May, 2010

Proceedings of the 2009 NRC Federal Facilities Council/James Madison University Symposium on Protecting Large Facility Complexes;

George H Baker, *James Madison University*
Cheryl E Wilkins, *James Madison University*

Institute for Infrastructure & Information Assurance
at James Madison University

in cooperation with the

Federal Facilities Council of the National Academies

presents

2009 NRC/FFC & IIIA Homeland Security Symposium

"Protecting Large Facility Complexes"

Wednesday, May 13, 2009

Washington Convention Center
Washington, DC

www.jmu.edu/iiia/2009symposium

JAMES MADISON UNIVERSITY

Proceedings
of the
Institute for Infrastructure & Information Assurance
and the
Federal Facilities Council of the National Academies

2009 NRC/FFC & IIIA Homeland Security Symposium
"Protecting Large Facility Complexes"

Held at

Washington Convention Center
Washington, D.C.

May 13, 2009

George H. Baker
Cheryl Elliott Wilkins
Editors

Institute for Infrastructure & Information Assurance
James Madison University, Harrisonburg, Virginia
 IIIA Publication 09-02

James Madison University partners with George Mason University on the Critical Infrastructure Protection Program (CIPP).

This research was supported [in part] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

Edited by George H. Baker and Cheryl Elliott Wilkins
Graphic Design by Cheryl Elliott Wilkins
Student Design Assistance by Amanda Desourdis
Proceedings by: CASET Associates, Ltd., 10201 Lee Highway, Fairfax, Virginia 22030 (703) 352-0091

Limited copies are available from the Institute for Infrastructure & Information Assurance (IIIA), 800 South Main Street, MSC 3804, Harrisonburg, VA 22807; 540-568-4442. This publication is available electronically on the website: www.jmu.edu/iiia/

IIIA Publication 09-02

Printed in the U.S.A. Printed by Mid Valley Press, Verona, Virginia

Table of Contents

Welcome from JMU's President

Dr. Linwood H. Rose, President, James Madison University

Welcome to James Madison University's 4th Annual Homeland Security Symposium, hosted by our Institute for Infrastructure and Information Assurance and the Federal Facilities Council of the National Academies.

This year's symposium builds upon the efforts of past symposia, where we have examined coordination of emergency preparedness strategies to engage organizations and people at the grass roots level; cascading failures due to the complexity and interdependent nature of infrastructure systems; and the benefits of public-private partnerships to secure critical infrastructure. Our current theme, "Protecting Large Facility Complexes," addresses the challenges associated with properly securing government structures, research and development parks, and private offices, to name a few. We have selected a seasoned group of moderators and panelists from academia, industry and government to engage and provoke thought on issues ranging from cyber security, to physically hardening a facility, to insider threats. In addition, we are privileged to have President Charles W. Steger of Virginia Tech and CDC Deputy Director for Security and Preparedness John Stevens as our keynote speakers.

We hope you enjoy today's event and look forward to future symposia in which we focus on the most relevant homeland security topics in order to better secure the nation.

LIVE @ the Convention Center! Check **http://www.jmu.edu/iiia/2009symposium** for interviews, clips and commentary about today's event. Are you on **Twitter**? Follow **@JMU_IIIA** for updates during the symposium, and participate in the discussion using the **hashtag #jmuiiia.**

If you are interested in learning more about the research presented today, please contact the presenters directly. If you would like more information about JMU, please contact Cheryl Elliott Wilkins (contact information is listed on page 27 of this program).

Please complete the event evaluation form, found on pages 25-26 of this program. Your comments will assist us with planning future events. Be sure to leave your evaluation form in the box at the Registration Table.

For more information on IIIA, please visit our website at: **www.jmu.edu/iiia**. The proceedings for this event will be posted on our website.

Over breaks and lunch, please be sure to visit the Poster Presentations in the Exhibit Area in 147B. Poster Authors will be available near their posters.

Please read about new and current research activities at JMU on pages 14-15. Read more about JMU's Office of Research and Public Service components on pages 18-19.

Questions during the Symposium? Please check with staff at the Registration Tables outside of Room 147AB.

Symposium Emcee -- Dr. George H. Baker, Technical Director, IIIA

Symposium Planning Committee -- Lynda Stanley, Teri G. Thorowgood, George Baker, Cheryl Elliott Wilkins, Benjamin Delp, and Lynne Murray.

A special thanks to Becky Rohlf for event organization and to Amanda Desourdis for graphic design assistance.

Many Thanks...

James Madison University and the Institute for Infrastructure and Information Assurance express our gratitude to the National Academies and the Federal Facilities Council for co-sponsoring this event.

Welcome from IIIA,

On behalf of James Madison University and the Institute for Infrastructure and Information Assurance, I am pleased to welcome you to the 2009 Homeland Security Symposium, Protecting Large Facility Complexes. Large facility complexes are owned and operated by federal and state governments, local municipalities and virtually all sectors across private industry. These complexes require a security strategy that addresses both cyber and physical threats that cut across multiple critical infrastructure in order to maintain a robust level of protection.

The nation's large facility complexes includes national laboratories, university research parks, government agency and corporate headquarters, nuclear power plants, sports stadiums and music venues. These complexes host research, commerce and policymaking vital to the future of the nation. The goal of this symposium is to gain perspective on the vast array of challenges those tasked with protecting large facility complexes are confronted with each and every day. Challenges like Supervisory Control and Data Acquisition (SCADA), insider sabotage, natural disasters, cyber attacks, response and recovery will be examined to share best practices and solutions.

Symposium participants include leaders with experience in academia, federal/state/local government agencies, private-sector companies, industry associations and standards organizations. The breadth and depth of this year's keynote speakers, moderators and panelists will undoubtedly expand the continually evolving strategies and plans to ensure the nation's most critical facilities are redundant, robust, and resilient, in order to effectively defend against not only the current spectrum of risks, but also the yet to be identified threats of the 21st century.

I would like to thank our gracious partner, the Federal Facilities Council of the National Academies, and The Infrastructure Security Partnership, the American Public Works Association, the International Association For Intelligence Education, and the Homeland Security Institute for their continued support of the symposium. I trust you will find the symposium to be both insightful and meaningful. Thank you for investing your time.

Sincerely,

John B. Noftsinger, Jr.
Vice Provost, James Madison University
Executive Director, IIIA

Section I: Symposium Themes

In this section, you will find the Emerging Themes from the symposium.

Emergent Themes

Large, complex facilities pose unique protection challenges involving multidisciplinary expertise and collaboration among government, academia, and the private sector. The symposium served as a forum for sharing experiences in dealing with large facility catastrophic events and risk management. The symposium was organized based on the value of interaction among different people representing diverse disciplines. In many instances, such interactions lead to solutions that would not have been developed within disciplinary stovepipes. The venue was divided into three panels addressing physical security, cyber security, and real facility case studies. We were also privileged to have three keynote speakers including Dr. Charles Steger, President of Virginia Tech, Susan Armstrong, Director of the Infrastructure Security Compliance Division at Department of Homeland Security, and John Stevens, the Center for Disease Control's Deputy Director for Security and Emergency Preparedness.

Despite the varied backgrounds of panelists and keynote speakers, we are excited about the important common themes from the proceedings that were reinforced by several presentations representing multi-discipline perspectives. These themes relate to dealing with multiple hazards, the vulnerability of complexity, the importance of standard approaches to risk management, multi-jurisdictional coordination, public-private partnerships, public awareness and education, technical and legal challenges. Of course, the most important part of the proceedings are many ideas concerning future directions – what we can do better to meet the challenges associated with protecting large facility complexes. We have distilled the common ideas from the proceedings below.

Large facility complexes face a set of common vulnerabilities.

These include easy access by a large number of people, accessibility to items of unique value or significance, certain events which guarantee a significant and mobile crowd, and numerous entrances and exits for people and deliveries. Prime examples of large facilities include universities, ports, and sports venues. The public nature of many large complexes and the large number of people moving through heighten the importance and difficulty of achieving security. Another major challenge is the variety of missions performed by these facilities.

When facilities become large, simple point defense is no longer adequate. The facility now must be thought of as a network of interdependent systems, both physical and human. Charles Perot's concept of the "vulnerability of complexity" applies. This complexity is characteristic of all major institutions. The scale and complexity of operations is not readily perceived or understood by the public.

A rational threat assessment is critical to successful protection of facilities.

The choice of a design threat is one of the most controversial and subjective components of the risk management process. The risk of some threats may be quantified such as fire, weather, and seismic related events. By contrast, we have found it difficult to articulate threats from asymmetric terrorism, aging infrastructure, and climate change. In this regard, the all-hazards approach makes sense. The identification of single-point failure locations in facilities is an excellent all-hazards method since, in many cases, these failure points are vulnerable to multiple threats and hazards and engender the same consequences, regardless of threat.

It is important to understand that terrorism targets our psychological as well as our physical well-being. We must avoid the tendency to be frozen by our fears, rather to make sure that we are ready. Although terror attacks often aimed at maximizing direct human casualties, infrastructure attacks are becoming more prevalent.

Improvised Explosive Devices (IEDs) are a growing concern. FBI data indicates there are on the order of a thousand unauthorized explosive events in the U.S. per year. Most of them are small and related to malicious mischief on the part of youth, but they nonetheless involved explosives that are readily assembled from components that can be purchased at Home Depot. DHS has implemented a "Bomb Making Materials Awareness Program" in collaboration with the FBI and the ATF. The program is of particular interest for distributors, wholesalers and warehousers in educating their employees on materials usable for fabrication of IEDs.

"How much security is enough?"

Managing expectations is just as important as managing risk. We must avoid setting the expectation of providing security that is absolute. The threats we face are too diverse, too deadly, and in many instances, too difficult to detect to secure every possible target. The public at large does not understand this.

In some cases our best preparations are thwarted. However, the option of doing nothing is, in fact, not an option.

Standards and metrics are very helpful in achieving credible and balanced protection.

Prior to 9/11, each federal department had its own approach to protecting facilities. These were quite diverse – there was nothing across the board. Much progress has been made in this regard.

In "voluntary space," DHS has developed a vulnerability identification self assessment tool that enables facilities to conduct their own standard vulnerability assessments. They have also published a pandemic influenza guide for critical infrastructure facility owners and operators. In "regulatory space," DHS is implementing a Chemical Facility Antiterrorism Standard (CFAS). CDC has implemented standards for hazardous biological materials. If a hazardous material is present in a facility of any type, there are certain standards that apply.

By law, DHS standards are not prescriptive. They have taken a risk-based performance approach that allows facilities to design their own layered defense. These standards are included in the risk-based performance standards (RBPS) document.

Federal facilities are now classified according to their security priority. There are five federal security levels (FSLs). The levels are determined by a prescribed risk assessment process that takes into account facility mission criticality and threat.

The Automated Critical Asset Management System (ACAMS) has great potential for standardizing identification, prioritization and protection of critical facilities. It was used successfully as part of the Super Bowl XLII security program.

Several legal issues are important considerations in the security requirement trade-space.

The question of how much individual liberty and personal privacy we are willing to sacrifice to advance incremental improvements in security continues to be daunting.

Fusion centers were created to exchange information and intelligence to improve the ability to fight crime and terrorism by merging data from various sources. The ACLU has called for an internal investigation of these centers, claiming that these organizations are exhibiting mission creep. They are advocating guidelines to limit the purview of these centers in collecting private information. Rights groups are also concerned about the growing number of metropolitan police departments and other law enforcement agencies that are embracing new collaborative systems to report suspicious activities.

Perfect security is not possible. When protection features fail, a complete new level of liability has been created. These pose challenges vis-à-vis the new trend toward formalizing risk acceptance.

Education and training initiatives including exercises should be incorporated in security programs.

Any successful security plan must incorporate education, whether it relates to physical protection or cyber security. All-hazards protection, response, and recovery strategies require the development and execution of training and exercise regimens to be effective when high consequence events occur.

The Interagency Security Council is implementing a nationwide training program. There are hundreds of security principals to be certified. The training covers security performance measures and best practices on the prevention of workplace violence.

It is important to increase the level of awareness of the public in general. A broad-based public education program presented outside the context of an immediate threat or crisis can certainly be of value.

Large, complex facilities need a well-defined risk management process.

The first priority is to manage expectations. Facility owners and managers must understand what is reasonable and how much protective measures will cost. There are three ways to buy down risk – by preventing attacks, hardening facilities, and/or improving response assets.

Symposium case studies indicated that the first attempt at identifying protection requirements has always exceeded available funds. Risk assessments were required in each case to reduce the costs to affordable levels. Thus, risk management is a priorities problem. The process starts with an assessment of criticality, threat vulnerability, response and recovery assets, assessing the overall consequences of various attack scenarios, and then coming up with a priority list of risks to individual critical assets. Facility priority sorting is accomplished based on protection cost vs. risk trades. There are cost-benefit methods available to quantify risk in a comparative manner that can be helpful in decision-making. These methods involve calculating and plotting the amount of reduction in risk achievable for a given cost.

Vulnerability assessments are an important part of the risk-management problem. They are used to identify single-point vulnerabilities within facilities whose failure will cause a facility mission abort. There is value in having assessments by external organizations. Insights from the military are particularly helpful based on extensive targeting experience. Organizations such as the Special Forces, the Navy Seals and the Defense Threat Reduction Agency (DTRA) are particularly good at this. We train our military very well to be able to defeat facility defenses. In that context we look at design bases to counter the tactics that they identify for us. Our objective is to raise the bar, to raise the amounts of effort and resources a malefactor would need to compromise the mission of any of our facilities.

Because facilities change in time, it is important to repeat the process on an annual or bi-annual cycle. Using this approach it is possible to measure the buy-down in risk over time.

An important trend in risk management is institutionalizing a formal risk acceptance process.

Risk acceptance has been a continuing, common issue relative to facility security programs. The National Response Plan addresses risk acceptance in a very cursory manner. A recent initiative to implement a formal risk acceptance regimen within the federal community is revolutionary. There is still no general process that has been implemented throughout the federal government.

The process being used in some locations involves establishing a desired security level. A standard countermeasures list is then used to allow the facility manager to develop a customized approach. It is most often not possible to implement all countermeasures due to resource and physical constraints. The manager formally accepts the risk associated with these constraints. This process results in a record that explains what was done, what was not done, and the underlying rationale.

Protection strategies must be expansive and, if possible, include at the beginning of facility development.

Protection strategies must involve more than gates, fences, and cameras. Protection strategies also include redundancy and resiliency.

Renovation of existing buildings is much more difficult than incorporating protective measures into new construction. It is expensive and cumbersome. Many unforeseen problems are created when protection is applied as a band-aid or as an afterthought. Providing protection for systems whose designs are inherently more difficult to protect can be cost-prohibitive.

Some protection problems for existing facilities can be solved by procedural means. Proper attention to human factors can save a lot of money.

Evacuation and rescue/recovery (ERR) are an essential part of protection strategies. An important lesson from 9/11 was that getting people out of buildings after they have been attacked is vitally important. It is important to identify ERR systems that warrant protection because they must remain operational after an attack. Factors include making sure that enough people can access evacuation systems, increasing stairway width, providing a concrete core to allow ERR systems to survive, and pressurizing stair shafts and lobbies in case of chem-bio attacks.

Life-cycle surveillance and maintenance of facility protection measures is critically important. Facility protection features should be documented in an "owner's manual" so managers will know what facility features are "hardness critical." Just as mechanical systems, security and protection systems need to be understood, maintained and operated appropriately. For example, relaxing or changing operational procedures can compromise the level of protection provided by structural systems.

Multi-jurisdictional planning is essential.

Large facility catastrophes affect more than the facility itself. For example the New York Port Authority serves a ten-state region of 70-80 million people. The Port is critical, not only to the economic life of New York City, but to the entire Northeast.

Local-State-Federal government responsibilities must be understood. Public-private partnerships including liaison with local businesses is also key. Because all disasters are local, the local responders must have a major role in operational planning. The right people need to know who is going to respond to a disaster. Organizational and interpersonal relationships are the key to achieve overall success.

Establishing a multi-jurisdictional emergency operations center is important for response coordination. Multi-jurisdictional exercises are important to establish and practice necessary coordination.

Cyber security is critical part of large facility protection.

The world has changed over the past five years and now important aspects of all large facility functions are performed on line. Complicating the situation are the wide variety of users and missions at large facilities.

Computer operations is a 24/7 enterprise. Many facilities continuously deal with new populations of users coming into and leaving the cyber environment. Users want to be able to work from anywhere. Increasingly, they are using high mobility devices. Technology environments are becoming decoupled from facility assets due to the general commoditization of information technology, including smart phones, PDAs and other new data/communication devices.

A number of years ago, if IT managers controlled their central system databases and built security around the central core, they were confident that security was adequate. At present, security is more dependent on the decisions that are made at network end points by the user behind the device. Much more time is needed in providing information security awareness and education efforts.

Software is a problem. The basic Enterprise Resource Planning (ERP) software packages used by large organizations are not secure. The packages are delivered in an insecure state.

An effective solution to the user diversity problem is to develop partnerships with different organizations within the facility complex including the human resources office, the IT auditing staff, department heads, departmental system administrators, and chief executives. Making computer security part of each employees annual review criteria is one effective measure.

Life-cycle management of systems and data must be explicitly addressed. Data itself may have urgency when first acquired and stored. But over time, the data loses its urgency. Older equipment is often less-secure than newer equipment and may need upgrades or replacement.

When handling highly sensitive data, it is important that IT departments conduct risk assessments and exercises analogous with the facility physical security departments. Getting functional groups together and encouraging them in their jobs and progress in perceiving external threats and securing their internal resources is important. We must understand the internal targets of external threats and whether those targets are protected.

An essential component of the governance and risk equation is compliance, both organizational and personal. Education is important for compliance. It is important to ensure that users understand what "highly sensitive data" means – this definition is quite involved. Regarding sensitive data, we are moving toward an approach that involves the concept of "trust but verify."

Computer security involves partnerships and collaboration. Capable and informed users are the security.

Control system security is gaining needed attention due to recent incidents.

Industrial control systems make it possible to affect real world physical/mechanical actions through the virtual realm of the Internet. Traditionally these systems were isolated. Now, for cost-saving reasons, they are implemented and run over the Internet, enhancing their vulnerability to outside attack. Modern control systems are becoming more interconnected, particularly with business systems within corporations.

There are major ramifications of control system failures. As examples, our national power grid and petroleum product pipeline systems are controlled by computer. The 2003 Northeast blackout resulted from a control system failure. Last year, a Polish hacker disrupted a railroad switching system causing some derailments. We are seeing attacks and evidence of attack planning by governments of hostile countries.

There is progress in addressing control system security issues. An Industrial National Security Cyber Emergency Response Team has been organized. A control system self-assessment tool has been developed by INL along with procurement guidelines for control system acquisition. INL also offers an education and training program on process control system security. A new Industrial Control System Joint Working Group has been organized that brings government and industry together.

Common Concerns and Challenges.

Symposium participants identified several important areas requiring attention.

Many large facilities remain unprotected commensurate with their value. These facilities have significant exploitable vulnerabilities that have not been addressed.

As a nation, we have put a great deal of effort into screening people, but very little effort has gone into perimeter protection. Airports are a case in point.

For commercial property owners, there really are no protection criteria. FEMA has put together an excellent series on risk management for the private sector, but they are only suggestions. The information is useful but it is not possible to design facilities directly from them.

A U.S. standard has yet to be developed for armed contract guards.

The news media often hinder facility security endeavors. There is an unfortunate conflict of goals with

respect to media representatives who are hoping to move up in the world by exposing vulnerabilities. Many online media services don't actually report – rather they lift pieces from the traditional media and tending to select the more provocative information. This causes the security departments to jump through unnecessary hoops answering public affairs questions. The news media can be a major help if they are willing consult with security managers in constructive dialog.

Future Directions.

In the past, much of our focus across the country has been analogous to filling sandbags before the flood. We have not focused nearly enough on facility and critical infrastructure interdependencies. This situation is changing.

