is to set standards for safety--a template for vulnerability assessment--and then oversee the deployment of either people or technology to make those facilities safer.

SESNO: You mentioned port security. One of the things we hear from critics is that only two, three or four percent of containerized cargo coming into this country is being inspected, and that is inadequate. The numbers change depending on who's talking. What do you say to the critics and to their observation?

RIDGE: Every potential vulnerability with which we are dealing has resulted in a series of layered security measures because, as a department and as a country, we no longer rely on a single point of failure when we are dealing with vulnerabilities. And, I would say to those who question that we are only x-raying five or six percent of the shipping containers that it is just one in a series of protective measures that we have deployed since 9/11. And, again, they're not randomly targeted, randomly searched. They are targeted very specifically, based on information that Customs and the Coast Guard has inherited and developed over the past 20 years.

We require the cargo manifest to be delivered 24-hours in advance before the container can be loaded. We've got a very sophisticated targeting system, and we know a lot about shippers. We know a lot about ports. We know a lot about countries. Depending on the results of the assessment, we now x-ray five to six percent of those before they're boarded on the ship.

We also board 100 percent of "high-interest" vessels. We have extraordinary cooperation with the private sector. In addition, we've got captains at all our major ports and facilities who have been looking into the private sector to assess vulnerabilities and make improvements. So we layer our defense around ports.

SESNO: Much of the critical infrastructure is held by the private sector in this country. How can critical infrastructure protection in the private sector be better incentivized?

RIDGE: We think good security is good business. You always want to secure your supply chain.

SESNO: But it is expensive.

RIDGE: It's expensive. But it is even more expensive if you fail to manage the risk associated with whatever your business enterprise is and if that flow of business is interrupted. Another approach taken is what we call job learning. It makes the big case for companies to invest in the security of their supply chain, their facilities and their assets.

[These companies] have a responsibility to shareholders, to their *(Continued, Page 5)*

FY 2005 Appropriation Bills for the Department of Homeland Security
Transportation Security

	HOUSE H.R. 4567	SENATE S. 2537
Aviation Security	$4,270,564,000	$4,386,083,000
Maritime and Land Transportation Security Grants	$65,000,000	$44,000,000
Transportation Security R&D	$174,000,000	$181,000,000

Secretary Ridge, speaking with Frank Sesno at "Target Washington", a town hall meeting aired on public television, co-produced by George Mason University and WETA-TV.

Discussion *(Cont. from Page 4)*communities in which they work and their employees. So far we've seen tremendous initiative across the economy where we have the opportunity to sit down with corporate leaders and convince them of the prudence and appropriateness of investments. Again, regarding the chemical companies, we haven't asked them to do anything yet beyond the development of the vulnerability assessment tools that shows them a way they can secure some of these facilities. This may cost about three-quarters of a billion dollars and is still not done. You can make a good business case for the supply-chain, to manage it and protect it.

SESNO: What impact did the Madrid railway bombing have on your view of our own vulnerabilities in the U.S.?

RIDGE: Overall, it highlighted the inability to protect the roads and mass transit. It is important to note that after September 11th, the Department of Transportation had oversight responsibility for railroads and mass transit. DOT had begun to do vulnerability assessments, particularly to mass transit operations within the country and based on their assessments, they had encouraged mass transit systems to begin to provide more surveillance equipment, more uniform and non-uniform security personnel.

Now that we have responsibility for the transportation sector, clearly the Madrid incident accelerated some of the vulnerability assessments and some of the measures that DHS has been considering internally.

Public transportation has clearly been consistently a target starting back with Sarin gas in Japan. You had Madrid and the bombings in Moscow, both of which are a horrible reminder of the vulnerability and a catalyst for us to accelerate some of the technological innovations which we are looking into. It also shows you how complex security is and that you can just go so far to increase security before you begin to compromise the purpose for which you have mass transit.

It's very unlikely that we'll ever come in with a robust aviation-style security plan because you basically compromise the use, the need and convenience associated with mass transit.