Preparedness planning is improving. We are not only using risk assessment now to think about how to protect our large facility complexes, but we are also beginning to think about how to use risk assessment before an event to project the impact of response and recovery strategies and the best sequence to use in restoring infrastructures. In some organizations, risk management is embedded as part of the continuous business model including planning, programming, and budgeting.

There continues to be more attention to regional interdependencies and addressing the effects of large-scale contingencies. There is much progress with state and local organizations working in concert with the federal level. Attention to regional-level consequences led to a much more realistic set of priorities. A great deal of work is being done to explore the consequences of infrastructure loss both downstream and upstream from critical facilities. In this vein, it will be important to balance survivability across infrastructures. It is not good practice to protect one infrastructure at a level beyond what others are addressing if the risks are commensurate. Standard risk assessment methods can help here.

An important emerging research sector is community safety and resilience. This field is now being created. Basic and applied research on community resilience informatics is a major thrust. Research into policy studies and social systems must address issues of distributed decision making, system linkages, and cascading effects of failing infrastructures, as well as issues of privacy and civil liberties.

From a technical standpoint, building architecture is getting ever more adventuresome and ever more complex. This poses protection challenges. WMD and IED detection technology has much room for improvement. Simulation and blast modeling techniques should be subjects of continuous improvement, including verification by test.

In the area of cyber security, progress is needed in the development of automated systems to trace attack paths from critical data locations to the outside world. This will be important to reduce the paper burden associated with manually tracing logs, which is presently beyond IT department throughput capabilities. Real-time network intrusion detection and diagnostic tools are needed. Securing digital control systems clearly deserves higher priority.

Large organizations will benefit from the implementation of intelligence analysis programs to anticipate malicious events before they happen.

We will continue to be challenged in competing for security resources. As the memory of 9/11 recedes, these challenges will increase.

Section II: Symposium Event

In this section, you will find the details from the event, including the day's schedule, information about JMU's programs and research efforts.

8-8:30 am Continental Breakfast, Registration, Networking	8:30-8:50	8:50-9:30	9:30-11	11-11:15 am Morning Break
	Welcome and Symposium Introduction Master of Ceremonies: Dr. George H. Baker, Technical Director, IIIA Ms. Lynda Stanley, Director of the Board on Infrastructure and the Constructed Environment (BICE) of the National Research Council (NRC), National Academy of Sciences Dr. John B. Noftsinger, Jr., Vice Provost, James Madison University, and Executive Director, IIIA *See bios beginning on page 84.*	**Morning Keynote Address** Dr. Charles Steger, President, Virginia Tech *See Dr. Steger's bio on page 84.*	**Panel One** **Physical Protection Problems and Approaches** Moderator: Richard Little, Director, The Keston Institute for Public Finance & Infrastructure Policy, University of Southern California Bill Austin, Chief, Balanced Survivability Assessments Branch, Defense Threat Reduction Agency (DTRA) Austin Smith, Executive Director of the Interagency Security Committee (ISC) Robert Smilowitz, Principal, Applied Sciences Division, Weidlinger Associates *See panel member bios on beginning on page 84.*	

11:15-12:45	12:45-1:45 pm Lunch Break	1:45-3:15	3:15-3:30 pm Afternoon Break	3:30-4:15	4:15-4:30	4:30 pm Adjourn
Panel Two **Cyber Protection Problems and Approaches** Moderator: Darlene Quackenbush, IT Planning/ Information Security Officer, James Madison University Wayne Martin, Information Systems Security Officer, University of Virginia Baird McNaught, U.S. Department of Homeland Security, Security Control System Program Manager, Idaho National Laboratories Joy Hughes, Chief Information Officer and Vice President for Information Technology, George Mason University *See panel member bios on beginning on page 84.*		**Panel Three** **Facility Protection Case Studies** Moderator: Mike Becraft, Senior Vice President, Federal Civilian Services Group, Serco North America David Achterberg, PE, Director, Office of Security, Safety and Law Enforcement, Bureau of Reclamation, U.S. Department of the Interior Ollie Gagnon, Protective Security Advisor, Central Florida District, U.S. Department of Homeland Security John Paczkowski, Distinguished Fellow, Naval Post Graduate School at the U.S. Department of Homeland Security; Director, Emergency Management and Security, Port Authority of New York and New Jersey *See panel member bios on beginning on page 84.*		**Afternoon Keynote Address** John R. Stevens, Jr., Deputy Director Centers For Disease Control and Prevention, Office Of Security and Emergency Peparedness (OSEP) *See Mr. Stevens' bio on page 85.*	**Symposium Recap** Dutch Thomas, National Security Consultant	

Academic Program Highlights

Several programs at JMU offer Homeland Security research and educational opportunities.

Public Policy and Administration (http://www.jmu.edu/polisci/publicpolicy.html)

The major in public policy and administration provides students with a general foundation in the nature of the public workplace and its political and legal environments. This major prepares students for professional employment and leadership in government and non-profit organizations. The program provides specialized training in management and management-related skills. Students are encouraged to choose a complementary minor with a narrower, applied focus. The minors recommended for students consideration include criminal justice, environmental information systems, health information systems, political communication, telecommunications, urban and regional studies, communication studies, conflict analysis and intervention, sociology, technical and scientific communication, economics, computer science, public health, and integrated science and technology.

For more information about this program, contact Dr. Gary Kirk – kirkgr@jmu.edu.

Justice Studies (http://www.jmu.edu/justicestudies/)

Justice is a concept that encompasses the principles of fairness, equity, and right action. Both as a personal virtue and a social principle, justice is necessary for sustaining and promoting the growth and development of individuals and communities politically, economically, and socially. To that end the field of Justice Studies provides a framework for the analysis and development of justice. The field of Justice Studies is broad in scope extending from the local level to the international level. Topics of investigation include those aspects of civil life that further the ideals of full citizenship participation and empowerment, the rule of law, human rights, conflict resolution, dialogue and reconciliation, and the integration of personal ethical inquiry and social agency. Through the rigorous empirical and normative analyses of justice and injustice it seeks to help students develop a personal definition of justice, a fuller understanding of the nature of the world in which they live, and identify careers and strategies for action.

For more information about this program, contact justicestudies@jmu.edu.

Information Analysis (http://isat.jmu.edu/IA/index.html)

The B.S. in Information Analysis was created specifically for students who want to become intelligence analysts (in either government or private industry). It will uniquely students equip to engage unrecognized, complex, and multidimensional challenges with innovative, rigorous, and transdisciplinary methods to produce proactive, reliable, and integrated solutions. Students learn to employ an innovative and integrated new information-centric approach to problem-solving by adept navigation through the expanding complex network of data, information, knowledge, and understanding.

For more information about this program, contact Dr. Joe Marchal - marchajh@jmu.edu or Dr. Noel Hendrickson – hendrinx@jmu.edu.

Integrated Science and Technology (http://isat.jmu.edu/isatoverview.html)

Integrated Science and Technology focuses on a wide range of factors in the design and maintenance and protection of complex socio-technical systems. It combines coursework in math, computing and technical fields, such as biological, chemical, physical and engineering, with social knowledge of markets, political processes, to solve concrete human problems of food supply, health, environment, energy, manufacturing, transportation and communications. In the Public Sector, Graduates of ISAT are in demand in local, national and international governmental or non-profit contexts, to analyze policy issues, helping organizations to understand and improve complex regulations. For example, ISAT graduates are working on technical programs in the U.S. Geological Survey, Environmental Protection Agency, U.S. Department of Health and Human Services, U.S. Department of Energy, Military Services and Intelligence agencies, and in regulatory bodies.

For more information about this program, contact Mr. Paul Henriksen - henrikpw@jmu.edu.

Engineering Program (http://www.jmu.edu/engineering/index.html)

Upon graduation from JMU's Engineering Program, alumni will be prepared for a wide range of opportunities in the engineering workforce or in engineering graduate school. Typical fields of engineering that students will be prepared to enter include Applications Engineering, Process Design, Product Design, Process Engineering, Project Engineering, and Systems Engineering. Other industry options include Product Service, Technical Sales, Management Training, and Technical Marketing. A wide range of graduate school options include Master's and PhD programs in Civil Engineering, Environmental Engineering, Industrial Engineering, Materials Engineering, Mechanical Engineering, and Systems Engineering. Other post-graduation options include Business School, Law School, AmeriCorps, Peace Corps, Military Service, Entrepreneurship (starting a small business), Applied Science Fields, International Experiences, Medical School, and careers in Politics/Public Policy.

For more information about this program, contact Ms. Lynn Radocha – radochlm@jmu.edu.

Information Security Master's Program (http://www.infosec.jmu.edu/)

The online distance education Information Security (InfoSec) Master's program at James Madison University caters to the needs of working professionals. JMU InfoSec was established in January 1997. It is one of the first graduate Information Security programs in the nation. 34 students graduated in 1999. Nineteen of those students were Department of Defense employees educated under a contract with the National Security Agency. Also in 1999, the program moved to 100% Internet-based, asynchronous interactive classrooms. Typically, 50% of the students are government employees. Students are never required to attend on-campus classes at JMU. Our classes are available world-wide at anytime. In addition to a Master of Science in Computer Science degree, all graduates receive two NSA approved certificates: Information Systems Security (INFOSEC) Professionals (NSTISSI No. 4011) and Information Systems Security Officers (CNSSI No. 4014).

For more information about this program, contact Ms. Katherine Laycock – laycockr@jmu.edu

Institute
for Infrastructure
and Information Assurance
at James Madison University

2009 Research Summaries

Each year IIIA extends invitations to JMU faculty to participate in the annual request for proposals for summer research funding. The projects chosen for funding for the 2009 cycle are as follows:

Identifying Determinants for the Effective Coordination of Critical Infrastructure Protection Policy

The issue of critical infrastructure protection has presented the Department of Homeland Security (DHS) with a tremendous coordination task. Critical infrastructure has been defined in such a broad manner to include many assets and sectors under federal and non-federal governmental jurisdiction. As such, DHS has created a new policy "regime," the primary goals of which can only be achieved by the effective coordination of numerous federal, state, and local government agencies. This project seeks to understand the factors that lead to effective coordination of critical infrastructure policy. The project proposes to undertake an in-depth analysis of government reports regarding the success and failure of critical infrastructure protection policy. The researchers [PI and graduate student] will identify and code Government Accountability Office reports that detail the implementation of critical infrastructure policy across the 18 critical sectors and key asset areas designated by DHS. The goals of the project are to 1) assess the current landscape of critical infrastructure protection, 2) assist future decision-making about critical infrastructure implementation and 3) develop a set of empirically testable hypotheses for future research.

Contact: Dr. Chris Koski, 540-568-6149, koskicj@jmu.edu

High Speed Cryptographic Hashing via Graphics Cards

A modern video graphics card (usually called a Graphics Processing Unit or GPU) actually contains tens, sometimes hundreds, of processing cores. Each of these processing cores is similar to the CPU in a computer, but much more limited, and the cores typically must operate in lock step with one another. While this is not applicable to most general purpose computer programs, it is a very effective strategy for graphics processing.

Recently the NVIDIA corporation has created an open standard for programming their GPUs. This standard, called CUDA, allows anyone to write programs targeted for NVIDIA GPUs. For certain highly specialized mathematical algorithms, this presents enormous potential. The ESSENCE cryptographic hashing algorithm is particularly well suited for implementation on a GPU because it has been designed for parallel implementation and uses very simple primitive operations (all of which are available on GPU cores). Dr. Martin expects that a well-written implementation of ESSENCE targeted for an NVIDIA GPU will be limited only by the speed at which data can be placed in main memory (a universal limit on all computational tasks). Such an implementation will also have the benefit of off-loading cryptographic function from the CPU.

Contact: Dr. Jason Worth Martin, 540-568-5101, martinjw@jmu.edu

Standardized Operations and Procedures (SOPs) for the use of basic biological, chemical, and radiological detection field tests for the City of Harrisonburg and the Rockingham County Fire and Rescue Departments

Standardized Operation and Procedures (SOP) for the use of basic biological, chemical, and radiological detection field tests will be instituted for both the Harrisonburg and Rockingham Fire and Rescue Departments. The basic radiological course must be taught by a FEMA/DHS certified instructor. These courses of instruction will establish an SOP to ensure consistency in a response to a WMD or Hazardous Materials event. These courses will be taught to all fire and rescue personnel in the city of Harrisonburg, and Rockingham County. The Harrisonburg Fire Department will be covered in each of the three shifts, resulting in 54 Harrisonburg Fire and Rescue personnel being taught. Rockingham County presents a geographical problem due to its size. It is impossible to bring all of the personnel from a shift together for instruction. Thus, the instructor must go to each company and shift to

teach. There are eleven companies with three shifts for a total of seventy personnel that need instruction involving the response of SOPs.

Contact: Dr. Ronald W. Raab, 540-568-2729, raabrw@jmu.edu

A Cyber Defense Competition for Recruiting Under-Represented Students into JMU STEM Program

With IIIA support, JMU hosted a very successful Cyber Defense competition for about thirty JMU students in September 2008. The event allowed JMU to strengthen ties with important industry partners (Computer Sciences Corporation and Gemini Security, both of whom provided attackers for our Red Team) and alumni (one of whom returned to serve on the Red Team). It also provided our students with invaluable experience putting their Information Security knowledge and skills to the test in a realistic environment. Due to this competition, we had a record number of students sign up to be in the JMU Cyber Defense Club this past fall. This event helped our team better prepare, and our team won the qualifying round for the Mid-Atlantic Collegiate Cyber Defense Competition in January, 2009. We would like to build on this successful event by hosting a Cyber Defense competition for high school students from 5-6 Virginia high schools. We plan to invite primarily high schools that serve under-represented students at JMU, and by demonstrating how challenging and interesting Science, Technology, Engineering, and Mathematics can be, we hope to inspire many of these students (and their peers who hear about the competition) to get interested in STEM in general and JMU in particular. We will maintain contact information for participants and survey them two years after the competition to determine how many of them are studying in STEM-related fields and how many are here at JMU. Current JMU students will serve as consultants for each team to provide suggestions and help (as needed) to the high school students.

Contact: Dr. Brett Tjaden, 540-568-2771, tjadenbc@jmu.edu and Dr. M. Hossain Heydari, 540-568-8745, heydarmh@jmu.edu

2009 IIIA Fellows

Institute for Infrastructure and Information Assurance
at James Madison University

The Institute for Infrastructure and Information Assurance welcomes the 2009 class of IIIA Fellows. These researchers have made outstanding contributions to Infrastructure Protection and Information Assurance.

Key criteria for IIIA Fellows include:

- demonstrated significant contributions through scholarship or practice in infrastructure and/or information assurance.
- demonstrated effectiveness as leader and communicator in infrastructure and/or information assurance (including publication).
- demonstrated excellence in and commitment to teaching and mentoring university students.
- demonstrated record of obtaining and managing external research grants.

The Honorable Robert P. Crouch, Jr., Assistant to the Governor for Commonwealth Preparedness, Commonwealth of Virginia

Robert Crouch currently serves as the Counselor to the Governor, where his responsibilities include working as the Governor's office policy lead on Commonwealth Preparedness. Prior to that, he served as the Chief Deputy Secretary of Public Safety, where he Co-chaired both the Commonwealth Preparedness Working Group and the Critical Infrastructure Protection Working Group. In 1993, Crouch was appointed by President Clinton to serve as the U.S. Attorney for the Western District of Virginia. During his eight years in the post, Crouch earned praise for his work to combat cybercrime, money laundering, drug abuse and child pornography. Crouch grew up in Southside Virginia. He holds a law degree from the University of Virginia, a Master of Public Affairs from the University of North Carolina and a bachelor's degree in government from the University of Maryland.

Dr. Chris Holstege, Director of the Division of Medical Toxicology, UVA

Dr. Holstege joined the University of Virginia Department of Emergency Medicine in 1999. He is board certified in Emergency Medicine and Medical Toxicology and holds a joint appointment in the Department of Emergency Medicine and the Department of Pediatrics. Dr. Holstege is one of only two board-certified, full-time medical toxicologists in Virginia. He conducts research in the area of clinical toxicology and manages poisoned patients in his medical practice at the University of Virginia. Dr. Holstege frequently lectures at both the regional and national levels on a variety of topics including agents of chemical terrorism, envenomations, drugs of abuse, and the medical management of the poisoned patient. He has over 100 abstracts and articles published in peer-reviewed medical journals, periodicals, and books. He is actively involved on numerous committees dealing with terrorism and disaster preparedness. Dr. Holstege is a member of the Central & Northwest Regional Virginia Disaster Plan Consortium Task Force, the Virginia Hospital & Healthcare Association Hospital Disaster Preparedness Task Force, the American Heart Association National First Aid Task Force, and the American Academy of Clinical Toxicology Chemical Terrorism Preparedness Task Force. Dr. Holstege received the prestigious National Faculty Teaching Award from the American College of Emergency Physicians in 2002 and the Deans Award for Clinical Excellence from the University of Virginia School of Medicine in 2003.

Lieutenant General Patrick M. Hughes, U.S. Army (Retired)

Lieutenant General Patrick M. Hughes recently joined L-3 Communications, Inc., as the Corporate Vice President for Homeland Security. In that position he is responsible for developing and enhancing Homeland Security and related activities throughout L-3 Communications. Lieutenant General Hughes most recently served as Acting Under Secretary for Information Analysis and Infrastructure Protection and Assistant Secretary for Information Analysis at the Department of Homeland Security. He was the past president of PMH Enterprises LLC, a private consulting firm specializing in intelligence, national security and international relations. He retired from the U.S. Army in 1999 after more than thirty-seven years of military service, beginning as an enlisted soldier and combat medic. His last active duty assignment was Director, Defense Intelligence Agency (DIA), U.S. Department of Defense. Other positions of responsibility included Director of Intelligence (J-2), Joint Staff and DIA; Director of Intelligence (J-2), U.S. Central Command; Commanding General, U.S. Army Intelligence Agency; and Commander, 501st Military Intelligence Brigade.

Lieutenant General Hughes led troops at the squad, platoon, detachment, battalion, brigade, and separate Army and Joint Agency level. He served twice in Vietnam, one tour in Korea, and participated in U.S. military operations Desert Shield/Desert Storm in the Middle East, and in Somalia. He also spent time in Bosnia and other strife-torn locales. He has visited 126 nations and was formally trained in the Vietnamese and Korean languages. His awards and decorations include the Defense Distinguished Service Medal (3 awards), the Silver Star, the Legion of Merit (3 awards), the Bronze Star for Valor (3 awards), the Bronze Star for Meritorious Service (2 awards), the Purple Heart, the Army Commendation Medal for Valor, and the award of the Combat Infantryman's Badge, the Parachute Badge, the Joint Staff Identification Badge and the Army Staff Badge. He is the recipient of the National Intelligence Distinguished Service Medal (2 awards), the Director of the Central Intelligence Agency's Director's Medal, and the Director's Award for Distinguished Service from the Executive Office of the President, Office of National Drug Control Policy. He has been presented with recognition from the United States Secret Service, Immigration & Customs Enforcement, the National Geospatial Intelligence Agency and the National Security Agency. He was recently honored for Distinguished Intelligence Service by Armed Forces Communications & Electronics Association. He has received numerous awards from foreign nations. He is a member of the Military Intelligence Hall of Fame. Lieutenant General Hughes received his Master of Arts in Business Management, and is a graduate of the U.S. Army Command & General Staff College and a two-year War College Fellowship at the School of Advanced Military Studies. He has received honorary doctorates from Montana State University (Business), and the Joint Military Intelligence College (Strategic Intelligence).