We have pilot programs that employ technology to deal with people and explosives. The most recent was up in Connecticut, using explosive detection equipment actually installed on *(Continued, Page 6)*

Cybersecurity: Prioritizing a Plan of Action

Emily Frye

While Secretary Ridge's comments canvassed cybersecurity broadly, he made two particularly important points. First, he noted a new emphasis on building security in from the creation point; and second, he noted that international cooperation in pursuit of a "culture of security" is an important aim.

Build It In ... and They Will Come?

In the early days of software and Internet deployment, developers were concerned with functionality: how can I design a product that performs a specific function? And later, in subsequent versions of software, the concern revolved around performing the function(s) more quickly or with less memory. As the market for software heated up, time to market for new functionality was key. The discussions in the developer community focused on increased efficiency within programming processes.

Not until very recently did the issue of software security emerge as a non-academic topic of conversation and debate among the developer community. Like other actors in a capitalist economy, developers aim to respond to the pressures of the marketplace. The market has not demanded security, because vulnerability has not been high on the awareness radar. There was no point in building high-security software for the non-existent consumer.

The Internet as the Ultimate Global Infrastructure

Secretary Ridge explained that other international vulnerabilities, like maritime and aviation systems, have moved toward international security standards. While Secretary Ridge does not advocate an international cyber-governance body, he advocates some form of minimal international cybersecurity standards.

Preliminary discussions about formulating an international governance regime are taking place in several fora. To date, these discussions remain vague and uncohesive. Some of them take place between high-level officials at multilateral meetings; some of them take place between trading partners in international business. Other useful ideas emerge from academe: Eric Posner and Doug Lichtman proposed an international curtailment standard for ISPs in their paper on ISP liability (forthcoming in The Law and Economics of Cybersecurity, sponsored by The CIP Program). The most promising may well come from groups like UNCITRAL, which originated the movement resulting in critical mass surrounding the adoption of digital signature standards and electronic commerce standards in the 1990s. Unfortunately, it remains uncertain which group or groups will spearhead or fund efforts to develop a workable set of international standards.

Until such time as meaningful progress is made, the obvious truth stares us clearly in the face: an ungoverned - and unprotected - Internet is the common global infrastructure. ❖

Discussion *(Cont. from Page 5)*

the train as people were coming aboard. We are looking at this sector very aggressively, hoping to find some additional technological solutions that can help us keep the trains not only running on time, but enhancing the way they run. [The test is to keep] people moving quickly through portals to get on these trains and move from one part of the community to the next without too much interference. Balancing the security with the operational needs is a real challenge of mass transit.

Cyber Security

SESNO: Let's talk cyber for a minute. When you announced the creation of the National Cyber Security Division, about a year ago, you said, "Cyber security cuts across all aspects of critical infrastructure protection." How has cyber security improved since you made that observation?

RIDGE: We realize internally that we may never have the total brain power within the Department of Homeland Security to operate in the cyber world without being an extraordinary supporter of the academic community.

One of the first things we did once we created the division and a cyber chief was to reach out to the private sector and the academic community to develop the kinds of relationships needed to diagnose a cyber problem, inform the cyber world a problem exists and immediately move to develop the necessary patches or antidotes to *(Continued, Page 7)*

Discussion *(Cont. from Page 6)*
deal with the problem. So the infrastructure to identify, warn and remedy is already in place.

SESNO: Looking ahead 18 to 24 months, what should be accomplished on cyber protection to move it to the next best level?

RIDGE: There are probably two things that I would feel much better about 18 months to two years from now, and we are pushing both. First is a general awareness, not just within the cyber community and the companies that make the hardware and the software, but the public's awareness. We really need a lot more public information and greater public awareness with regard to how vulnerable the Internet is to individual citizens and students who do not take cyber security measures.

Secondly, I think we'll make progress if those companies responsible for developing the software are far more concerned about the vulnerabilities of their software before an incident occurs, rather than afterwards. I think in a post 9/11 world with the emphasis and collaborative relationships with private companies who develop hacker and tamper resistant systems from the get-go, rather than pulling together resources after the system has been inundated, we have made huge progress.