The IIIA Fellows

Dr. J. Peter Pham, James Madison University (2006)

Dr. Lennis G. Echterling, James Madison University (2006)

Dr. Massoud Amin, University of Minnesota (2007)

Dr. Michael D. Deaton, James Madison University (2007)

Dr. Mark A. Kirk, University of Virginia (2007)

Dr. Greg B. Saathoff, University of Virginia (2007)

Dr. Frank J. Cilluffo, The George Washington University (2008)

COL (Ret.) Dennis Barlow, James Madison University (2008)

The Honorable John O. Marsh, Jr. (2008)

Ms. Lynda Stanley, National Research Council of the National Academies (2008)

The Honorable Robert P.Crouch, Jr., Commonwealth of Virginia (2009)

Dr. Chris Holstege, Division of Medical Toxicology (2009)

Lieutenant General Patrick M. Hughes, U.S. Army (retired) (2009)

Dr. Malcolm G. Lane, James Madison University (2009)

Dr. Malcolm G. Lane, James Madison University

Dr. Lane began his computer science career with General Electric Corporation in 1965 after receiving his B.S. degree from Davidson College. He worked for IBM Corporation in Research Triangle Park, NC while in graduate school at Duke University. He completed his Ph.D. in Mathematics with an emphasis in Computer Science at Duke in 1971. Dr. Lane joined the Computer Science faculty at West Virginia University in July 1971 on a joint appointment with the WVU Computer Center. He became Professor of Computer Science at WVU in 1978 and remained on the faculty until August 1990.

Dr. Lane began working with foreign governments in automating financial applications in 1983 as a consultant for the Harvard Institute for International Development. He has since worked in over 40 countries on projects funded by the World Bank, UNDP, and USAID. In 1990 he left WVU to become Director of the International Computer Practice at KPMG Peat Marwick in Washington, DC. He became a principal (partner) at KPMG in 1993 and a Managing Director of KPMG LLC in 1994. He joined IBM Corporation as Managing Principal in Global Government Consulting in 1996.

After 10 years in the private sector, Dr. Lane decided to return to the academic community and accepted the position of Professor and Head of the Department of Computer Science at James Madison University in August 2000.

Dr. Lane is President of the WVU CSEE Academy (2003-2005) and Chair of the WVU CSEE Industrial Advisory Committee (2002-2004). He has been an invited lecturer on computer ethics at a number of civic and professional organization meetings in the Shenandoah Valley of Virginia. Dr. Lane's research interests include operating systems, networking and data communications, and software engineering. He is Co-Principal Investigator of the NIST-funded Critical Infrastructure Protection Project at James Madison University.

DELIVERING ON THE PROMISE
Commonwealth of Virginia Innovative Technology Symposium
COVITS2009

IIIA Wins!
2008 COVITS Governor's Innovative Use of Technology in Higher Education Award

Category: Innovative Use of Technology in Higher Education

Winner: James Madison University with August Medical Center and the Virginia Department of Health

For: Pandemic Flu Modeling Partnership

Accepting the award: Dr. John Noftsinger, Vice Provost, James Madison University

Project description: Preparing for response to a health related crisis such as a wide spread flu outbreak requires prior coordination and planning. James Madison University, Augusta Medical Center, and the Virginia Department of Health have developed a unique partnership to provide solutions to surge capacity issues impacting regional hospitals. The Flu Pandemic Model was developed by Patricia Higgins, Cheryl Elliott and four graduate students at JMU's Institute for Infrastructure and Information Assurance. The software enables hospital management to understand the ramifications of a patient surge. Hospitals can use the model to explore different scenarios and the impact a surge can exert on the standard level of care at a particular hospital. The model demonstrates staffing levels of various nursing competencies, hospital bed and medicine availability.

For more information on this project, please see the "Analysis of Perceptions toward the Use of Modeling for Emergency Preparedness Planning" poster, or contact Ms. Patricia Higgins or Ms. Cheryl Elliott.

The Office of the Vice Provost for Research and Public Service facilitates strategic alliances, supports premier research and service centers, enhances the climate and infrastructure to support intellectual property, supports regional economic advancement, and seeks sponsored program funding and research opportunities especially in the following focused areas:

- Biotechnology/health and life sciences;
- Nanotechnology/advanced materials;
- Homeland security and national defense;
- Alternative energy and environmental sustainability;
- Education reform in science, technology, engineering, and math; and
- Accountability and outcomes assessment.

VISION STATEMENT: Our vision is to be an engaged leader in higher education scholarship, with an emphasis on innovative discovery benefiting society.

MISSION STATEMENT: Our mission is to develop and advance academic and scholarly endeavors by leveraging resources through research, public service and engagement to foster innovative discovery and advancement for the university, local, regional, state, national and global communities.

VALUES: Utilizing a student-centered, applied and interdisciplinary approach, we are an engaged, respectful and passionate community that values:

...Innovation...Empowerment...Impact...Integrity...Service...Stewardship...

Research and Public Service

Institute for Infrastructure and Information Assurance
The Institute for Infrastructure and Information Assurance (IIIA) facilitates development, coordination, integration and funding of homeland security activities and capabilities of the James Madison University academic community to enhance information and critical infrastructure assurance at the federal, state and local levels.
Executive Director: Dr. John B. Noftsinger, Jr., 540-568-2700, noftsijb@jmu.edu
http://www.jmu.edu/iiia/

Center for Assessment and Research Studies
The Center for Assessment and Research Studies (CARS) supports assessment related to each of these stages: 1) matriculating student assessment during summer orientation for all entering freshmen; 2) mid undergraduate point assessment in February; 3) graduating senior assessment in the academic major(s); and 4) regular surveys of alumni.
Executive Director: Dr. Donna Sundre, 540-568-3483, sundredl@jmu.edu
http://www.jmu.edu/assessment/

Economic Development and Partnership Programs
The Office of Economic Development and Partnership Programs makes the resources of James Madison University available to the greater Shenandoah Valley in support of economic development which is culturally and socially acceptable to the region.
Director of Community Partnerships: Ms. Elizabeth Knight, 540-568-2702, knighteb@jmu.edu
http://www.jmu.edu/research/econdev/

Institute for National Security Analysis
The fundamental purpose of the Institute for National Security Analysis (INSA) is to discover, develop, and deliver new analytic methods to our national security community. INSA offers support for the most central (and neglected) element of Defense and Intelligence analysis: the cognitive process by which analysts reason to well-justified conclusions for their decision makers.
Director: Dr. Noel Hendrickson, 540-568-8941, hendrinx@jmu.edu

James Madison Center
The James Madison Center was founded in 1999 to honor the legacy of the nation's fourth President and Father of the United States Constitution. It serves as a repository for information on Madison's life and times (1751-1836) as well as that of the Federalist Era.
Director: Mr. Philip Bigler, 540-568-2549, biglerpb@jmu.edu
http://www.jmu.edu/madison/center/

CISR/Mine Action Information Center
The Mine Action Information Center (MAIC) is a public policy center which manages information and conducts training relevant to humanitarian mine clearance, victim assistance, mine risk reduction and other landmine-related issues.
Director: COL (Ret.) Dennis Barlow, 540-568-2718, maic@jmu.edu
http://www.maic.jmu.edu/

Outreach and Engagement
The Office of Outreach and Engagement supports, facilitates and promotes excellence in lifelong education through programs of distinction, innovative outreach programs, and a diverse student body.
Associate Vice Provost: Dr. James Shaeffer, 540-568-4251, shaeffjm@jmu.edu
http://www.jmu.edu/continuingeducation/

Research Compliance
The ORC serves the JMU research community by coordinating institution-wide research compliance policies and procedures development, and by partnering with researchers, so that the University is compliant with federal, state, and local laws and regulations as well as University policies.
Director: Ms. Patricia Buennemeyer, CRA, 540-568-7025, buennepd@jmu.edu
http://www.jmu.edu/sponsprog/complianceplan.html

Research Development
The Office of Research Development builds collaborative interdisciplinary teams to pursue a variety of externally sponsored opportunities, facilitates research and development opportunities for faculty, staff and student researchers to promote the growth of JMU's sponsored research activities and faculty career development, and assists in identifying and responding to strategic initiatives.
Director: Mr. Kenneth Newbold, 540-568-1739, newbolkf@jmu.edu
http://www.jmu.edu/research/

Shenandoah Valley Partnership
The Shenandoah Valley Partnership (SVP) is a regional economic development partnership for the central Shenandoah Valley whose purpose is to market the valley for economic development purposes.
Executive Director: Mr. Robin Sullenberger, 540-568-3100, svp@jmu.edu
http://www.shenandoah-valley.biz

Shenandoah Valley Technology Council
The Shenandoah Valley Technology Council (SVTC) is a non-profit membership organization, helping technology businesses in the area succeed and grow.
Director: Ms. Nicky Swayne, 540-568-7882, swaynece@jmu.edu
http://www.svtc-va.org

Sponsored Program Administration and Accounting

The Office of Sponsored Program Administration and Accounting provides support for research opportunities and sponsored research-related information to James Madison University faculty, staff and students.
Director: Mr. John Hulvey, 540-568-6872, hulveyjd@jmu.edu
http://www.jmu.edu/sponsprog

SRI Partnership
James Madison University has developed a unique collaboration with SRI International to enhance research and economic development opportunities within the Shenandoah Valley.
Executive Director: Dr. Krishna Kodukula, 540-568-5757, kodukukx@jmu.edu
http://www.sri.com/

Technology Transfer
The Office of Technology Transfer (OTT) promotes innovation, enhances research by connecting inventors and industry, and fosters economic development through protecting and commercializing intellectual property in an efficient and effective manner.
Director: Ms. Mary Lou Bourne, 540-568-2865, bourneml@jmu.edu
http://www.jmu.edu/ott/

Dr. John B. Noftsinger, Jr.
Vice Provost for Research and Public Service
MSC 4107, Harrisonburg, VA 22807
Phone: 540-568-2700; noftsijb@jmu.edu
www.jmu.edu/research

Section III: Symposium Appendices

In this section, you will find the symposium transcripts, presenter bios, and research posters.

Welcome and Introduction

DR. GEORGE H. BAKER: I welcome you on behalf of the National Academies' Federal Facilities Council and James Madison University's Institute for Infrastructure and Information Assurance. This is our fourth annual Homeland Security Symposium, this year focusing on the protection of large facility complexes. We greatly appreciate each of you being here.

I am George Baker and will be serving as today's master of ceremonies. I'm on the faculty at James Madison University and also serve as the Technical Director of JMU's Institute for Infrastructure and Information Assurance.

I hope you won't mind if I take an academic approach to the agenda today. I have class assignments for everyone here. My assignment, and it is a rather daunting one, is to reinforce today's schedule - to keep us on time. Your assignment, and I'm speaking to each one here, is to interact. We find that the main value of this kind of event is the interaction among different people representing diverse disciplines. We find at the university that in many instances, solutions that nobody ever thought of result just from this kind of interaction.

To help you with your assignment, we have developed some tools for you to encourage interaction here. First, we have refreshments in our exhibit hall behind you. By the way, it is quite acceptable to bring refreshments into the lecture hall. We also have enlisted some media relations people here who just may approach you for an interview. We are trying to get some of your thoughts captured on tape – so heads up; the media folks are gunning for you. That includes everyone. We also have instructions for Twittering, another form of interaction, on page two of your program. I encourage you to pay particular attention to the program. There is a lot of information there.

Today's topic is one of particular concern and interest: the protection of large facility complexes. Planning this event, we felt like we were getting a "facility complex" – to use psychological terminology. We hope that today's agenda will help provide the cure. But we have this problem - when facilities become large, simple point defense is no longer adequate. We're now dealing with networks. We have, as Charles Perot coined the phrase, vulnerability of complexity. And it is a very, very challenging set of problems.

And now I would like to introduce the two principal motivators and enablers of this event: Lynda Stanley of the National Academies and John Noftsinger of James Madison University. The bios for Lynda and John are included in your programs.

Briefly, Lynda Stanley is the Director of the National Academies' Board on Infrastructure and the Constructed Environment. This is an arm of the National Research Council which is the operating organization of the National Academies. She served for ten years as the Director of the Federal Facilities Council. The FFC is a cooperative association of the 27 federal agencies with the mission to identify advanced technology and policy to improve federal facilities over their entire life cycle.

Lynda will be followed by John Noftsinger. He is the Vice Provost of James Madison University. In this position, John directs all university research and public service programs. Because of John, there is an interesting confluence of research and public service at JMU. John is concerned that our research should be performed with public service in mind. I must say that this has been an effective combination. Dr. Noftsinger is in charge of all university grants and contracts. He cofounded the Mid-Atlantic Accelerating Innovation Foundation, the Virginia Technology Alliance, and the Shenandoah Valley Technology Council. He co-chaired Mark Warner's Virginia Research and Technology Advisory Commission, and he serves as the Executive Director of our Institute.

DR. JOHN B. NOFTSINGER: Thank you, Dr. Baker. I appreciate your leadership in our program.

It is a pleasure to welcome you to our fourth Symposium in partnership with the National Academies. The theme as you know is protecting large-scale facilities. It is a true partnership between our Institute and the Federal Facilities Council at the National Academies.

In a moment you will hear from Lynda Stanley. I would like to recognize Lynda for her outstanding assistance. She is a true selfless partner, and none of this unique relationship that our university has with her office would be possible without her creativity and her commitment. Our presence in this wonderful facility today is due to Linda's efforts. Because the National Academies is under renovation, she was able get us into the Convention Center. This is my first experience with the DC Convention Center and I must say that I am quite impressed.

As many of you know, the Institute for Infrastructure and Information Assurance at James Madison is a coordinating organization for our university in the increasingly vital area of homeland security. We provide a catalyzing point for leading our security research within the broad context of improving both infrastructure and information assurance.

We find that the intersection of information security and physical infrastructure is a very complex area, and something that our faculty and our students get very excited about.

In addition to Lynda's efforts, I would also like to acknowledge the efforts of the IIIA staff. I marvel at their energy and their creativity in putting together this program. It starts the day after we finish here. They look at your responses and start planning for the following year's event.

I would also like to acknowledge that the IIIA was born in a partnership with George Mason University. The former chief research officer there and myself had this idea that we could do more together than we could separately. President Steger and I were chatting this morning at breakfast about universities getting a bad rap for not collaborating. If we have a reason to collaborate, the necessary trust is there and we do work together. As he said this morning, when there is a defined reason to collaborate, the institutions in Virginia, especially the public institutions, are very good at it. We are in our eighth year of our collaboration with George Mason. You will hear from Joy Hughes, George Mason's CIO, later today.

This event builds on the past three events. Our first homeland security symposium looked at grassroots planning for emergency preparedness. The second addressed preventing and responding to cascading infrastructure failures. Last year's symposium was devoted to encouraging public-private partnerships. This year's theme, "protecting large-scale facility complexes," provides something of a capstone, addressing elements of our three previous symposia.

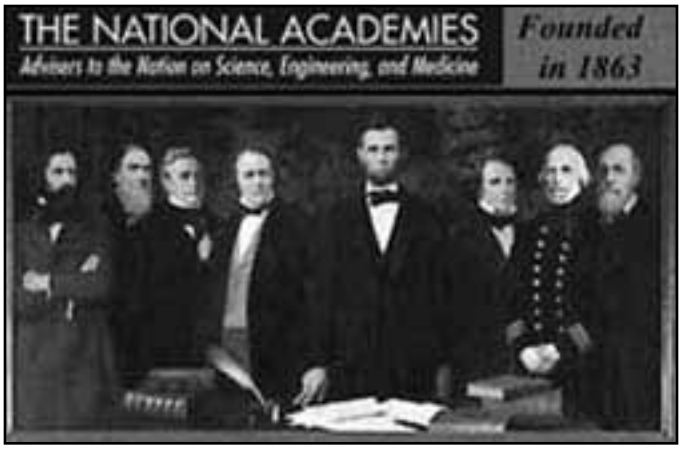
Following our tradition, we have assembled internationally recognized panelists here in the heart of our Capital. It is our goal to bring insight to causes and solutions of real and challenging infrastructure assurance problems. If you have been reading the headlines, you know that the problems that we have been studying are very real and apparently growing. We are now in the course of a flu pandemic. We have been modeling surge preparedness for medical systems through our program. There has been a security breach in Virginia's health records. There have been foreign nationals tampering with control systems within our national power grid. These problems are not hypothetical and are made more challenging by the interconnectedness of our world.

I am very pleased that today's program, through the planned agenda and your conversations and interactions, will provide occasion for improving our collective understanding and developing innovative solutions to the real security problems confronting large facility complexes. I thank each of you for being here. I know how many events you are invited to and the effort that it takes to come into the heart of downtown Washington. On behalf of the university, thank you for your presence and contributions to homeland security.

At this time, I would like to turn the podium over to Lynda Stanley of the National Research Council.

MS. LYNDA STANLEY: Thank you all very much. I also want to extend my welcome. I am very pleased that you are all here this morning, very pleased to see the mix of federal people and people from academia and from the private sector. It is a really good group that we have here today.

I would just like to build on what George said, in terms of taking the advantage of this group and networking and talking to each other about what is going on, because there is a lot of good information. There is no one in this room who doesn't have a lot of information to share and who isn't doing really great work. So you ought to be talking to each other.



Just very briefly, the reason this picture is here, obviously in Washington this year and probably around the country, our 200th anniversary of Lincoln's birth is quite a big deal. We are always very proud at the Academies to talk about the fact that Lincoln did sign the charter that established the National Academies in 1863, with the idea that we would be providing independent and objective advice to the federal government and to others on all issues of science and technology – and that we would bring together the best minds in the country to do that. That is essentially what we have always been about and still are today, although the issues have changed and the way we do things has

changed a little bit. We still have the same overall mission.

There are actually four groups comprising "The Academies." It always gets very confusing when we talk about the Academies. It is actually the National Academy of Sciences, the Academy of Engineering, and the Institute of Medicine; all of which are honorific bodies. You are elected to those bodies based on your contributions to society and to your field. The National Research Council is the staff. We are the group that gets to work with all the honorific people and all the real experts, and it is a real joy to do that.

The Federal Facilities Council has been around for over fifty years now. It started out as the Federal Construction Council. We operate under the Board on Infrastructure and the Constructed Environment. As George said, our mission is to identify and advance technologies, processes, and practices that are going to improve federal facilities from concept all the way through demolition.

We do that by helping to organize events like this. These events come about through collaboration. Our agencies inform us of subjects that would be of interest to them, and then we work to bring together the right people and pass along the information they need.

We convene standing committees. We have five of them, one of which is on physical security and hazard mitigation. This committee was key in helping today and deciding on topics. And we disseminate our findings through reports, all of which are published by the National Academies Press and available on our website. You can get a free executive summary online for every report that we publish – beyond that we do charge for reports. If there is something you really want, you can give me a call and I might be able to get you a copy.

We are sponsored by twenty-seven agencies. It includes all the major defense groups and the major civilian groups that own facilities such as the GSA, the State Department, and groups like the Smithsonian, the Indian Health Service, and NASA. It is a diverse group, but they all have common interests in terms of how they manage their facilities. What we are really about is getting them together in an independent forum to talk about their issues and find common ways of solving some of those issues to the extent possible. We do have a website. Our reports are all published there.

I just wanted to let you know that here today is Doug Hall, who is the Chair of our Physical Security and Hazard Mitigation Committee. You will be hearing from him at the end of the day. He is going to be helping to summarize today's proceedings.

With that, I will turn it back to John Noftsinger to introduce our keynote speaker.

DR. NOFTSINGER: Lynda, thank you for sharing that context and background on the National Academies. If you have ever been in the National Academies special board room you've seen the portrait of Lincoln with the founders of the National Academies. For me personally it is very moving because it makes me realize that in the midst of a civil war, Lincoln was such a visionary leader to move beyond the strife and a war-torn country and look to the future and what science and technology could do. I don't think he was probably very popular to actually sign that charter in those times, when the people were thinking that maybe he needed to be focused on other matters. For me, to see that picture of him both in your building and here is very inspiring.

Our first speaker is a person that has been tested in some of the most extreme situations, a person whose humanity and leadership have shown through in the most difficult situation on national television, and a person that I, from my days as an aspiring college administrator, have learned to admire. I am impressed with Dr. Steger's humility and his ability to just sit down and talk to you like a regular person. If you hold any preconceptions about university presidents being unapproachable, you will be pleasantly surprised by Charles Steger. He is a wonderful person to sit down with and talk to about life in general.

So it is my honor to introduce Dr. Steger. He is a long time friend and a mentor to James Madison's President, Linwood Rose. Dr. Steger and I were talking in the hotel last night about Dr. Rose and his service as President at James Madison, and I was so proud to hear him talk about one of his highly successful Virginia Tech graduates. Because Dr. Rose is a graduate of Virginia Tech, there has been a long history of collaboration between James Madison and Virginia Tech. We took their graduate to be our President. Also, they took our first president, Julian Burruss, to be their president in 1918.

In the year 2000, Dr. Steger became Virginia Tech's 15th president. He possesses both breadth and experience in all three missions of the university: teaching, research and service. In addition, he has international experience combined with a long history of engagement in both the state and federal government. He has a unique record of accomplishment and is a visionary thinker with concrete achievements. He also established Virginia Tech's

research and public service office in downtown Richmond. He gave support to start the Virginia Bioinformatics Institute, whose first phase of investment exceeded $39 million, bringing together the exciting new disciplines of biotechnology and information technology. The Institute holds great promise in the prevention and treatment of disease, expansion of the world's food supply, and protection of the environment.

Dr. Steger's previous position is as Vice President for Development and University Relations. He directed the university's successful capital campaign, raising $337 million, exceeding the $250 million goal by 35 percent. It is the most successful fundraising endeavor in the university's history, with 71,000 donors and 500 volunteers in the six-year effort.

Dr. Steger has been appointed by two governors of Virginia to serve on important commissions. The most recent was the Governor's Commission on Population Growth and Development, where he served on the executive committee.

Dr. Steger's ties to Virginia Tech are broad and deep, and they span four decades. He has been a student, teaching faculty, academic dean, department head, vice president and now, president. While faculty member, he won two teaching excellence awards – if you are at a university, those are the highest, most cherished awards. He authored a portion of a textbook which is now adopted by 230 universities, in its seventh edition. When he became dean of the College of Architecture and Urban Studies in 1981, he was the youngest dean of any college of architecture in America.

Twenty years ago, Dr. Steger was inducted into the College of Fellows of the American Institute of Architects. He has spent two decades since employing his architectural skills in both sketching and vision, and designing the plans for Virginia Tech. Most recently he has been asked by the Swiss Ambassador to the U.S. and the World Bank to serve on a committee to establish a foundation in the United States to conduct research on mitigating global disasters.

It is my honor to welcome President Charles Steger.

Morning Keynote Address

DR. CHARLES STEGER: Thank you, John. It is a real pleasure for me to be with you this morning. I appreciate the invitation. I appreciate the kind introduction. I want to thank all the folks at James Madison and also the Federal Facilities Council for inviting me to speak at what I think is a very important function.

The academic year is coming to an end this coming Friday and Saturday. We are going to graduate about 6,000 undergraduate and graduate students. I have been teaching a class this past spring and have just submitted my grades, which is the worst part of teaching.

Last year I did a seminar. We have an activity called the freshman book project in which every incoming freshman reads the same book. We then conduct symposia to discuss the ideas in the book. Last year's symposium focused on a book called Einstein's Dreams. The book had different chapters on various conceptions of time. The session I was involved in addressed the issue, "if you had just one day left to live, how would you spend your time on earth?"

So I had this group of students. A couple of them raised their hands and presented some interesting ideas. One young lady said that if she just had one day to live, she would spend it in my class on Urban Systems Dynamics – a class I actually did teach, by the way. I replied, "Well, that is interesting, but why on earth would you want to do that?" She said, "Because I have heard that every moment in your class seems like an eternity." So I hope I won't have that impact on you today.

I remember a preparedness slogan from a few years ago that stated, "Don't be afraid, but be ready." Terrorism targets our psychological as well as our physical well-being. In fact, the fear generated by unpredictable acts is one of the key goals of terrorism. We all know, though, that we can't be frozen by our fears, as nightmarish as they might be, and being ready is one of the reasons we are all here today.

I think it is very significant that we have people from state, federal, local governments and academic institutions participating. Each person here has his or her own special perspective and expertise. What we can do in terms of sharing this information, the best practices and ideas, I am convinced, can make a substantive contribution to all of our efforts.

Abraham Lincoln said in a message to Congress on December 1 of 1862, "As our case is new, so must we think anew and act anew." Whenever threats are received or tragedies occur or are reported, it is often very difficult, as we all know, for the public to grasp the scale and the complexity inherent in securing facilities. The incident could range from an operation with a single building to a campus

like Virginia Tech with several thousand acres. We have 156 major buildings and a population of users, students, faculty, staff, contractors, et cetera, on a typical workday of 40,000 to 45,000 people.

A further point of interest. We have students enrolled at Tech, as most public institutions do, from over one hundred different countries around the world. Those of us who are responsible for the management of these large scale facilities are running small cities. Our facilities are intertwined with the surrounding community and, in fact, some campuses are larger than the surrounding community – which is the case with Blacksburg.

At Virginia Tech, in addition to the main campus we have an airport, we have an airport authority, we have a regional water authority, we have a sewer authority. We own the Virginia Tech electric service which provides power to a large portion of the surrounding community. We own a corporate research center with 160 companies and 2,000 employees. We own and operate two hotels and two golf courses. All of this together falls under the institutional umbrella. I say this to give you some sense of the complexity of the enterprise. This complexity is not unique to us, it is characteristic of all major institutions. Many public universities and federal and state facilities have the same array of complex arrangements and entities. My point in enumerating these items is that the scale and the complexity of the operations is not readily perceived or really understood by the public.

When we look at some of the reports or events that go on around the country, people will say facility X went into lockdown mode during an emergency. We don't really know what that means. If you have an enterprise of a few buildings, it is certainly possible to do that. But when you have to control, as in our case, an unfenced perimeter of six miles, lockdown has much more difficult implications. If you took the time and the resources to secure it, it would probably be three days later.

In thinking about risk management strategies, we have to consider the interdependence of systems – of critical infrastructure – and as was pointed out earlier, the vulnerability of our cyber networks. Since the elimination of all risk is really impossible, there are several basic questions that we need to ask. For instance, what do we mean by 'securing' a facility? More importantly, what is the appropriate tradeoff – and this is one of the really hard ones – what is the appropriate tradeoff equation that balances safety, security and cost with the risk that you are reducing?

For a start, we need to consider the problem in terms of different levels and classes of risk. We must avoid setting the expectation of providing security that is absolute. The threats we face are too diverse, they are too deadly and, in many instances, too difficult to detect to secure every possible target. It is simply not possible. Although the public at large does not understand this, I think we all realize that we cannot protect everyone everywhere all the time.

I realize it is early in the morning, but I am going to give you a little test just to get things going. There is a train that is going down the track, and in the compartment of the train are three individuals. One is the Easter Bunny, the second is a high-priced lawyer and the third is a low-priced lawyer. There is a stack of money on the table in the compartment. The train goes through a tunnel and it becomes completely dark inside the compartment. There is scrambling and shuffling around, and when the train comes out of the tunnel, the money is missing. The test question to you is: "who stole the money?" … the correct answer is: "the high-priced lawyer." This is because the Easter Bunny and the low-priced lawyer are just figments of your imagination. My point is it is simply not possible; it is unfair and unreasonable to propose or to expect that we can achieve absolute security. Absolute security is a figment of our imaginations.

All of you know that we can look at these issues in terms of three stages in time. One is the general security preparations before the incident. The second is the management of the incident itself, and the third, of course is the post-incident management. I am going to focus the majority of what I have to say on stage one - the preparations before the incident. This is the phase that has been most affected by the broader public policy questions.

Since the tragedy of April 16 in 2007 that occurred on our campus, we have expended over $15 million on facilities and added additional staff to try to reduce the risk of further incidents. This number does not include the many millions of dollars for the staff time of people who already work for us. We hope that this investment will reduce the probability of a future incident.

After the shootings, I commissioned three groups to look at all aspects of issues that ranged from communications to physical infrastructure to the interface between counseling services and judicial affairs. Governor Kaine also put together an investigative panel. These four studies together resulted in over 300 recommendations. We went through an elaborate process to evaluate and

prioritize the recommendations, and also to manage the costs. The costs would have been many, many millions more if we had implemented everything or if all the recommendations had been feasible.

All the recommendations were considered. The ones that were viable we have put in place or are being put in place as I speak. Let me give you a couple of examples of the resulting security upgrades. These are problems that all of you face. Prior to the attack, the person that did the shooting chained several of the doors together to keep people from leaving the building. We have replaced the panic bars on 1800 doors on our campus so that they can no longer be chained together. In fact, one of the constraints was that the manufacturers of the new panic bars didn't have the capacity to produce enough for us. We installed sirens on campus. We have a VT alert system which sends messages to cell phones, computers, et cetera. We have increased the staffing of police and strengthened our threat assessment team and added staff to the counseling center. All of this is a commendable effort. It is being done by every major institution across America these days.

Further, when you consider that we must manage the risk of other types of threats, such as natural disasters, flooding and hurricanes, pandemic flu outbreaks, as well as terrorists, how should an organization allocate its assets across this range of potential problems? Risk must be managed knowing full well that all hazard protection, response, and recovery strategies require the development of training and exercise regimens if you are going to be effective when the event occurs.

Just to put this in some perspective, our security improvement expenditures amounted to $500 for every student in the university. Students pay tuition and a comprehensive fee. The comprehensive fee, which covers health services and bus fare and athletics and everything else, is only $480. So we spent $500 additionally per student on the security features. The state was able to provide about a million dollars. The state has many demands on its resources, as we all know, so the rest of that was absorbed in our own budget. When people ask why tuition is going up faster than inflation, improved security is a significant factor. Literally every institution across the country has put in these alert systems.

Two other important questions are how much investment is enough and what are the tradeoffs? In the 2008 book, Terrorism, Economic Development and Political Openness, two economics professors, Todd Sandler and Walter Enders, concluded that the economic costs of terrorism in rich countries like the U.S. are relatively low compared to the economic costs of combating terrorism. For example, the attacks of September 11, 2001 had significant cost, of course, estimated between $80 and $90 billion. But the cumulative costs were a small percentage of the U.S. GDP, which approaches ten trillion dollars.

The direct costs of the 9/11 attacks included damaged goods, the value of lives lost, the costs associated with injuries, et cetera. Attack-related secondary or indirect costs due to subsequent losses are also significant and include things like higher insurance premiums, increased security costs, greater compensation for those at high risk locations, and costs tied to attack-induced long range changes in commerce. Indirect costs may surface as reduced growth in GDP, loss of foreign investment, changes in inflation or increased unemployment.

As I indicated, in the past two years Virginia Tech has expended some $15 million to increase the security on our campus. We are looking at all kinds of new mechanisms in terms of threat assessment and emergency notification systems. But the cost to the organization and the community is far greater in terms of the emotional cost that it has and effects on human behavior.

The Pentagon recently announced that it spent more than $100 million in just the last six months responding to and repairing damage from cyber attacks and other computer network problems. Military officials said that they are only beginning to track the costs that are triggered by the constant daily cyber attacks against military networks, ranging from the Pentagon to bases around the country. You may find this difficult to believe, as I did when I first was briefed on the issue by our own IT people, but we receive 35,000 attacks on our computing systems per day that originate from around the world. Someone – it could be an individual or an organization – is trying to hack into our systems. Even if significant expenditures are made to deal with this, how do you measure the impact of the security measures on the openness of a place like a university or other large facilities?

Then there is another critical question. How much liberty and personal privacy are we willing to sacrifice to achieve incremental improvements in security? This is a major public policy question that we are all going to be debating for years to come.

It has been said that nothing is so threatening to individual liberty as extended war, and we are indeed in an extended war on terror. Almost all credible assessments that I have seen say these threats are going to continue and, in fact, will probably increase. Today we have our bags

inspected at airports and we have to remove our shoes to pass through metal detectors. You enter a federal courthouse and your briefcase is going to be opened and inspected.

At our Lane Stadium where we play football, you cannot bring bags or containers inside the gates, and even baby strollers are examined. The next step, we may need to start inspecting emails and telephone calls. Can we really stop every visitor, delivery truck or parent as they come in the campus? The answer, of course, is no.

To assist in sharpening the issue a little bit, looking at some of the problems that we face in making these tradeoff decisions, I offer this hypothetical but not improbable example. Imagine that it is Friday evening at the Virginia Tech campus before a big football game on Saturday. We receive a credible threat of a possible suicide bomber with the Virginia Tech game as a possible target. We don't know the identity of the potential bomber. Clearly we hope never to face such a situation, but a suicide bombing near a university football stadium has already occurred in another part of this country.

How does one even begin to think about such a horrendous possibility? In looking at that scenario, what measures do we take to try to prevent this from happening? Before football games now we have bomb sniffing dogs go through the stadium, security guards check everyone going into the stadium. However, when you are managing the attendance of 66,000 people to each game, the inspection is really only cursory. Further, a concentration of people waiting to go into the stadium at the screening point is as dense as it is once they have gone through the checkpoint. So the screening may have little or no effect if the bomber chooses to set off the bomb in the dense crowds outside of this perimeter. You can move the perimeter farther away and have more entry points, but the basic problem doesn't go away. The level of screening could be more intense. We could put everybody through metal detectors and cause an increased delay, but there is a point where all this becomes counterproductive.

To reiterate – the question is how much individual liberty and personal privacy are we willing to sacrifice to advance incremental improvements in security? It was instructive to me that not too many months after the April 16 tragedy, we were looking at putting in surveillance cameras in various parts of the campus. This measure was strongly opposed by our students. We can reduce the risk of the suicide bomber succeeding at the football game with some deterrent measures. Most importantly, we can increase the level of awareness of the public in general. But just think about on a cold November day, when the fans are wearing heavy coats and carrying blankets, the possibility of detection and interception is pretty low. The very sad reality is that if an individual is intent on taking his or her own life, there is not a great deal anyone can do to stop them from threatening the lives of others in the process.

My conclusion from this example is that the protection of large-scale facilities cannot be done in isolation. Obviously we have to do everything we reasonably can do, but local measures must be part of a broader national framework that is operational well before any incident occurs.

By using this example, one can begin to approach the issues of homeland security in general and some of the public policy questions. Enhancing the public awareness of a threat, as many of you well know, comes with its own set of complex issues. A broad-based public education program presented outside the context of an immediate threat or crisis can certainly be of value. It becomes increasingly difficult, for example, if a serious threat is identified and the suspect is not known.

Think about issuing a warning to a crowd of 66,000 people, that could result in panic and loss of life through stampeding and heart attacks. The heart attacks occur at almost every game when that many people are together. And the warning may do nothing to prevent the attack. In any crisis, the decision maker is faced with the dilemma of how long to wait to get accurate information and to advise the public on the proper course of action. My sense is that it is really almost a case by case judgment call.

I recall vividly an event in August of 2006 when we had a shooting near campus. The person of interest had been hiding. Nobody knew where they were for at least 24 hours. There were all kinds of false sightings reported. It was reported to me that one of our custodians thought somebody was hiding under the stage in the auditorium in the Student Activities Building. That rumor was circulating around the building. We have a branch bank in this building. A teller was talking with her mother, and happened to say that they thought the shooter was holding someone hostage. The mother on the phone thought the daughter was being held hostage. This is how it escalates. This is a true story. So all of a sudden, based on rumor, somebody decides to evacuate the building. The mother had called 911 and a SWAT team was dispatched to the building. I hate to think what could have happened if a car had backfired. Receiving and verifying accurate and timely information is a real challenge that we all face. Obviously the warnings have to be timely, but it is also important that they be accurate.

If I may also take a slightly divergent path for a moment to raise what I believe will prove to be a serious problem regarding warning and warning systems. Since the incident on our campus on April 16, 2007 the mindset of universities across America has changed forever. As you remember, it was the worst mass shooting ever in the history of the United States.

Every major university has installed some form of alert system. Now that this notification capability is in place, what happens if you attempt to use the system and it fails, which does happen? We test this system regularly and sometimes it doesn't work. Thus, a complete new level of liability has been created. Some would say, the answer is to have redundant systems, and that is part of the solution. But then how many redundant systems should we have? How much is enough, and how much are we willing to spend to do all that? So we are facing a new set of issues.

In a recent Council on Foreign Relations working paper, Daniel Prieto, a Senior Fellow for counterterrorism on national security at the Council, maintains that counterterrorism policies are sustainable over the long term only if policy makers design them with the co-equal objectives of improving national security and protecting civil liberties. Any policy or program that consistently prioritizes one objective over the other is not going to be durable in the long term, and eventually will fail the country on both counts.

What about the sharing of information that goes on in the fusion centers which, among other purposes, were created to exchange information and intelligence and improve the ability to fight crime and terrorism by merging data from various sources? Last month the ACLU called for an internal investigation of these centers, claiming – this is a quote – "fusion centers have experienced mission creep in the last several years, becoming more of a threat than a security device. With no overarching guidelines to restrict or direct them, these centers put Americans' privacy at huge risk."

Other civil liberties groups have sued the Department of Homeland Security, seeking access to public records on the questioning and searching of U.S. travelers. These suits were in response to complaints from U.S. residents who claimed that they were grilled about their families, religious practices, volunteer activities, political beliefs and so on when returning to the United States from travel abroad. In addition, it is alleged that Customs agents examined and sometimes made copies of travelers' books, business cards collected from friends and colleagues, handwritten notes, photos, et cetera.

Time and again the National Security Agency has been at the center of controversy, if not lawsuits, over whether it has the right or how much right it has to intercept telephone and Internet communications of Americans without a court warrant. These are not just at issue on the national level. A few weeks ago, the New York Times reported that a growing number of big city police departments and other law enforcement agencies across the country are embracing a new system to report suspicious activities that officials say could uncover terrorist plots, but that civil liberties groups contend might violate individual rights. The ACLU and other rights groups warn that the program raises serious privacy and civil liberties concerns. The behaviors identified – and this is a quote from ACLU – "are so commonplace and ordinary that the monitoring or reporting of them is scarcely any less absurd." That was in a report they put out last July.

We also think about cyber attacks and threats to our critical infrastructure systems. They multiply both the complexity of our task and the serious damage that can be done to the large-scale facilities we manage but often provide support for critical infrastructure. For example, [our cyber network] ranges from having very sensitive data on research projects in our computing systems to providing electricity to the town, the university and surrounding community. Although we have had many stories in the media recently about cyber spies infiltrating our power grid, those who work in the information technology security area know that this threat has existed for many years.

We don't have to wait for a successful cyber attack, however, to imagine the consequences. We got a chilling glimpse of what could happen in the summer of 2003 in the Northeast Blackout. It was the largest blackout in North American history, affecting an estimated ten million people in the Canadian province of Ontario, which is one third of the population of Canada, by the way, and 40 million people in eight states, which is about one-seventh of the population of the U.S. According to the official analysis of the blackout, more than 508 generating units and 265 power plants, including more than 20 nuclear reactors, were shut down.

During the blackout, some other essential services remained semi-operational in some areas, although backup generators were frequently not up to the task. The phone system continued to function in some areas, but the circuits were overloaded. Water systems in some cities lost pressure. Cellular providers continued to provide standby service, but the systems were overloaded. Interestingly, televisions and radio stations remained on the air with their backup generators, but the fact that

the public didn't have electricity themselves meant that the people most in need of the news were unable to receive the broadcast. Most interstate passenger rail transportation was affected or shut down, and the power outages continued to affect international air travel and whatever else. Thankfully, there was no immediate direct threat to human life, but this gives you a sense of the magnitude of this type of infrastructure failure.

Certainly, as I hope I have pointed out, there are a huge number of variables that need to be considered and monitored when we think about how to protect our facilities and our people. Today we are developing mechanisms and technologies that will help us to comprehend the variables and make the best decisions possible.

I wanted to just take a minute or two and tell you about a new center that we are creating between IBM, Virginia Tech and Arlington County. We are working together to establish a research laboratory called the Center for Community Safety and Resilience that will focus on advanced research and systems for routine and crisis event management with local, regional and national impact. The partners and future collaborators, of which there will be many, will engage in basic and applied research that focuses on what we have labeled "community resilience informatics." This is a field that is being created as we speak. But it will conduct policy and studies and social systems research to look at issues of distributed decision making, systems, linkages, cascading effects of failing infrastructure, as well as the issues of privacy and civil liberties. We will use real world data that is available in the public domain to develop a set of tools to monitor what is going on.