SESNO: The bad guys are always at work. Is that possible?

RIDGE: Absolutely.

SESNO: Isn't it possible that building so many protections just causes the bad guys to move to the next level?

RIDGE: Well, I think the fact of the matter is that our job is to stay as far ahead of them as we possibly can, and the best minds and the best people to do that are those who brought their extraordinary Internet world to the global community. Those responsible for developing products, for official or unofficial use, never really saw it being a tool of destruction; they really considered it the interdependency, between the physical and cyber. They have got to help us stay one step ahead of terrorists, and if they are smarter than the terrorists, I am sure they will.

> *"We realize internally that we may never have the total brain power within the Department of Homeland Security to operate in the cyber world without being an extraordinary supporter of the academic community."*
>
> -- Secretary Tom Ridge

SESNO: Cyber security is unique to critical infrastructures and cuts across borders. Article five of the National Cyber Security strategy requires the U.S. to work with international institutions to create what's called "a culture of security." How is it going?

RIDGE: We are going to have to pick up the pace a little bit. We've been focused early on domestic cyber security but there are a couple of international organizations that we need to engage too. Since you can access the internet globally , we're going to need global partners to find global solutions to deal with these terrorists.

Therein lie many challenges associated with how different countries deal with access, privacy concerns and the like, so it's much more complicated than most people realize. So I would accelerate the pace; we still have a lot of work to do.

SESNO: When you say pick up the pace, who are you talking about?

RIDGE: Government to government. It's one thing to deal with a mix of companies whose systems are controlled through the internet and yet another thing to encourage foreign countries to crack down on cyber crime and to identify collaboratively incursions in the cyber world as they protect their security and international security.

SESNO: Some say there needs to be an international regulatory regime for the protection of cyber space. Do you agree, and if so, what are the next steps here? *(Continued, Page 8)*

Discussion *(Cont. from Page 7)*

RIDGE: I'm not sure it's possible to get an international body overseeing the international cyber world. But, before we can even contemplate such an oversight body, which I think is very unlikely, I think we need to come up with some cyber standards and some international standards. This is similar to what we've done for a couple of other potential international vulnerabilities like maritime and aviation and moving to the biometric standard. So, I don't think we need an international body. I'm not sure we need to promote one. I do think we need to reach some consensus around minimal cyber protection and standards for our protection.

SESNO: The cyber security piece in the National Response Plan [NRP] recognizes that cyber attacks are a form of terrorism. It is not just focusing on physical attacks but the entire cyber annex that contemplates what are the coordinating structures, processes and protocols for government wide response to a coordinated cyber attack. So is that being built into the way of doing business?

RIDGE: Yes. NRP has been pretty good about the standard for protocol we have developed domestically. Internationally, we're going to need government to government. I think the G-8 will take the lead. I don't think any country has ever surrendered sovereignty with regard to a cyber regulatory agency. But setting standards is a great place to start, and then figuring out internationally how we can help each other enforce those standards. However, we have a long way to go.

Information Sharing Efforts

SESNO: Compared to the U.S., much more of Europe's critical infrastructure is owned by government, or directed by government. How does that affect efforts to coordinate and better protect this global critical infrastructure you spoke about?

RIDGE: The private sector has been very engaged from day one with the Department, in an effort to identify real vulnerabilities and qualities to which both the private sector and public sector must pay attention. We have this Information Sharing Analysis Center (ISAC) as a means of communicating threats and warnings. These ISACs provide a very comprehensive look at the different sectors of the economy, and help us decide where in the public and private sectors we ought to invest to make that sector more secure. [The private sector] has been supportive. They've invested hundreds of millions and they have only just begun. There is still a lot more work that we need to do out there. [For example] with ports. They've invested a lot of money in the ports themselves. We expect the private sector to step up and invest even more to help us improve the security and safety of our ports.

SESNO: Would it be easier if we had more of a European system where the government has more of a hand in all of this?