Now, the two things that are probably obviously to everyone in this room are first, to monitor these types of things, the amount of data to be collected and examined is massive; and second, the amount of computing capability is going up exponentially, if you are going to track and look for patterns to anticipate as well as manage crises when they occur. We are going to hopefully try to transform the community's resiliency capability through the data integration of cloud computing and virtual technology, and develop a set of standard consumable commercial capabilities that you don't have to have a Ph.D. in computer science to use. You could be most anyone in the first responder or other decision-making communities, and be able to look at this data and know quickly what was going on.

We think that the engineering of information systems with highly sophisticated information processing and focusing on actively of monitoring and of early warning generation will greatly assist planners and responders. This community resilience informatics capability applied to perform "what-if analysis" based on various containment strategies can assist official responders and reduce the impacts of large scale disruptions, whether caused by acts of man or by acts of nature.

There is a lot going on. Many people have been involved, including our Networks Dynamics Lab, in forecasting what might happen with the H1N1 virus and other health threats. So this is a step that we are beginning as we speak. We think it can be very beneficial to the community. We are using Arlington as a case study because, as you know, Arlington has a lot of high value targets. The NSF is there. They also have a very sophisticated information system in place already. So we hope that we can be of help by learning some things from this examination, and developing some strategies with the kind of computing capability we are talking about in real time.

So we are going to combine the strengths of IBM and Virginia Tech and Arlington. And we will be asking others to join with us, in government and other universities. We think that we can produce some results that will really be beneficial.

So let me wrap it up here – let me restate. I think the following questions are going to continue as we go along. We all are committed to providing a safe and secure environment for the people for whom we are responsible. But how much investment is enough? And what is the proper tradeoff equation that balances security and risk and cost? And how does the organization allocate its assets across the range of potential hazards? How does one measure the impact of security measures on the openness of the university and other large facilities? And how much liberty and personal privacy are we willing to sacrifice to achieve improvements in security?

In 2007, the Homeland Security Advisory Council's report on the future of terrorism said that the evolving complexity of our adversaries challenges existing paradigms. Walls separating state, local and federal responsibilities are counterproductive. The protection of critical assets, as well as the initial response to an attack, are primarily state, local and private sector responsibilities, with federal assets and resources provided as a supplement.

I am certainly no expert in this field, but I have had some first-hand experience. My conclusion is that we must do everything we can on-site to have reasonable measures, but we cannot operate in isolation. There is going to have

to be some sort of national framework on which we are all a part. This is necessary to help us monitor critical data of all varieties and that also provides us rapid with the capacity to generate real time crisis management plans for human and technical systems that are extremely complex, and growing more complex every day.

In closing, I applaud your efforts to be ready, to minimize the effects of these events, whether they result from nature or intentional acts by human beings. I thank you for the opportunity to speak to you today, and wish you great success for the conference.

DR. BAKER: Thank you Dr. Steger. An important and far-reaching message. The protection of the universities is extremely challenging. They are the institutions that by their design are supposed to be open which makes the security problem extremely challenging. We greatly appreciate the efforts of Dr. Steger to improve the security at Virginia Tech. It is a very difficult problem, and I also appreciate and endorse his call for a national framework to do this.

As you have probably noticed from the program, we have three panels today. The first panel will deal with physical protection. The second panel will look at cyber protection, and then the third panel, this afternoon, will present actual case studies of large facility protection implementation. President Steger's talk has really whetted our appetites for case studies, how people are dealing with these problems in real applications.

The first panel is chaired by Richard Little, professor at the University of Southern California, a Senior Fellow in the School of Policy, Planning and Development, and Director of the USC Keston Institute for Public Finance. He is former Director of the National Research Council Board on Infrastructure and the Constructed Environment. He has about 40 years of experience in this regime and is an expert on financing, life cycle management and risk management of critical infrastructures. He also serves as editor of the journal Public Works Management and Policy. He has just recently been elected to the National Academy of Construction. I want to thank Rich for agreeing to organize this panel on physical protection of large facility complexes.

Physical Protection Problems and Approaches

MR. RICHARD LITTLE: Thank you for that introduction, George. I realize, as you were going through that, you could have just said I was old, which is true.

What was interesting from the previous presentation is that it really did set the stage for the complex kind of environment in which security exists. I first became involved in these issues after the bombing of the Murrah Building in 1995. There was enormous concern about large vehicle bombing attacks, and a great deal done to prevent those or mitigate their effects. And of course we saw what happened on 9/11, which gave us another threat scenario. That subsequently morphed into attacks against the metro physicals in London and Madrid and, most recently, the attacks in Mumbai, which again was another scenario. Interspersed with these, we have had incidents here at home at Virginia Tech and Columbine High School, which was just ten years ago this year. It seems that regardless of what we think we know, events evolve to thwart our best intentions.

But having said that, I would argue that the option of doing nothing is, in fact, not an option. We are very fortunate today to have three speakers who I think will very nicely set the stage for the physical side of what we confront. Austin Smith is Director of the Interagency Security Council, which is the federal group that basically determines guidelines and standards for physical protection. The second speaker, Bill Austin, does threat assessments or balanced survivability assessments for the Defense Department, in essence helps client agencies determine what their vulnerabilities and risks might be. Then finally, Bob Smilowitz, who is with Weidlinger Associates, actually gets to implement what we have determined are good guidelines and what we have determined are realistic and credible threats, into a physical engineering packages that, in fact, produce buildings that people can live in and use without having to hunker down in the bunker. We can learn a lot from these three presentations.

The panel will work as follows. We will have each speaker make a presentation of about 20 minutes. Then I will pose some questions to draw the three of them in. Finally, time permitting, we will also take questions from the audience. So without further ado, I will turn the platform over to Austin Smith.

MR. AUSTIN SMITH: Thank you, Rich. First I would like to thank everyone for being here. Good morning. Again,

my name is Austin Smith. My normal presentation slot always seems to be right after lunch on the third day, so this is a rarity for me – to get everybody bright-eyed and bushy-tailed. So I will try to continue the momentum of the opening and the kickoff for this.

I am going to talk to you about the Interagency Security Committee today and cover basically what it is. I'm sure a good number of you know about the ISC. Several of you in the audience are very familiar to me. Some of you have seen versions of this. I definitely won't be standing behind this podium. I can't stand here for more than fifteen minutes. I have twenty, so I will probably run around out front a little bit. I promise to speak as loud as I possibly can.

I will begin with a little bit of the history of the ISC, and then talk to you about a major development coming out this summer, which is going to impact the federal community dramatically. So I will get started.

Just sixty-nine days after the April 19, 1995 Murrah Federal Building bombing, the Department of Justice published something called the DOJ vulnerability assessment study. Its purpose was to answer the question, "How are our other buildings protected?" The research revealed that each individual department of the agency had their own approach on whether and how to protect their buildings. The Department of Agriculture had their rules, the Department of Commerce had their rules and the Department of Defense had their rules. Some were good. Some were not as good. But there was nothing across the board. Guidance existed for the Department of Defense, overseas embassies, and the Overseas Policy Board, but there was nothing that covered non-DoD federal entities within the U.S.

Thus, one of the 52 recommendations of the DOJ vulnerability assessment study, which we just called the DOJ report, was the creation of an interagency committee to oversee security standards for non-DoD federal facilities within the U.S. Thirty days after the report was issued, President Clinton signed executive order, 12977, which created the ISC. Twenty-one permanent primary members were commissioned to vote and create standards for the federal community.

The committee is approaching our 15th anniversary. We meet quarterly. We have published quite a number of standards over the years and have also developed best practices. The committee's vision is very simple: for people to be secure and safe in the federal facilities throughout the country. Our vision encompasses not only federal employees, but contractors and visitors. Facilities include leased as well as owned. The way general counsel has interpreted it to us is, if there is one federal employee housed there, it is considered a federal facility within the bounds of the Interagency Security Committee. Although we have mainly focused on physical security of the large-owned facilities, we have published some lease standards.

The committee has representatives from 41 departments and agencies. We have since added associate memberships. The primary members are the ones mentioned in the executive order. There are actually two executive orders that affect our operations. The second one just moved us under the Department of Homeland Security from GSA. It also did a little housecleaning related to the creation of DHS. Later, the committee added twenty additional agencies. We soon found out there are a lot of other interested parties that needed a voice in the creation of these standards, so the associate members were added. We have been adding one a year now for the last couple of years, and we will be adding one more at our next meeting.

I am the committee's Executive Director. Our former chairman was Bob Stephan, Assistant Secretary for Infrastructure Protection, whose position is currently vacant. We are waiting for our political appointee, hopefully very soon. We did get our Under Secretary two weeks ago. We have a steering committee that runs the governance of the ISC. We also have subcommittees for standards, technology, convergence, and training. We run most everything through these subcommittees. No products are developed exclusively by the leadership. Every idea, every product that we publish comes from the members.

I would now like to discuss our products in the context of our organizational structure.

We have subcommittees and we have working groups. The subcommittees are standing groups that have ongoing work. The steering subcommittee makes all of the major decisions for the subcommittee. The standards subcommittee serves a judiciary function to answer questions based on standards' content. Likewise, the technology, best practices, convergence, and training subcommittees provide guidance to the federal community on their respective topics.

A major difference between the subcommittees and working groups is that the working groups are task based. They have one particular deliverable. Today I want to devote particular attention to the physical facility criteria being developed for federal facilities. I may be going a little

quickly for you, but I am trying to compress an hour's worth of material into 20 minutes.

We have published three major standards since our inception 14 years ago. We adapted the DOJ report as the standard for existing owned facilities. In 2004 we published something called "New Construction - Major Modernization." It is a security design criteria. Many of you in the design community are already aware of this publication. The document was needed because, obviously, the approach to protecting an existing owned facility is much different than starting from scratch. Then the very next year we published our third major standard governing protection of leased facilities. These are buildings that the federal government doesn't own and consequently pose unique protection challenges due to the peculiarities of leased space.

Our baseline approach was developed for existing buildings that we owned. We recognized that the approach may differ depending upon whether we are building a new building, or using leased space, or we are protecting an existing owned building. The owned-building approach was the baseline for us, but the problem was it resulted in substandard security in some respects for non-owned buildings. The problem was that federal employees working in leased space were being protected differently from federal employees working in owned space. We asked ourselves, "Why are we using different standards for each type of project?"

There are also lots of legal problems along the way, too, related to responses to construction solicitations. If Solicitation for Offers or SFO goes out for a leased space in a building already occupied by a federal agency, it is most often best if we can get another floor in the same building. If the owner of a building across the street has a lower bid, they win. Thus, they are building security from scratch to lease standards. Although the Interagency Security Committee frowns on such outcomes, we end up having to do it based on current legal requirements. There are three projects presently underway that are caught in that conundrum.

Another issue I want to address is the question of facility security level determinations. The Department of Justice Report introduced the concept of security tiers or levels. There are five tiers that are used to classify all federal facilities. Level five buildings are the most highly protected due to their exposure to the highest threats. Level one buildings are the least protected. The initial DOJ methodology considered the number of people working in a building and its size. In 2008, we replaced this methodology with one that uses a matrix approach that adds the threat to the tenant agency, mission criticality and allowed adjustment of the tier level based on an intangible. If the new matrix puts a given building at a level three, it is possible to adjust the security level to two or four based on intangible factors. The system allows assigning levels up or down by one number. Every non-DoD federal building within the U.S. has been assigned a level from one to five.

We are now combining the three other standards that I just mentioned, the DOJ report for existing facilities, the report governing leased space which came out in 2005, and the report governing new construction and major modernization which came out in 2004, into a single, comprehensive countermeasures document. Implementing building security will involve determining a facility security level (or FSL) and performing a risk assessment, and applying the countermeasure package, which provides physical security criteria for federal facilities.

Nothing has really changed, other than the fact that we have taken the three documents based on ownership and we have put them all in one package. There are a lot of reasons for this. One, they were published over a 14-year period, so a lot of technology has changed over the years. Secondly, the guidance is easier to understand and use. In the past the security manager in the field had a difficult time trying to explain requirements to the design team, given that they needed to look at two executive orders, three standards documents, and an old DOJ report. Now there are two documents, the FSL and the physical security criteria.

The physical security criteria document is a major help. First, it is comprehensive update. Countermeasures for every building, every federal facility in the U.S. including new construction and new leases will be based on this document. At present it appears that we will probably go final this summer. It will make a big splash. There will be lots of training involved. I have been excited about it and bending people's ears for a year now. Some of you have probably heard my presentation before.

Obviously, the major update is an important selling point. But there are a couple of others. I'll conclude my presentation with a discussion of the key elements. The first of these is formalized risk acceptance.

Back to the questions from Clinton – who did it and how are the other buildings protected? We still don't have an answer to question number two. Fourteen years later we have the standards document. We can identify, for

example, that a given site is a leased facility, it is level three, and it should have the following twenty countermeasures. But during the build-out for that lease for this example, we cannot identify which countermeasures were implemented and accepted. There may have been a requirement for a six-foot fence. Based on cost-benefit analysis, the fence may not have been built because the manager decided to accept the risk. Someone may have accepted the risk along the way – which is perfectly fine.

Allowing for the previously accepted risk as part of a formalized process is revolutionary in the federal community. Some departments and agencies have a process for accepting risk. But there is no formalized process throughout the federal government.

In the past we might have a level three building with 30 recommended countermeasures. The manager implements the ones that he can afford based on undocumented risk acceptance. The Interagency Security Committee hands him his document. End of process.

Moving forward, same system. We establish the security level – the FSO. A countermeasures document is provided that specifies the same 30 countermeasures. We allow the facility manager to tailor and customize based on a risk assessment. If it is not possible to implement all of these based on resource limitations, physical constraints, or preferences, the manager can formally accept the risk. But now, at the end of the day we have a package for every property which explains what was done, what was not done, and why.

At present we are trying to develop the mechanism for answering Clinton's second question: how are the other buildings protected? At the end of the summer, we will have a mechanism. Every building will have a descriptive package. We have yet to designate who collects the package. But each federal department will be responsible to develop them.

I'm out of time. There's much more I could say. I'll close with a couple of our newer focus areas. Nationwide training is a very important part of our security program. I always get a lot of questions about who is going to train the hundreds of physical security principals in how to do this. We have been able to get funding for training and we are organizing four classes right now. Training covers performance measures and best practices on prevention of workplace violence. That is a three-way team with the Chief Human Capital Officer and the National Institute of Occupational Safety and Health. Another big initiative is developing minimum standards for armed contract guards. They don't exist. We're hoping to have an initial document in two years.

Thank you very much, everyone. I've jammed a lot of information into a small amount of time. I hope my presentation has given you the overall idea of where we are headed. Please feel free to e-mail me or you can visit our website, www.dhs.gov/isc. Thank you.

MR. LITTLE: Thank you, Austin. Too many Austins on this program. Now we will move to learning about vulnerability and risk are assessed. We are fortunate to have Mr. Bill Austin, who is the Director of the Balanced Survivability Assessment Branch of the Defense Threat Reduction Agency.

[*Bill Austin's presentation is not included in the proceedings at the author's request*]

DR. ROBERT SMILOWITZ: I'm Bob Smilowitz. I am a principal with Weidlinger Associates and an adjunct professor of engineering at the Cooper Union.

We do a lot of protective design of individual buildings around the country and around the world. For this talk, when we are talking about large facility complexes, I drew from my experience – in particular working on the redevelopment of the World Trade Center site, the renovation of the UN complex, the protection of large transportation complexes, and the protective upgrade of VA facilities. The National Institute of Building Sciences conducted an extensive risk assessment or evaluation of facilities of varying types, and came up with a very succinct set of criteria.

Anyway, I will start with a little history – a little background. Our practice started almost exclusively with hardened military facilities, silos, command centers, et cetera. In 1983, with the bombing of the U.S. Embassy and Marine barracks in Lebanon, the focus was then shifted to U.S. Department of State facilities around the world. In this time period, we helped develop some criteria for hardened structures.

Then in 1993 with the bombing of the World Trade Center in New York, the threat became domestic. We became involved in extensive forensic studies. After the Oklahoma City bombing in 1995, the GSA adopted design criteria for protecting federal employees in federal buildings. Then Khobar Towers was hit in Dhahran, Saudi Arabia. It was overseas but a U.S. asset and very expensive. It was a huge explosion, as I will indicate later. But the building didn't actually collapse, and there are reasons for that as well. Then U.S. embassies in Kenya and Tanzania

were attacked. At that time, the State Department had different tiers of protection, depending upon whether embassies were in friendly nations or non-friendly nations. At that point there was a realization that terrorism knew no boundaries, and that all facilities were equally vulnerable to terrorist threats.

Why do we talk about explosives so much? The world is getting so complex and threats are becoming so insidious. If you look at the news, we are still chasing pirates and defusing bombs. FBI data which was last published in 1999 showed that there were about a thousand unauthorized explosive events in the United States. Most of them were small, most of them were malicious mischief on the part of youths, but they nonetheless involved explosives that are readily accessible. All the components have been improvised. An explosive device can be purchased at a Home Depot, and it takes relatively little sophistication to assemble them.

Aside from the buildings that are perceived to be targets, and we always say that our clients know which ones they are, and what the perception is. There are a lot more buildings in the neighborhood, in the vicinity of targeted or potentially targeted structures that are affected. If you look at the effects of the Murrah Federal Building bombing, shattered glass was distributed out to a distance of about three quarters of a mile. In the case of the World Trade Center attack on 9/11, we think of the two buildings that were impacted by the airplanes, but 37 buildings sustained moderate damage. So being in the neighborhood of an iconic building or a building with some threat-worthiness or target-worthiness makes you vulnerable as well.

If you look at the video that I will show of a bombing in Manchester captured on a security camera, you will see extensive devastation. The bomb's presence was called in advance. People were evacuated. When you look at the effects it is clear that it was all collateral damage. If we want to improve the ability to recover from an event, if we are not able to deter it or detect it, then we have to be able to improve our infrastructure.

Risk management is important. Our first priority is to manage expectations. We explain to the owners and facility managers what is reasonable and how much protective measures will cost.

In a study that we performed for a transportation authority, we identified some 29 projects to improve protection to selected facilities. We calculated the vulnerability or risk of these individual assets by looking at the importance, the vulnerability and the occurrence or the accessibility of the threat, and then proposed retrofit measures to reduce those risks.

It is very useful to plot the amount of reduction in risk vs. protection cost for facilities. We can then determine which facilities offer the most risk reduction for the least cost. A priority list can be generated from this assessment. This agency marched through these projects in prioritized order to be able to take advantage of the cheapest, most effective measures first, until their budget was exhausted for the year, and then continued down the list in subsequent years.

So risk management is something that we can quantify. It is something that we can prioritize. I am always reminded of a security manager for a financial institution that told me, "we don't manage risk, we manage anxiety." This company is no longer in business. But had they managed risk, they may have been able to identify a more useful and defendable set of priorities.

The "Interagency Security Committee for Federal Facilities" is an excellent document. I won't go into this in great detail. It provides very comprehensive, broad overarching attention to the different components of protection for a facility.

The Department of Defense had a different agenda in developing its Uniform Facilities Criteria (UFC). Their agenda was to provide enough standoff such that conventional construction is adequate if debris mitigation is included in the façade. The problem is that we rarely can provide 148 feet of uninterrupted standoff distance for most facilities. But the UFC is good and appropriate for the applications that it is intended.

The Department of State recognizes the fact that these buildings are overseas. They are not protected by U.S. citizen security folks very often. They have contract guards often at the outer perimeter. As in the case in the Moscow Embassy when there was a fire, the first responders were the KGB. So there are some very stringent protective measures for these facilities.

For commercial property owners, there really are no criteria. FEMA has put out an excellent series on risk management for the private sector. These documents provide a lot of good information. I authored a couple of the chapters. But these documents are not criteria. They offer information. You can't design directly from them.