RIDGE: The government has a guiding hand, at this point.

SESNO: But, you don't own the industry.

RIDGE: We don't own the industry, but when we have had the opportunity and the responsibility to make the business case to them, they've been responsive. We do have the responsibility to give them the tools to help them identify a baseline threshold of security that we, as a government, expect from them.

And, one of the ways that we believe we can generate that kind of support is empowering those local first responders, that is the police and fire chiefs, to go over to that chemical site, as well as that transportation hub, or to go over that particular venue, and talk to the owners. If first responders are satisfied with the level of preparation and security around their communities, then we need to ensure that those protected levels are met and then maintained.

SESNO: In terms of meshing our private sector driven efforts in this country with other governments - what are the pressure points?

RIDGE: Well, aviation is probably the best example because a lot of the countries with whom we deal have major carriers and domestic carriers that are owned by the government, while ours are all privately owned. And, we've had *(Continued, Page 9)*

Discussion *(Cont. from Page 8)* the experience since last December of basically going to these airlines, and therefore to their governments, and saying "based on the information we have, we believe these enhanced security measures would be an asset, or better yet, you shouldn't even put those planes in the air."

This constant interaction among officials, France, Mexico and Great Britain among others, has led to a much broader discussion with regard to thresholds and standards for international aviation. These same kinds of discussions and standards have developed with maritime concerns. So in the future, we will have a global response to the concerns that we all have.

Again, whether it's publicly or privately held, the world is beginning to realize that whether the terrorists strike an airline coming into the U.S., or elsewhere, the repercussions to the airline industry, and the travel and tourism industry, will be monstrous. We're beginning to see an understanding of global threats, global standards, global measurements and global cooperation, which is accelerating across the board.

SESNO: GMU is coordinating with Assistant Secretary Liscouski to bring together the sector coordinators and the ISACs. What do you want to see from this initiative and in the year ahead?

RIDGE: Standards, priorities and investments. Standards of protection can vary. For example, a favorite subject of pundits, analysts and critics, is getting and using chemical sector plans so that depending on the location of the chemical site and the toxicity of the contents, we have to set priorities as to where we go first with our investment and the level of security. We need to set standards. It could be across the board because *(Continued, Page 10)*

Private Sector Programs: Helping to Bring Homeland Security to the Private Sector

The CIP Program's Private Sector Programs (PSP) initiative supports the private sector with respect to information sharing and homeland security. PSP's work primarily focuses on issues that cut across most critical infrastructure sectors. PSP also assists in developing interdependency, legal, economic, business, and information sharing structures for information sharing among private sector groups as well as between the private sector and the government. PSP receives funding from the Department of Homeland Security (DHS) and is recognized as a key liaison between DHS and the private sector.

Over the past several months, PSP has assisted DHS and the private sector in making several advances in CIP. For example, GMU hosts quarterly meetings of key private sector participants, including Sector Coordinators and the ISAC Council, to discuss critical infrastructure protection issues among themselves and to organize communications with the government. Some sessions of these meetings are well attended by invited government officials and provide a mechanism for exchanging information. This institutionalized forum has proven to be the incubator for new initiatives to be addressed by task forces drawn from the attendees of the meetings as well as from other private sector corporations.

As an outgrowth of these meetings and relationships, PSP has identified areas for critical infrastructure research and assists several task forces formed from the private sector to address issues such as: (i) the relationship between physical and cyber security, (ii) identification of key elements of business continuity practices, (iii) the effect of corporate governance issues on information sharing, and (iv) identification of uniform approaches to address interdependencies.

PSP's role continues to expand and evolve in response to both government and private sector needs. As a flexible forum for academic, business and government information exchange, the CIP Program, through its PSP work, continues to play a lead in critical infrastructure protection issues.

GMU's role in private sector and homeland security issues has been recognized by key private sector participants. "The critical infrastructures supporting the nation's different economic sectors are mostly in private hands, and coordinating across each of those sectors to achieve effective protection for those infrastructures is a complicated job. The support that GMU's Private Sector Programs initiative provides is absolutely critical for that very complex coordination effort to succeed," said Donald F. Donahue,Chief Operating Officer of the Depository Trust and Clearing Corporation. PSP is managed by Rod Nydam, Associate Director for Private Sector Programs. ❖

Discussion *(Cont. from Page 9)*
we need collaboration and greater investment on behalf on the private sector. And that's the best place to make the business case for the private sector investment.

Actually, one of the things we are doing here with the private sector is connecting our Homeland Security information network to private companies. We have started to run four pilots - Dallas, Seattle, Indianapolis and Atlanta. It is a non-classified network that sends out threat warnings from the Department to the private sector. It is a very comprehensive communications infrastructure, which we didn't have prior to this effort.

Citizen Education & Engagement

SESNO: You and I have had the opportunity to participate in a series of town hall meetings around the country where we did a lot of listening. What is your sense of how federal, state and local governments are doing, with respect to connecting with their citizens on the priorities, expenditures and preparations for Homeland Security?

RIDGE: It's my sense that most Americans want more information than we have been providing. Not just in terms of the nature of the information or intelligence, but what can they do as a individual citizen, or a family member, to better prepare themselves in their communities.

The series of town meetings that we both attended and engaged in were very revealing in the sense that the majority of people raised their hands when asked whether or not they could become more engaged in helping their community in preparing for a terrorist attack. It was pretty clear that many citizens were not aware of the Citizen Corps in many of these communities, where volunteers would be warmly welcomed.

My sense is that citizens want more information to be better prepared and more engaged. I think they are just going to have to continue to sustain the message that there are ways for you to help your community. Frankly, it's one of the reasons that we are going into the second phase of our national approach toward preparedness, with our launch of a National Preparedness Campaign in September.

We've heard pretty loud and clear people want to be involved. Hopefully, this second year of outreach with regard to preparedness can connect more Americans and ultimately give them an answer to the question: What can I do to help AND dramatically influence the safety and security of this country? ❖

Citizens Weigh In on Homeland Security

A Report by the Council for Excellence in Government

When it comes to ideas and actions to improve the nation's homeland security, the American people have plenty to say.

Their concerns and suggestions set the agenda for nearly 50 recommendations for national action in *We the People: Homeland Security from the Citizens' Perspective*, a report by the Council for Excellence in Government, a Washington-based nonpartisan, nonprofit think-tank. The report concluded an unprecedented nine-month long dialogue with the American people regarding a variety of homeland security issues.

Among the recommendations:

- The President should direct the Department of Homeland Security to convene leaders from federal, state and local governments, the private sector and civic organizations to update the National Strategy for Homeland Security, with input from citizens.
- State and local governments, schools and workplaces should update and practice their plans, with direct involvement of citizens, parents and employees.
- Local governments should produce index cards of critical information in a user-friendly format that can be distributed in multiple languages through many channels to homes, workplaces and schools.

(Continued, Page 11)

Citizens *(Cont. from Page 10)*

- Local officials should set up one telephone number (similar to 311 or 911) for citizens to report homeland security threats and emergency information; and offer citizens a service that will send emergency information to phones, cell phones, e-mail addresses, pagers and other personal communications devices.

- The National Strategy on Homeland Security should set the goal of a seamless network for authorized public safety officials to share information and talk to each other at a level of reliability and security that can withstand the demands of a national emergency.

The recommendations flowed from several activities by the Council to look at the entire homeland security enterprise through citizens' eyes. The effort included state-of-the-art town hall meetings in St. Louis, Miami, San Diego, Houston, Fairfax, Boston, and Seattle (many moderated by GMU's Frank Sesno and featuring U.S. Department of Homeland Security Secretary Tom Ridge) and national polls which were reviewed by expert working groups to identify ideas and activities–at the national, state and local levels, in the public sector, private sector and in communities and homes across America– for individual and collective action.

"The recommendations are truly of, by and for the people," noted Patricia McGinnis, President and CEO of the Council for Excellence in Government. "Our hope is that leaders within the homeland security enterprise - as well as everyday people - will use them as a blueprint to make the citizens' homeland security vision a national reality."