A lot of commercial property owners ask how the government would protect similar buildings. Their concern

is protecting their occupants to the same level as does the government. It is also protecting themselves to make sure that they maintain or live up to a standard of care that the federal government might provide to their own employees.

There are a number of protective design strategies that emerged from the NIST study of the airplane impacts into the World Trade Centers. They explain features that will improve the protection of this type of facilities. It was adopted in the design of buildings in Lower Manhattan. It includes structural and facade protection of emergency rescue and recovery systems, et cetera, down to implementation of CPTED [Crime Prevention Through Environment Design] principles. It is clear that there are a lot of factors involved with protection. The challenge is to identify the right balance and the right level of protection for each of these factors.

Evacuation and rescue recovery [ERR] systems are very important. A lesson we learned from 2001 is that getting people out of buildings after they have been attacked is critically important. We have identified the ERR systems that warrant protection; things that should remain operational after an attack. Protective measures that are effective are diverse and redundant mechanical systems including standoff distances and hardening enclosures and cases. People don't realize it, but the emergency generators are important, but the cabling from the emergency generators to the electrical distribution systems is equally important. So we hardened those cables, those connectors, et cetera.

Enhanced evacuation, understanding how people get out of buildings, how people vacate after an event were to occur, is vitally important. Other factors include making sure that enough people can access evacuation systems and that they remain operational, increasing stairway width, providing a concrete core or hardened core to allow these systems to survive, pressurizing stair shafts and lobbies, et cetera. All these systems are vital to enhancing or maintaining evacuation following a catastrophe, following an extraordinary event.

Please understand that I am only addressing physical security. My specialty doesn't extend to CBRNE – it doesn't extend to cyber – it is purely physical security. There are about five major components that are common to just about every project.

If a building is considered to be a target, then perimeter protection is effective. If it is collateral damage that is of concern, perimeter protection is not going to buy you any additional safety. So perimeter protection and access control, debris mitigation; this pertains to the glass, the facade, the exterior of the building, prevention of progressive collapse.

We talk about threat specific and threat independent designs. I will get into that when I talk about structural response in a little bit, but it is not only understanding how the structure performs in response to an actual event that might be postulated, but an umbrella of threat independent prevention or performance to allow a structure to be resilient or robust. Robust is generally considered fault tolerant, able to accept some sort of insult, and then continue to function.

Finally, isolation of occupied spaces and critical life safety equipment from an explosion is an important factor. If an event were to happen within a lobby or a mailroom or a loading dock, underground parking or even exterior to the building, the occupants must be isolated from these areas of increased hazard.

When an explosion goes off, the energy is released and it expands. Think of it as an expanding bubble of energy. The front is moving outward, and as it moves outward, the surface of that bubble is increasing, so the energy is being spread over a larger and larger surface. Thus the force dissipates with distance from the explosion. We can calculate and plot the contours of decreasing intensity as you move the explosives away from the building.

In the case of an urban streetscape, when the explosion goes off, the energy doesn't just radiate hemispherically outward – it is reflecting off of surrounding buildings. It is channeled down streets and alleys. This concentrates the intensity much differently than that hypothetical explosion in an open field.

We are working with Department of Homeland Security on the "urban canyon" effect to identify what are the true loadings resulting from an explosion in an urban center, and what are the true effects on structures. This is a very interesting, very exciting project that will change perhaps the way we view the performance of buildings in dense urban centers.

The choice of the design threat is perhaps one of the most controversial, one of the most subjective topics or components to the design process. Everybody is familiar with the charts that identify the weights of explosives that can be transported in different types of vehicles or packaged in different types of containers. Explosives weigh about 100 pounds per cubic foot, so if you have

five cubic feet of luggage space or cargo space, that is a 500-pound potential. Similarly, a semi-tractor trailer, 600 cubic feet, you can pack 60,000 pounds. So it is one thing to talk in terms of the capacity of the vehicle as the maximum credible threat, but often it is unrealistic to design to these actual maximum credible levels.

On the right you will see a listing of actual events that have occurred from the Unabomber up to Khobar Towers, and how it relates to the types of vehicles that were used to transport these explosives. Once again, this is the most subjective component of the threat assessment, and, quite frankly, it is the most debated, and rightfully so.

I will now briefly touch on some of the components of physical security, just to give you a flavor of the issues. Everybody is aware of the protective bollards that surround federal buildings or assets of high vulnerability. These are the tip of the physical security iceberg. What you don't realize is where they are constructed, what is below grade dictates their effectiveness or the type of construction. When you are working in an urban context, the subways, underground vaults, and utilities will dictate the type of foundations possible.

The State Department tests a lot of barrier systems out in an open field. They run a 15,000 pound vehicle at a certain speed into these barriers, and give the barrier a thumbs up or thumbs down depending upon whether the vehicle is actually stopped. What you deal with in an urban environment and actual designs is a foundation that doesn't often conform to the one that was tested. So rather than build foundations in test facilities that are representative of actual conditions, we develop finite element models. We do computer simulations of these events to be able to predict their effectiveness as installed.

Just as important as the barrier effectiveness is understanding the impact of these foundations on the existing sub-grade conditions – on the vaults, the subways, the utilities underneath. God help us if a vehicle were to crash into one of these barriers accidentally – not at their rated speed, not at the full design threat – but in a parking mishap or a traffic incident that cuts power or communications lines to Wall Street, for example. You can imagine the lawsuits that would result in those circumstances. So understanding the impact of these protective measures on the streetscape is equally important to understanding their protection effectiveness.

The façade of a building is the single largest component of the building that is exposed to an explosive threat. There are different types of strategies for façade protection, depending upon whether it is an existing building or a new building. If it is an existing building, you may consider a protective film on the glass. If it is a new building, options include laminated glass, different types of construction, and other techniques for protecting the facility. But it all comes down to minimizing the spread of the debris.

Unprotected glass shatters into thousands of flying pieces. Protected glass falls directly in the vicinity of its frame. In tests of curtain walls in New Mexico some of the components come off the building, but occupants within the building are protected. These types of tests give us good information and help us develop our modeling tools. We are developing models for the Department of Defense to analyze the curtain wall protective systems.

The results of these tests have shown us that properly designed curtain wall systems withstand higher blast loads than glazing glass within rigid supports – just because it is a more flexible system. The glass itself is not subjected to large discontinuities of stiffness, so the systems work together. The flexibility of the system is beneficial to the overall response, and advanced analytics are really important to understand the performance. This summarizes the components: laminated glass, the ability to hold the glass within the frame, frames that can take the forces and anchorages that can hold these curtain walls back to the structural slab.

When we have large span roofs, the problem gets more difficult. The blast loading sweeps over the building, excites higher modes of frequency, and therefore predicting the response is actually much more complex.

Window protection was installed in a building in the Washington area that underwent renovation before 9/11 and afterwards. Hardened glass is attached to H frames. Frame uprights are attached to the floor and ceiling slabs so that no loads are applied to the masonry walls. The masonry walls themselves are potential debris. Originally they were being protected with some geo textile fabric that was bolted to the sills and to the floor slabs to contain the debris that could result form an explosion. This approach was very cumbersome; it was very difficult to drill through these slabs, constantly hitting rebar. It was cost prohibitive.

Amazingly, some researchers down at the Air Force Research Lab down in Florida were doing some explosive testing. One of the guys just had his truck bed relined and thought that it would make sense to spray bed liner material on a masonry wall. They had access to explosives. The next thing you knew, they had discovered a relatively

efficient, effective way of spraying a polyuria onto masonry walls to control the debris. We performed a numerical simulation of the effectiveness of polyuria applications to investigate its effectiveness with a positive outcome. So these types of inventions, these types of systems, come from the most unexpected places.

The actual structural upgrade of responsive structures is a matter of detailing. Continuity of reinforcement is important to ensuring that structures can respond to unusual load patterns. Most structures are designed to carry gravity loads which pull downward. When you have blast uplift forces, they reverse the curvature with the shape of the deformed patterns, and therefore you need reinforcement in both the top fibers and the bottom fibers.

So continuity of reinforcement, appropriate detail, and confinement of concrete are all good principles. We learned a lot of these concepts from the seismic community. But applying them to the loads resulting from blast is a big challenge. So learning from the past and applying it to the threats of the present and the future is really what we are trying to accomplish.

We have changed the name of "progressive collapse" to "disproportionate collapse." It is the propagation of failure from some local initializing event that causes a disproportionate or much greater effect in the overall structure. I am the Chairman of the American Society of Civil Engineers' Disproportionate Collapse Committee and Council of Tall Buildings and Urban Habitat Committees on Disproportional Collapse. We are trying to develop standards for the prevention of progressive collapse and the protection of buildings of all types, whether they are considered subject to explosive threat or not.

The one thing that you must realize is that architecture is getting ever more adventuresome and ever more complex. Structural analysis to our known loads is getting ever more precise and ever more exact and efficient. These developments make us vulnerable to the uncertainty of extraordinary events that may not have been anticipated in building codes. So these are major concerns that the engineering community must deal with.

I will end with the following points. (1) A rational threat assessment is critical to successful design. (2) Managing expectations as well as managing risk is very important. (3) Simplified assessment tools aren't really up to engineering design standards. Advanced analysis is essential for complex systems. We come up with much more cost effective facade designs using these advanced analytical systems, but (4) confidence in these advanced analytical systems or methods rests in good correlation with test data and experienced personnel. So it is a matter of testing, it is a matter of modeling and simulation, and then it all comes down to detailing.

So with that, I now will return the floor to our moderator.

MR. LITTLE: Thanks to our three speakers. To break the ice for discussion, I have one question that I will throw out to the group before I take questions from the floor. We have heard a lot about threats and vulnerabilities and how to address them. We heard from President Steger about how a university is diverting resources that ought to be spent on education to security purposes. My question is, how do you all feel? Are the budgets adequate to address realistic threats and vulnerabilities? And if not, what might you suggest to try to bring that into line? I will put that to a group as a whole.

DR. SMILOWITZ: Let me start off.

As a practitioner, as an actual designer working on large projects, the last things we want are redesigns. Then the project will finish over budget and the redesign is on our backs. So we want to manage the expectations. We want the owner to be aware of what they are asking us to do and what the design can actually bear. One of the most difficult things is that owners often get seduced by the different options that are available to them. They see the concepts and designs, and then they want to add layers of protection onto them. Unless they start from the very beginning to understand what is being requested of us in terms of protective design and integrating it within the system, we are going to run into problems later on.

One of the best examples in my experience was when we worked on the redesign of the Oklahoma City Federal Building. At the very beginning of the process, Carol Ross Barney, the architect, held a two-day charette during which she listed five different design concepts. Then each discipline identified what the different protective measures and how they would interact with these designs. She winnowed down the process from those five initial designs to reducing them into a composite design which at the end of the day incorporated the program requirements, the protective design requirements, and the architectural intentions. The project came in on budget. It came in very affordable, because it was integrated from the very beginning. It was well thought out.

When protection is put in as a band-aid or as an afterthought or as a "let's see what we can do now," then it runs into problems. We often end up providing

protection for systems whose designs are inherently more difficult to protect, and that drives the cost up.

MR. SMITH: I'd like to follow on that. Speaking for the federal community, hopefully what we are trying to do in the ISC [Interagency Security Committee], is formalizing the acceptance of risk. One of the pieces that I didn't have time to address in my presentation is that we are doing a design basis threat for every countermeasure. This will be in the new package. This is a challenging but very useful thing to do. The idea is to do our homework ahead of time. Not every tenant has the luxury of having Robert on board to help with design trades. So the better their requirements packages are before they go out, the better the security is going to be. They are not going the band-aid route.

Our guidance includes 20 criteria. In some cases, project managers will pick five of the 20 because they are easier or because they like them. Unfortunately, they may not be any better protected, picking those five. If they had picked only two of the other criteria, that may individually have cost, but averaged out the same and afforded better protection.

So to answer your question for the federal government, the system of risk measurement isn't in place. I would say that probably the budget is there, but the system to measure how everyone is implementing the security funds across the federal government isn't in place. You can measure each independent agency, but the comprehensive cross-agency measuring stick isn't yet there. That is what we are trying to achieve within the ISC – providing a framework for measurement. Someday our work will not involve "filling in the gaps."

MR. BILL AUSTIN: I just would echo what Robert said. Most of what we do involves assessing the protection of facilities that are already built. More and more, because of our experience, federal project managers are bringing us in during the early facility design phase. There is a major cost and effectiveness benefit to design protection in from the beginning. Also, we find that about half of the identified vulnerabilities can be solved by changing procedures. So many costly upgrades can be avoided if we can alert managers to procedural fixes. Proper attention to human factors can save a lot of money.

MR. LITTLE: We would like to take some questions from the floor. Because we are recording, please step to the microphone, identify yourself and put the question to the panel.

QUESTION: Good morning. My name is Gary Staffo. I am with the Department of Energy. I was glad to see that there seems to be a consistency across all the panels about the use of a basic strategy to approach these areas. I look back to the work that William Hadden has done on general countermeasure strategies. But getting to this issue concerning major facilities, I am concerned that the work that we are doing identifies facilities that are soft targets. How do we work this process to insure that we make the appropriate efforts to address this issue?

As follow-on to that, from a historical perspective, a lot of this effort started in the '70s. I was first involved with private sector efforts to address Weather Underground-type threats. At this time, business was involved without government assistance in protecting their critical structures related to with the finance industry and some others. I hope the private sector is still involved given their long term experience in protecting themselves.

I also hope that the guides and standards that are being developed are based on performance rather than specification. To succeed, it will be necessary to have living documents for each facility because the roles and missions of the organizations as well as threats change over time. If we are going to make these investments, history has proven to us that we generally have to come back many times to reassess protection requirements. How do we create living documents for these facilities, insure that over the life cycle we have a process that we can continue to upgrade or reduce the level of protection appropriate to the facility's mission at that time?

DR. SMILOWITZ: Let me draw back on my recent experience down at the World Trade Center site. We worked extensively with the Port Authority. We worked extensively with the developers – Larry Silverstein in particular. We also worked with the operational security consultants, the mechanical engineers, the architects, and the structural engineers. Our objective was to make sure that there was a comprehensive plan – not just the design plans for the building – but operationally thereafter.

The criteria document for each facility is 95 pages long, going into great detail on how the protection system is to be maintained. Just like mechanical systems, you just don't hand them over to the owner and assume that they will run on their own. They have to be maintained. They have to be operated appropriately. The same is true for security systems. Everything is interdependent including the access control, the lighting, and the cameras. The procedures that go into maintaining the necessary protection levels are the basis for the design of the

individual components. If people relax or change the operational procedures then the level of protection that these structural systems provide will be affected as well.

So there has to be, as you say, a living document. In a real sense it is an owner's manual written for the facility so that the owners know how to maintain and operate the facilities. Fortunately the Port Authority has a good collective history. They retain and will continue to apply this guidance. We are fortunate to have the New York City Council of Terrorism, a division of their police department, to have oversight. This high valued asset will maintain its protection.

I can see that, for smaller facilities, this type of information could be lost. But the Port Authority approach should serve as a model for all major facilities.

MR. SMITH: You actually posed several questions. One dealt with the need for living documents to share with the private sector on soft targets. I believe you were talking about the private sector there and performance-based criteria.

Again, I can only speak for the Interagency Security Committee and the federal entities. It was a major challenge to combine the three standards into one. They are still in draft format. We still are receiving quite a bit of pushback from a number of entities within and outside the government in gaining final approval.

We were able to turn a good percentage of the countermeasures into performance-based criteria; but they are by no means all performance based. That said, we are not trying to eat the elephant in one bite. We are moving in that direction. Fortunately, we have a very good relationship with the chemical compliance enforcement division. Sue Armstrong, the director, will be speaking this afternoon on the CFATS – the chemical facility anti-terrorism standards. These standards are all performance based. So we are trying to push this approach, although I won't promise you they all will be.

Another of your questions had to do with private sector sharing. The ISC was written for use by the federal government. We are making great strides in trying to share it. We are close to being able to release the documents for state and local governments. We need one more signature and we will be able to do that. This has been a long time coming. It has been awkward not being able to share our time-tested approaches and lessons learned.

Again, they were intended for the federal government, but the strategy outlined in the FSL [Facility Security Level] criteria in the physical security criteria [PSC] document for the formalized acceptance of risk could be applied to any facility. It is a standard protocol for accepting risk and producing countermeasures. For example, you could use it for a 7-Eleven store or a major university campus although it is a process developed for the federal government.

You also asked about "living documents." We have published several standards over the 14 years. Part of the subcommittee's job is to regularly update our standards and also mandate which standards will be implemented in the field on a regular basis. The FSL, federal security level of a facility should be updated every three years – which should drive a lot of the countermeasures to be updated as well.

Good questions. There is no final answer to any of them. Part of the answer to each is working on the process and moving forward

MR. LITTLE: We have time for one more question.

QUESTION: Mike Becraft from Serco North America. I was struck by Bill Austin's conclusion there that large facilities are still not protected commensurate with their value. In late September of 2001, I was part of a Department of Justice interagency task force charged with assessing our vulnerabilities. The task force was led by Larry Thompson who was the Deputy Attorney General. The task force included Defense, Energy, Health and Human Services, the Surgeon General's office, Transportation, the U.S. Coast Guard and all the critical key players in each organization. We looked at everything from the Port of Boston and the Charles River to our nuclear facilities. We looked at our dams, which we will hear more about this afternoon. What we quickly realized was just how vulnerable we were and how much we didn't know about these facilities.

Now, eight years later and listening to you all talk about the interagency efforts and about the assessments, what have we really accomplished in eight years? It is kind of a provocative question, but seriously, it seems like we haven't gone nearly as far as I think many citizens would expect we would have gone. Thank you very much.

MR. AUSTIN: Thanks for your candor. For my vantage, even though I am more of a front man for the true technical experts I think there is a growing realization of how important these facilities are. Unfortunately, the protection problem can be overwhelming, because there are so many dimensions.

One of the dimensions that will be the subject of the next panel is cyber security. The cyber threat is a critically important thing. Folks like Ollie Gagnon, in his past life, wouldn't need to plant high explosives, risk getting captured or killed, when he can bring down a facility by cutting the fiber optics. That paralyzes the organization just as much. Organizations are becoming aware that protection is not just putting up a fence and keeping the bad guys out of their physical space. The problem has become much more complicated, and costly. Fortunately, there are lots of very cost-effective procedural solutions that people have not considered. But it is true that we are finding many facilities with significant exploitable vulnerabilities that have not been addressed.

DR. SMILOWITZ: It is a prioritization problem. Risk management involves identifying your first assets that you want to protect, and going down the list. It is very expensive, it is very cumbersome. Renovation of existing buildings is much more difficult than incorporating protective measures into new construction.

But I think we are raising the awareness. It is important that people accept the concept of considering the unintended or the unexpected. A lot of people in the engineering community insist that the building codes are perfectly fine the way they are – "if they ain't broke, don't fix them." But even as something as simple as the prevention of progressive collapse is going to change the national standards. New construction moving on forward will be considering damage mechanisms as well as conventional wind or seismic loading.

It is a slow process, but getting protection into new construction is something that is doable. Renovating existing buildings will occur on a very slow, case-by-case basis.

MR. SMITH: Since 2001, we have made great strides. They are incremental strides, but they are also much separated – there has been no overreaching. We have created the Department of Homeland Security, which I have been a part of since the beginning. We are moving forward.

I think over time, you are going to get to see the results of the hard work that has been occurring. But if you revisit those dams that you evaluated in 2001, I guarantee that they are much better protected. The Bureau of Reclamation will be here this afternoon and I suspect they will concur. Since I have the last word for this session, I want to make the point that it is easy to poke holes in our protection efforts. You only hear about security when security fails. But I contend, and I can provide evidence that there are major improvements in major facility security and people are much safer out there because of our work.