The recommendations are targeted at all levels of government, from the President, the Department of Homeland Security and other federal agencies, the U.S. Congress, and state and local governments to schools, the first responder community, private employers, managers of privately-owned critical infrastructure facilities, industry and trade associations, the local and national media, and families and individual citizens.

Topic areas for the recommendations cover a wide landscape: collaboration, informed and engaged citizens, strategic/appropriate uses and sharing of information, and innovation and rigorous evaluation.

The Council's national poll of citizens' views on homeland security, released in March, 2004, found that while a majority of Americans describe themselves as "concerned" and believe that the nation is likely to be the target of another terrorist attack in the months ahead, very few are aware of state and local security preparedness plans.

When asked for ways that government can improve homeland security, more than one-third of citizen respondents said they believe that the two most-effective measures are creating information systems that can share data across law enforcement, health and emergency agencies, and improving border security. Nearly half (47 percent) of Americans surveyed said that the United States is safer today than it was on Sep. 11, 2001, up from 38 percent one year after the attacks.

Other key findings of the report:

- Three-quarters (77 percent) of adults said they believe it is very or somewhat likely the United States will be the target of another major terrorist attack in the next few months. However, half (49 percent) of the adults surveyed said that they are not concerned about an attack in their neighborhoods;

- While 26 percent of Americans describe themselves as "calm," nearly three-quarters (73 percent) describe themselves as either "anxious" or "concerned";

- The most-feared types of attacks are bioterrorism and chemical weapons, selected by 48 percent and 37 percent of citizen respondents, respectively;

- Only one in five (19 percent) Americans said they are aware of or familiar with their communities' preparedness plans; 18 percent said they are aware of or familiar with their state's preparedness plans; 36 percent said they are aware of or familiar with their workplace's preparedness plans; and 27 percent said they are aware of or *(Continued, Page 12)*

Citizens *(Cont. from Page 11)*
familiar with their schools' preparedness plans;

■ Citizens view information systems that share data across agencies (interoperability) and tighter border security as the best steps to strengthen the homeland, each selected by 37 percent of respondents;

■ More than three in five citizens (62 percent) said they would be willing to volunteer to help homeland security efforts, including planning, training, and practicing drills in their communities. The same percentage supports a new nationwide hotline to report suspicious activity;

■ Fifty-six percent of Americans believe that the Patriot Act is good for America. Thirty-three percent believe it is bad for America. Eleven percent of Americans are unsure. Half the public believe that it must be debated thoroughly in Congress before any decisions are made about whether it should be renewed next year;

■ A majority (59 percent) of the public said they believe the government should have access to companies' personal information about their customers if there is any chance that it will help prevent terrorism.

In addition to the national survey of Americans' attitudes, the Council surveyed front-line emergency responders across the nation, including fire chiefs, police chiefs and sheriffs. Although a majority (53 percent) of this group said they believe that the country is safer today than it was two and a half years ago, two-thirds (65 percent) of all of these respondents said they believe that their agencies are only somewhat prepared to respond if disaster strikes, and only one-quarter (26 percent) said they believe that their agencies are adequately prepared.

As with citizen respondents, first responders' most-feared types of attacks are bioterrorism and chemical weapons, selected by 67 percent and 42 percent, respectively. But first responders show considerably more concern about attacks on critical infrastructure than does the public, with nearly two-thirds (62 percent) of first responders saying that they worry "a great deal" or "quite a lot" about attacks on infrastructure.

When asked to prioritize measures to promote homeland security, first responders rated emergency response equipment training first among their priorities, selected by 51 percent, followed by the two areas selected as most important by citizen respondents: interoperability, selected by 34 percent of first responders; and tighter borders, selected by 25 percent of first responders. Two-thirds (66 percent) said they support the establishment of a nationwide homeland security telephone hotline.

The recommendations and poll results are available at www.excelgov.org. ❖

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

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/archives/cipp-report-l.html.