My Assistant Secretary, Secretary Stephan, could provide you with some examples that would make you leave here with big smiles. We must always remember that we are always one event away from the next catastrophe. We have tried to anticipate catastrophes that may be quite different from 9/11. We have a lot of very talented people who have done a good job of developing and implementing solutions to be prepared.

MR. LITTLE: My thanks to the audience and to our panel.

DR. BAKER: We are now on our break. I want to alert you to the fact we have posters available in the break area behind the lecture hall. Please fill out and return the evaluation forms in your program. In the very back there are evaluation forms, and we would like to have your feedback on each of the keynotes and panels today.

I wanted to add one thought in response to Mike Becraft's question. Bill Austin was a little modest. I have been associated with the facility assessments there at DTRA [Defense Threat Reduction Agency] since about 1989. We find that in many cases, our recommendations are taken very seriously by the facility owners and managers – many of them are implemented. As one example, we assessed the security of the Centers for Disease Control in 1996, prior to the Olympics in Atlanta. We made some major upgrade recommendations in terms of changing traffic routes, enforcing perimeters, and implementing a badging system. Our recommendations were implemented in a multi-million dollar upgrade program that resulted in significant security improvements. Mr. Austin is correct in stating that the risk reduction generated by such upgrades is hard to measure. CDC is a good model for a facility that has really taken security and facility protection seriously.

Cyber Protection Problems and Approaches

DR. BAKER: Our next panel will address cyber protection problems and approaches. I am very pleased to introduce Ms. Darlene Quackenbush as the moderator. She is James Madison University's Information Security Officer. Because JMU is one of the 50 most wired universities in the United States, it is no small task to manage cyber security there. I can attest that Darlene runs a very

tight shop when it comes to information security, as one of thousands of computer users there. She is also the Director and a founding member of the Virginia Alliance for Secure Computing and Networking, which is otherwise known as VASCAN. She has also worked with the Association of Collegiate Computing Services of Virginia. Darlene is an expert in technology policy and has 25 years of experience. In addition to her many other duties, she is a member of the JMU faculty. My sincere thanks, Darlene, for organizing and chairing this panel. I am looking forward to your session.

MS. DARLENE QUACKENBUSH: Good morning. I would like to begin by thanking the Institute for Infrastructure and Information Assurance and the Federal Facilities Council for inviting me to moderate today's panel. I feel a little bit intimidated by all the great minds in the room, and certainly following Dr. Steger's remarks this morning. I think he did such a great job of outlining the challenges that come from the university setting. My hope is that I have something to contribute here, and that we get lots of interaction from the group.

Our hope in today's panel is to use our various perspectives and organizations, our individual roles in cyber security, to paint a backdrop from each panelist, and then to use those perspectives and the challenges and approaches that they include to talk further about information assurance and cyber protection in large facilities.

Our examples hopefully will find some common characteristics that we share, some strategies that we have in common. We plan to reserve plenty of time for the Q&A, so I hope you will participate with us on that.

Today's panelists include Joy Hughes. Dr. Hughes has been the CIO and Vice President for IT at George Mason University for 12 years. Computing World has named her one of the top 100 CIOs in the nation in 2008. Ryder University has named her to its Science Wall of Fame, and she has been honored by the Information Security Executive Association, the March of Dimes, and Women in Technology.

She was formerly CIO at Oregon State University and SUNY-Potsdam, and she chairs the Microsoft Higher Education Advisory Council. For three years she also co-chaired the Internet II Computer and Network Security Task Force. She is a member of boards of two wireless television companies which specialize in television services to the D.C. area region, which provide many millions of dollars back to the university. Joy earned her Ph.D. in information systems from the Union Institute, holds an M.S. in computer science from New Jersey Institute of Technology, and an M.S. in mathematics from Rutgers. So you can see that Joy is very well qualified to speak with us today.

We also have with us Wayne Martin, who is the information systems security officer with the University of Virginia Health Systems. He has 35 years experience in the health care industry, with 21 of that in computer related roles. His personal and professional interests focus on strategy information systems planning, a unified theory of acceptance, and use of technology, and the focus of that within the health care industry. He is also interested in the relationship of organizational culture to cyber security. Wayne holds an M.S. in computer information systems from the University of Phoenix.

Our last panelist is Baird McNaught, who has supported the DHS control systems security program since its inception in May 2004. He has contributed to the development of many cyber security products which his program shares with the control systems community to promote implementation of sound cyber security practices for control systems. Most notably, Baird led the team which developed the initial version of the control systems cyber security self assessment tool, with which some of you may be familiar. Baird recently led the working group for the chemical sector control systems security. He also supports a control systems security program addressing multiple industry areas. So we are very pleased to have Baird with us today.

Since I am the panel moderator, I would like to take the privilege of talking just briefly about some of the cyber security issues and challenges that we face at James Madison University. Dr. Baker mentioned that my role is based largely on developing policy solutions. One of the main challenges that I face is trying to knit public policy, university policy and day-to-day operations together in effective ways.

The university started out as a small women's college in the Shenandoah Valley, and over the last 20 years has changed quite significantly, to put it mildly. We have been on the rapid growth chart for some time now with little sense when the growth will stop. As a result, we are continuously dealing with new populations of users coming into our environment. We think traditionally of previous standard student-faculty-staff-employee roles. But in addition to that, we also cooperate in extended lifestyle patterns with pre-admit students, parents, business partners – those sorts of things. So when it comes to thinking about who the customer is, we have many more challenges than in the past.

We also are working, by virtue of that, to become more granular in the way we assign rights and authorizations to assure appropriate content delivery and, at the same time, manage information security. The issues of transitive rights, IT federation of identity – all of those sorts of things – are on our internal radar. And in many of these areas we are working cooperatively with other institutions through the Virginia Alliance for Secure Computing and Networking (VASCAN).

As Dr. Steger mentioned this morning, the university environment commingles a lot of different aspects of network operation and cyber functionality. On the one hand we have a fairly controlled administrative environment that is focused on standard service delivery and assurance of quality. But we also operate a fairly open network that has a lot of public traffic, not to mention serving as the Internet service provider to our students.

So trying to knit all that together leads us to seek balance – which is a good way to put it. We want to find means to provide flexible service models at the same time achieving cost effective implementation and maintenance of maintaining information security. We are in a situation where we are outsourcing more of our services, either to existing business partners or more recently to cloud conglomerates. So that has been an additional challenge.

We also see a general trend within the young population toward more self-regulated work patterns. Many of our students who have come to us very technology savvy and they tend to stretch the limits of our business process controls. This leads us to seek new just-in-time solutions regardless of the security that they provide.

We provide a very time-intensive system of services in some aspects, in that we must have registration services running during certain hours that we are committed to. That is a very obvious business commitment. But we also operate 24 hours a day, seven days a week, 365 days a year.

We have students and faculty members and researchers as well who must be able to work from anywhere. Increasingly, they are using the high mobility devices that I see around the conference room today. They want to work, however, they want regardless of the particular tool or content modality that they are using, and as I mentioned, from a large variety of different devices. We seek information assurance. We are very focused on assuring the quality and timeliness of our data. That is certainly one of the things that our security is oriented toward. But we also have to deal with the text based messaging systems, the Twitters, the Facebooks, the mash-ups of data and how to manage those.

I have a friend and colleague at the University of Virginia who is the CIO there. She refers to this trend as the decoupling of our technology environments with the university. To a certain degree in universities and elsewhere that is driven by the general commoditization of information technology.

Largely due to a number of the compliance regulations, another focus for us has been data minimization. If we don't have highly confidential pieces of data, or we can minimize the places where these are stored, then we can ease the cost burden and increase the efficiency of delivering information security. But that effort toward data minimization and control is often counterbalanced by the increased demand for collection of data, right down to the availability and present state of an individual. That counterbalance demand sometimes is very difficult to explain to people and to manage on a day to day basis – it is a huge challenge for us.

It is important to understand the way that information security challenges have developed over time. I remember back a number of years ago, if we controlled our central systems databases and we built security around the central core, we felt confident that we had security, because we understood where the largest part of our data store was. We had terminals that connected directly to those databases. So, to a large extent, we could control those end points.

That is not the case any longer. Now we find that the decisions that are made at the end points are in some ways compatible with central management but, in other ways, very much a function of the user behind the device. So we spend a lot of time in information security awareness and education efforts.

The goal is to try to protect the environment as best we can, insure quality of our data and, in the end game, maintain trust. It is a difficult proposition when something bad happens to argue that you did enough. At that point, or regardless of what the situation was, there is a certain degree of emotional impact and direct impact on trust. So we work very hard on the prevention aspects of information security, trying to establish good controls at meaningful points in our environment, and working with partners wherever we can find them to try to improve things as we go forward.

With that said, I will turn it over to Joy.

DR. JOY HUGHES: Thank you, Darlene. Darlene has done a good job of explaining the environment of a modern complex ever-growing university, which is how I think of both James Madison and George Mason University – my university. We now have 31,000 students. That is 7,000 more than we had a few years ago. Three years ago we had six million square feet of space. By the end of the next two years we will have added four million square feet of space bringing us to 10 million. It has been difficult to grow in a time of economic recession because we have not seen a commensurate increase in faculty and staff.

A few years ago, I was feeling very frustrated by the extraordinary amount of attention that I, as the CIO, was paying to cyber security. I was concerned that maybe I wasn't making as much progress as I should be. As Darlene pointed out, our major challenges are not with the big boxes in the data center where we keep our finance data and our student data, et cetera. We know how to protect those – they are in the vault. The problem is that the world has changed in the past five or so years, and now almost everything that a university does is online.

In some cases, we deliver services both online and using on campus delivery – for example, courses can be both and research can be both. However, in many cases, we don't use the paper systems anymore. A prime case in point is recruiting students. When they apply for admission and send their credentials, it is not through the U.S. mail any more – it is all online. We digitize, we image, et cetera. Payroll is another example. We don't get a paycheck anymore. We don't get a W2 form anymore. It is all online. Where are these systems, these intermediary systems? They are not in my data center. Moreover, they are not managed by people who report to me.

One system that carries very cutting edge research, for example, is managed by a graduate assistant in the School of Engineering. Another system is managed by a professional IT person in the Health Sciences School. But they don't report to me. So the systems are distributed, and the employees are distributed. They are distributed across our four campuses in Virginia, and they are also distributed across the institutions we partner with throughout the United States and around the globe. We have a program in China called the 1-2-1 program, where students take their first year at a Chinese university and the next two years at George Mason. Their last year they return to the Chinese university while working on their senior project with our faculty in Fairfax, Virginia. So our systems have to commingle.

So I was wondering how we are going to do this. Then when you add to the mix what Darlene mentioned and that we outsource so much now. One of the ways that we deal with diminished budgets funding services for a larger number of students is that we achieve efficiencies through outsourcing. For example, we are outsourcing the management of our residence halls. These folks need access to our student database. We outsource our bookstore. Those folks need access to portions of our employee database. And the university parking service has access to our databases.

I was complaining about this to my boss, President Merton, who happens to be an ex-military officer. He said, "Joy, what you need is an army of volunteers." He told me that he, as president would help recruit that army – which he did. So today I will speak to you about the army of people throughout George Mason who do not report to me, but who are a part of our information security apparatus.

The first group we got on board was the human resources office. They agreed with us that when anyone is hired by George Mason, they are required to sign a document laying out their security responsibilities. They agreed that each year's performance evaluation for every employee would have in it a section where their supervisor rates them according to how well they are protecting the data that had been entrusted to them.

The next group that we enlisted was the internal audit division. I have been a CIO for many, many years. I thought of the auditor as the examiner whose purpose it was to tell you what you are doing wrong and then to leave. I realized that kind of relationship was counterproductive to cyber security. We have reworked the relationship. Now, once a month, the IT auditor comes to see me and, together, we select the department that will be audited. Once the auditor assesses our vulnerabilities, she comes back to me and we strategize what we will do to help that department.

Sometimes it is technical support. We have, for example, many students majoring in cyber security, and we employ some of them work as interns. Thus, they are available to deploy to departments needing help. But sometimes political support is needed. For example, one of our departments that shall go unnamed told the auditor that they had decided to accept a certain security risk. The auditor came to see me and explained why we should not let that department accept the risk. It is too great. My task was to go to the VP to which this department reports to convince the executive that this risk could not be accepted. In this way, the auditor and I work in

partnership to improve cyber security.
Another group that works very closely with us is the university budget and planning group. I love one of our previous charts that graphed the cost to remediate versus the amount of remediation achieved. Our budget group asks me every year to come in and to talk about my top five initiatives, and to place them in that perspective. What is the cost and what is the benefit? They have introduced a recurring item in the budget to enable the high impact cyber-security activities.

We also work closely with a group of distributed system administrators. We formed a group called the system administrators leadership team. President Merten charged the group with being responsible for training all system administrators. So even though these people don't work for directly for me, the committee is co-chaired by my security officer and co-chaired by the chief IT person in the engineering school. They are responsible for training of all university system administrators.

Another group we have is a non-technical group. Those of you who work with universities know that deans have busy schedules and large egos. We asked each dean to select the person on their faculty that they listen to, a person whose opinion they trusted to work on our security liaison group. Once a semester, I bring the "security liaisons" in and I feed them, I pay homage to them, and then I ask them to vet any new security policy we are coming out with, and I actually make changes in the policies based on what they tell me.

These arrangements fit in with Dr. Steger's message. We have to balance the loss of personal freedom with the need for security. If the mandates came from me, then I would spend most of my time fighting with people who were resisting central administration. But when the mandates come from the security liaisons which are the trusted representatives of the deans, then I am not in the fight. Generally, these policies just sail through. When policy decisions are communicated to our academic units by these security liaison representatives, they are better understood and accepted.

I would be remiss if I didn't comment on two executives at my institution. They are the two most important people to get on board at any university. One is the chief academic officer and the other is the chief finance and administration officer. We work in partnership. Typically, I write a policy letter for their signature. As an example, we have been able to implement a policy that no one in this university is authorized to store highly sensitive data unless they have in their file a letter signed by the chief academic officer and the chief finance officer. The implementation letter also went out under their signature. The letter contained a phrase from human resources office stating that penalties for violating this policy range up to job dismissal. The chief officer's participation has been extremely effective.

As I mentioned, our president is the muscle behind all this. I am the front person and he is the muscle. His latest mandate addressed a system that was poorly administered which I brought to his attention. He issued an executive order that prevented people from administering a university system unless their security credentials have been validated by the chief IT security officer. So with one action, he put an end to the practice of having untrained, uninterested people managing computer systems. I am very grateful for his efforts.

The large number of people across the university working to advance cyber security has created a fantastic environment for me. But we still have problems, mainly due to vendors providing systems to us that are insecure. One university, George Mason alone or James Madison alone, cannot change vendor practices. We don't have the clout. A coalition of forces is required. I am going to mention just two of these today that have greatly benefitted us.

Darlene mentioned one of these – the Internet II Security Task Force. We do a lot of work with security officers, helping to educate them and organizing security awareness campaigns, et cetera. One of the things that we realized is that the basic Enterprise Resource Planning (ERP) software packages that universities use are not secure. I am talking about PeopleSoft, SAP, Oracle, Banner and SunGard. The packages are delivered to us in an insecure state.

To try to effect change, we spent two years on research to investigate and identify specific insecurities. We documented our research by publishing an article in a national journal and made a dozen conference presentations. We framed our message in a context that would cause ERP vendors to listen… we presented our findings in the context of a procurement decision.

Our articles and our conference presentation said, if you are considering buying an ERP, do not buy one if it has the security flaws we identified. We called these "deal killers." For example, in one of the systems was designed such that the password to get into the most private data files was a six-digit number. That was one of the deal killers. In another system, to get anything done in payroll required access to a non-encrypted password file

containing all user passwords. We also documented this and presented it nationally. We warned the university community not to buy an ERP with these flaws. You can imagine what happened – the ERPs corrected the flaws. Collectively we succeeded in affecting change where, as individual universities, we had been able to do so.

The second coalition of forces I will mention has to do with a combination of the REN ISIG. As you may already know, most industrial sectors have an "information security industry group" or ISIG; for example, the finance industry has one. Higher Ed has one too called the Research and Education Network ISIG. Our group has been very frustrated with Microsoft – we were unable to get the information from Microsoft that the greater Higher Ed community needed to fight vulnerabilities. There was a very good reason for that – Microsoft's people were working around the clock in Ridmund and all over the world developing and testing patches and other methods to overcome their vulnerabilities. We were banging on their door asking which patches to use including some that third parties had developed. Microsoft was insisting that they couldn't answer our queries. The reason was that they had not finished their own testing and realized they would be liable if they gave us erroneous advice.

So we brokered a deal that took two years to implement. It wasn't just that Microsoft is a huge bureaucracy – higher education is also a huge bureaucracy and our group has 2,000 members each with different rules. After two years of negotiation, we finally brokered a deal where Microsoft opened their back door and they allowed the REN ISIG representatives to sit with their security researchers to see what they were developing to fight a particular vulnerability. The REN ISIG then sanitizes that information to protect Microsoft and then distributes it to us. Thus, we now have a trusted source offering best-practice solutions. I estimate that between the ERP project and the REN ISIG project, we have cut down millions of hours of staff time in higher education.

I will close with this observation. We have heard about some daunting challenges today. After this morning's session it is easy to become discouraged given the large amount of work yet to do. The good news is, based on our experience at George Mason University; the job is so much easier when we do it together.

DR. WAYNE MARTIN: This is a great place for me to start. Working at the University of Virginia health system, I sit at the juxtaposition of patient care, research, and education. In my position, I must make sure that I cross boundaries and understand the researchers' need for data, the patients' need for confidentiality and then being sure that we can provide the level of education that the University of Virginia students expect.
On the health systems side of the University of Virginia, we have the Medical Center, the School of Medicine, the Health Services Foundation, which is the physician billing arm, the Claude Moore Library, and the School of Nursing. So again, our missions are patient care, research and education.

We are dealing with several new initiatives. The High Tech Act is an expansion of the HIPAA security initiative. The new Electronic Medical Records (EMRs) system focuses on trying to get the information to the right person at the right time in the correct format to help inform decision making. In the long run, the goal of an EMR is to reduce costs by enabling a much better job of diagnosing and treating patients.

One of the key points from this morning related to physical security was the importance of early involvement in building design. Likewise, it is critical that security be considered early in the design of a data infrastructure systems. When we have to weigh in late in the system development process to try to plug holes, as with physical security, we run into major cost issues. If data security is built in from the start, it is easier, more effective, and less costly.

This leads us to the discipline of life cycle management. One of the largest challenges I've had since 1988, when I became involved with computer systems, is getting people to understand that when you build something today, you can't expect it to stay static over time. There is a definite life cycle. You have to put something in place that will mature, age, and need to be replaced.

Applying this principle to users, it is important to understand that they come in, they do their thing, and they eventually will leave the organization. The same applies to data. The data itself has urgency while it is being used in the treatment of the patient. But over time, the data loses its urgency. Obviously, it still needs to be maintained as part of the record for the patient for future reference.

Understanding the level of sensitivity and urgency of data is an important part of life cycle management. On the university side, we have already heard from both Darlene and Dr. Hughes concerning challenges associated with sensitive data. At the University of Virginia we are focused on highly sensitive data –pieces of data that could lead to identity theft including medical identity theft. The HIPAA security rules cover PHI, protected health information, which obviously consists of highly sensitive data elements.

This leads me into a concept that I find very intriguing. I'm sure many of you have heard of the governance risk and compliance model which involves getting business owners to understand their place in the HIPAA security rule. When the HIPAA security rule came out, everyone looked at the legislation thinking as pretty onerous – that it would take lot of work to implement. But there were several key terms that I found very intriguing as I studied the language. "Reasonable and appropriate" was one of the phrases used – namely, that organizations needed to take reasonable and appropriate steps to secure their data.

I think we saw some interesting parallels this morning in the physical security discussion. The physical security folks talked about considering what needed to be protected, how it needed to be protected, and the resources that were available to protect the particular item in question. These considerations relate to the "reasonable and appropriate" concept.

Another interesting part of HIPAA security rule language is the phrase "reasonably anticipate." From a data security standpoint, we are trying to understand what the risks are from external sources, what the risks are from internal sources, and then "reasonably anticipate" what we might have to deal with. This understanding provides the basis for determining how we are going to structure our data security practices.

The different information technology teams find themselves in a unique situation because of their differing perspectives. The network team becomes very focused on the firewalls and the routers. The server team becomes very focused on administrative privileges, lease privileges and other mechanisms to lock down access to the core systems to selected system administrators. One of the things that can happen in that kind of environment is teams planning and implementing security measures without necessarily informing other teams what they are doing, why they are doing it, and the overall effect that could have on the basic security infrastructure.

So as the person that sits at the confluence of patient care, research, and education, one of the tasks that I have is to create those partnerships and collaborations, which have been a main theme of today's presentations. It involves getting functional groups together and encouraging them to perceive the external threats and secure their internal resources. We must understand the internal targets of external threats and whether those targets are protected. Do we truly understand the locations of our vulnerabilities? Should someone successfully breach our external boundaries, are we protected? Are we prepared to respond quickly should an attack situation occur?

So from the governance perspective, we must work with our business managers to make sure they understand what we are trying to accomplish and what we mean by "reasonable and appropriate" and "reasonably anticipated." As we talk about implementing any measure that might limit a user's access or time to access, business managers are going to push back. They will argue that patient care is critical and we can't impede the patient care delivery team and timeline. So that is the balance.

We have recently performed a risk assessment involving all our business managers in which we walked through an exercise that addressed risks of concern. During the exercise I could see lights going on and ideas starting to take hold. Business managers must be engaged. They need to dialogue with us to determine where they can adjust their practices to achieve better security.

All in all, it is a partnership; security involves collaboration. When the rubber hits the road, the users are the security. Security for the health care system complex is challenging because the data are both highly sensitive and critical to success. We must create intelligent and high confidence standards, policies and procedures to manage the protection of the patient care information. The problem is made more complex because in the research realm, practitioners want access to the same data – but they want it, in most cases, in a de-identified way. The HIPAA security allows this, as long as the information can't be re-identified should a researcher's database be compromised. That is represents a major discussion that could be the subject of another seminar.

Researchers must understand that when they ask for data, they must go through an institutional review board or IRB to get permission for access to certain sets of data. When they make the data request to the health systems side, they must be very, very specific. Database administrators may receive a request for certain data elements. If the request is not specific enough, they may provide more data than is required that may include highly sensitive data. This reinforces the importance of ongoing conversation across all stakeholders so that everyone understands what data is being reviewed and accessed, what the risk of that data to individuals' privacy might be, and necessary steps to take to protect sensitive information.

At the University of Virginia, we have been actively looking at encryption. It is an approach that most organizations

consider. We are perhaps a little bit ahead of the curve. We have begun active pursuit and implementation of data encryption including hard drive encryption, USB encryption, and PDA encryption. Basically, our objective is to encrypt all of the data that flows outside our secure systems. We have purchased a product and have now implemented the data encryption processes. We have experienced very minimal impact and pushback from users.

We reached the point where we had implemented USB encryption. Our solution involved simply encrypting the entire USB drive and having the user provide a password. The process was centrally managed so we could recover passwords. The system facilitated performing compliance and auditing tasks. We thought our solution was pretty slick and one that the users would appreciate. We believed that it would help us meet our three missions without disrupting users too much.

Unfortunately, we misjudged our educational requirements – we didn't consider the possibility that our users might not understand how the system could be used. There were some situations where enhanced technical understanding of computer operation and use was needed. I certainly remember how I was back in the '70s, when I was in the military and we were still doing optical character recognition – decoding colored-in little circles. This was my first exposure to computers and I remember thinking, "I hate computers, I don't want anything to do with computers." So I can certainly relate to users who think they know how to run computers and are suddenly confronted with an issue that they don't understand. We have now addressed this problem and are doing a better job of working with the end users to understand their needs. Our encryption initiative is working much better now. Once again, it goes back to accepting and realizing that we need to communicate – we need to interact with the users that will be most affected by system changes brought about by information security improvements. Planning information security in a vacuum is not a good approach, because you will inevitably run into issues that you can't anticipate alone.

The third component of the governance and risk equation is compliance. Based on my experience with encryption over the last 18 months, there are two elements related to compliance. There is organizational compliance and then there is a personal or an employee staff compliance element. Our university charges each individual with responsibility and accountability for receiving sensitive data, getting permission to store it, and then protecting it during and after the approval cycle.

The IT teams on UVA's health systems side felt they had a duty and a responsibility to take compliance one step further. Hence our full encryption of the USB drives with the password protection. On reflection, we realized the need to provide end users with a tool to help them meet their compliance responsibility and accountability requirements. So we have improved our encryption implementation. Users now have a location on their USB drive called "the encryption zone" where users can store highly sensitive data and are able to manage all their other files on the unencrypted portion of the USB.

That leads us into a new educational realm. We need to make sure that our users truly understand what highly sensitive data means and also what PHI [personal health information] means. We work with highly educated, highly motivated knowledgeable individuals who may believe they understand what PHI is. But it can get tricky. For instance, when you have a patch image that has the embedded patient name and other pertinent information – that is PHI. When that image is included within a conference PowerPoint presentation, patient data has been compromised. In this case, we would advise the presenter to put the presentation in the USB drive's encrypted zone and then crop the picture so that information goes away. Most of the time, the presenters are cropping the information, but they don't realize that the information is still retrievable from the file so it still needs protection.

I view my role as more of a translator. Where I sit, I interact a lot with the C-level folks. They are reading the HIPAA security rule from a very distinct perspective. I also encounter users who are obviously hearing about the security rule. They are probably not reading it, but they are hearing about it so they have their own interpretation. My job is then to go to C-level folks to make sure they focus on our reasonable and appropriate concepts and reasonably anticipated threats and vulnerabilities. I also consult with them on ways that we can craft the budget and move forward with implementation. I am then able to educate the users our rationale and how they apply our solutions to protect the data that they are working with.

Based on my experience, I predict we are moving toward an approach that involves the concept of "trust but verify." We saw hints at this approach this morning associated with physical security. After physical security features have been implemented, due diligence is still need to make sure that the features are properly installed and maintained. The experience and training of security guards is one important ingredient. Without follow up life cycle management, security provisions will become stale and likely to be ignored. The same principle applies to

information security. When people become used to the routine of entering their usernames and periodic changing of passwords, they can lose sight of the underlying rationale. It is important in our educational efforts to explain why security measures are in place and the importance of security vigilance.

I appreciate the opportunity to provide a brief perspective on my experience working in a complex organization like the university. Because of the university's prime mission of education, freedom of information is extremely important. Information must be available and flow to support not only the faculty, but also the students. The challenge on the health systems side has been isolating our core systems at the same time working to insure that the researchers have the information they need. Risk assessment provides the basis for everything we do.

MR. MCNAUGHT: Good morning. I am Baird McNaught. I work with the Control System Security Program at the National Cyber Security Division of DHS, and I'm here representing Sean McGirk, who is our program director. One clarification on the printed material you have. I was inadvertently given the honorary title of Dr. McNaught on the program. I greatly appreciate having this honor for the day, but I must relinquish the title when I leave today.

This morning, I will talk to you for a few minutes about control systems and cyber security as it relates to these systems. Control systems are in the news lately, particularly with regard to cyber security. There was a recent article on this topic in the Wall Street Journal. There is also a bill, the Cyber Security Advisory Act, that is before Congress right now.

There are four things I want to point out about control systems.

First of all, a quick definition. Control systems provide a means of sensing of a physical process and then being able to change that process in order to get a desired result or outcome. Modern control systems are becoming ever more interconnected, particularly with business systems in any corporation. This interconnectedness introduces vulnerabilities into the control systems.

Control systems are quite different from your typical IT system. They have a much longer life cycle. Reliability is of the utmost importance. It is not possible to shut down control systems every night to do a patch. So the maintenance approach is a lot different than a typical IT system.

Control systems have many diverse actors. We have vendors – Dr. Hughes has already spoken about vendor issues. I'm going to address these as well in a minute. We have owner-operators, and we have, of course, the interfaces with the IT and business systems.

A few years ago when the national infrastructure protection plan was issued, the government identified 17 then, 18 now, of what we call infrastructure sectors. Our program works with all of these sectors – some more than others – to try and improve the cyber security of their control systems.

Industrial control systems are the one means making it possible to affect a real world physical action through the virtual realm of the Internet. They are becoming more secure. Traditionally they were somewhat isolated. With the advent of the Internet they have become more and more connected without any concern for security. But the culture is changing, and these systems are becoming more secure. Awareness is out there, and people are taking the actions to implement security measures.

The risk equation includes threat, vulnerability and consequence. Typically we can't do a lot about the threat other than become aware of it and consequences are what they are. So we focus mostly on vulnerability and ways that we can strengthen our defenses against attacks.

We concern ourselves with four categories of attackers. There are "crackers" who are doing things for bragging rights or for profit. Terrorists are acting based on some ideology that they are trying to prove or implement. Attacks may be perpetrated by the governments of hostile countries. I have a friend that used to work with us who is now working for a major defense contractor. He spends 40 hours a week just countering the attacks from a certain country against that company. Finally, we must be concerned about the insider and the importance of defending ourselves against an insider who may be in a position and have motivations to disrupt control system operations.

I wanted to mention some actual incidents and consequences that we have seen from attacks or cyber incidents in control systems. The 2004 blackout on the East Coast is an important case study. Much of the grid was out for many hours because of a control system failure from a cyber event. In 2003 where there was a computer virus that affected a train signaling system. Train services were delayed for six hours. In 2005 Daimler Chrysler had a worm that infected their control system in one of their plants causing a one-hour shut-down. I must

admit, this pales in comparison to what the economy has done to Chrysler. But this is an example of how a worm can affect a control system. We have learned many lessons by studying these failures. Critical patches and antiviruses need to be applied and updated regularly. A defense-in-depth strategy is required including firewalls and isolating system control networks from corporate networks.

In 2006 a disgruntled employee of the City of Los Angeles hacked into their computerized traffic control system and disrupted operations for four days while they were trying to diagnose the problem and repair their system. Again, major lessons were learned. Organizations must not underestimate the insider threat. Ensure that separation of duties and auditing are in place to make sure that no one person has all the rights to get into control systems. Change passwords regularly.

In Harrisburg, Pennsylvania, a foreign hacker penetrated the security of their water system by disrupting the control of their water filtering plant. In this case, the lesson was that critical antivirus patches need to be applied and updated regularly.

Back in April 2009, the Conficker worm affected a couple of electrical utilities. As with the Harrisburg water system, the cause was that an available patch had not been applied to their Microsoft operating system that was available in October 2008. In many cases, simple updates can protect us from debilitating cyber events.

In 2008, a Polish teenager was able to hack into the train switching system and caused some derailments. The Hatch Nuclear Power Plant experienced a system shutdown in 2008 and took 48-hours to recover. Again, patch management policies were not in place.

The most recent incident involved someone hopping a fence and accessing an electronic highway sign control system. Because the default password had not been changed in the system, they were able to enter the words "Zombies Ahead" onto the roadside display. There were no accidents but the incident was obviously distracting to motorists as they viewed this sign.

I will take my last few minutes to discuss some mitigation ideas. We always encourage owner-operators to apply a defense-in-depth strategy, including perimeter controls, their Internet and corporate perimeter, their access controls with their people and policies, and then applying cyber security controls at their lower levels. Security is a process – it is not a product. You are really never done. You have to keep at it all the time. You need focused policies and practices, and you must review them regularly. The threat is constantly changing, and the vulnerabilities that pop up because of those threats have to be dealt with on a regular basis.

With regard to our control system security program, we encourage asset owners to apply resiliency, security and reliability into the infrastructures that they manage. We have developed program products for owner-operators to use. I don't have time to present them all, but I will cover the high points.

We have organized what we call the industrial national security cyber emergency response team. This is a team that will take incidents as they occur in the community, analyze the incidents, and then disseminate information to asset owners so they can be prepared to defend against future cyber attacks and events.

We have a cyber security self-assessment tool. This is a laptop or a desktop software tool that does not tie into the control system. Rather it is a questionnaire to help asset owners find vulnerabilities. I like to compare it to Turbo Tax. Based on operator answers to series of questions, the tool will generate a list of vulnerabilities in priority order of highest to lowest risk. We work with asset owners all over the nation in the various sectors to get this tool out and help them to get started with their self assessments of their security profile.

We have several published documents. Dr. Hughes talked about the importance of including security requirements in system procurement. We have a procurement document that helps owner-operators to specify the security that they need for the equipment that they are buying at the beginning of the acquisition process. A patch management program is an example.

We also do a lot of education and training. This is really in high demand now. We have both web-based and instructor-led courses. We have an advanced training course which we teach at the Idaho National Lab. It is a week-long course in which we set up a red team and a blue team. Our practicum includes an actual control system. The blue team operates the control system while the red team tries to hack in and shut it down. We find this kind of exercise to be very helpful in learning how to protect yourself against cyber attacks.

Then lastly, we have the Industrial Control System Joint Working Group that we started in March of this year. This is a venue in which we get the government coordinating councils and industry sector coordinating councils

together. We are able to get subject matter experts from the vendor community and international community all working together on a consolidated approach to solving cyber security for control systems.

MS. QUACKENBUSH: Perhaps you are forming some questions that you would like to ask the panelists. I have a couple that I would like to ask that hopefully will spur some additional discussion.

One question involves leveraging the role of mass media as being the public face to the population related to information security incidents and different aspects of cyber protection. I am wondering whether the panelists can mention some of the things that they are doing perhaps to work with outside constituencies or, at best perhaps, manage the media in relation to some of these challenges.

DR. HUGHES: I could start with that. Do we have any media people in here? There is an unfortunate conflict of goals with respect to the younger media people who are hoping to move up in the world. They perceive moving up in the world requires them to look for the dirt. So it is frustrating sometimes to work with them. They seek to find some secret you are not telling them, or finding someone on the campus who will say that a key building really isn't secure – the administration thinks it is secure but it is not. So that is a conflict of goals vis-à-vis assisting us in communicating with the public.

However, on the other side, we have media who want something from the university. These tend to be the more sophisticated media people who want access to our faculty, who make interesting interview topics on national television, on NPR, et cetera.

What we have been doing at George Mason is creating relationships with those more sophisticated media people, accommodating them by making sure that if they call with any request to speak with any expert on any topic, that we do not turn them away. We work with them to find the expert and follow up with the media person to make sure that they were satisfied. This process is working very well. We are hoping that these savvier, sophisticated media people will have a tempering influence on the hot shots.

Another danger that we have noticed is the online media services that don't actually report. They don't have any reporters. They don't call you up to find out what really happened after an incident. Rather, they lift pieces from the traditional media and use only the more provocative sentences from the traditional articles. Unfortunately, when this information is published in the online service, it lives forever.

So if I were to Google Darlene, I may find some quote from five years ago that one of these predatory services had lifted out of context. The same would be true if you Google my name. I'm not sure how you deal with that. If other panelists or people in the audience have learned how to mitigate these unauthorized online services, I'd be interested to know your approach.

DR. MARTIN: We are developing tabletop exercises around an event in which we have a breach. I am getting training on media capabilities and roles. I am working with our media department. They have been very thorough in making sure that I, first and foremost, recognize the severity of the problem and the impact it could have on individuals.

But it goes back to what was said this morning. We can't stop everything. There is no such thing as 100 percent security. That is actually a part of the message - that despite our best efforts, it is unfortunate that a breach may have occurred. Despite their many harmful consequences, breach incidents provide invaluable information on how to create an even better security environment.

It is important that we coordinate with the people that are responsible for the initial press releases. UVA is very fortunate – we had someone who is very talented handling the television presentations for the one or two occasions we have needed media coverage. They have been very effective in making sure the issue was presentled clearly, what steps we were taking, and then what affected individuals should do. Sincerity and authenticity are all important in responding to the media.

MR. BAIRD MCNAUGHT: We try to work with the media and provide interviews and information sharing as much as possible. We actually have a staff person that is our communications specialist.

We dread it when an article comes out on control systems' cyber security because we find that a lot of the information is not very accurate. We find ourselves jumping through hoops answering questions up the chain concerning the validity of the information and what are we doing about it.

DR. QUACKENBUSH: Do we have any questions from the audience? If not, I will pose one more.

One of the things that strikes me about the cyber environment is that time "warps." We have some types

of vulnerabilities that are very fast moving once they are exercised. On the other hand, we have Trojans and bots that may exist for long periods of time in our network, and we don't know they are there until they are released.

So as we are looking at various governance models and risk management architectures, we need to consider the time factor. We have many "bells and whistles" on our network that are going off, giving us a lot of data just about what is currently happening. I am wondering whether the panelists see the need for game-changing approaches to analytics in terms of helping serve the information security cause.

DR. HUGHES: We have a researcher at George Mason whose name is Sushil Jajodia who heads up our Security Institute. As part of his research, he has analyzed the amount of information that comes into a typical large facility data center. He looked at logs including the visuals that the network guys watch, the telephone calls from the support center reporting ongoing incidents, and paper generated by intrusion detection and intrusion prevention systems.

After studying many data centers, he concluded that the amount of paper generated and the amount of information that has to be processed and analyzed is beyond our throughput capability. He told me that as CIO at Mason, I would have to assign every single IT person in my organization to do nothing but analyze information. Obviously, this is not possible. Our IT people have many other responsibilities not related to security, i.e. installing and fixing computers.

Dr. Jajodia then tasked his research team on investigating a new approach. His new idea is, "enough with the paperwork." What we need to do is start with the "crown jewels," the highly sensitive data, and analyze whether there is a path to that sensitive data from the next level in the perimeter. Dr. Jajodia would typically identify five or six paths in the next level – because people use the data so there are multiple paths. Then he would find the originating points of these paths, moving back level by level, machine by machine. The end result was, he was able to capture for me a path from a student lab machine that went through five layers and eventually was able, with a password it had captured in the third layer, to get into data that I thought was highly secure. Dr. Jajodia's research team has now developed an automated system to do this that we are testing out.

My hope is that this system will be generalized and lots of facilities will be able to use it, because otherwise I don't know what we are going to do with all these logs. At George Mason, we have now passed a rule that you cannot turn the logging algorithm off on any machine, and that if a machine has sensitive data, the logs have to be delivered to the security officer. But I can't make a rule that the security officer will read them, because he is already working 60 hours a week.

DR. MARTIN: This is one of my particularly difficult struggles. We have been experimenting with the log correlation engines and related tools to try to pull the logs in electronically, sort them out and try to bubble up the most important things to look at. There are many challenges here.

As I previously mentioned, we have silos that are created when each team is performing a highly focused security effort. The teams understand what is happening within their areas of responsibility, but there is not an effective communication across those areas of responsibility. That is an area ripe for improvement. If we can better facilitate information sharing across the silos such that if someone is seeing a security issue of importance, they can more rapidly relate their findings to the other teams.

MR. MCNAUGHT: I will echo what Dr. Hughes has said. Intrusion detection systems are not very useful unless you have a rule set that goes with them, and you have some way of managing the large amounts of data generated. This is one of our important research areas. We are developing better intrusion detection systems that will provide the data that is most needed to ferret out who is attacking your system and where.

DR. MARTIN: I did have a second thought related to Dr. Hughes' model that her team is experimenting with. I think the model may have value as we explore the health information exchanges. We are now discussing layering access to sensitive data further and further away from the span of control that we have. It will be very important to be able to send that information out and know exactly who is getting to that information and how they are getting to it.

DR. BAKER: Lunch is now available in the exhibit area. Please fill out and return your evaluation forms. We will reconvene at 1:25 to hear a keynote presentation from Susan Armstrong from the Department of Homeland Security. This is a late addition to our program. We will need to constrict the afternoon panels a little bit to accommodate Susan.

DHS Keynote Address

DR. BAKER: I am very pleased to be able to introduce Susan Armstrong. Her title is not accurately listed in the program. She is the Director of the Infrastructure Security Compliance Division at DHS. In that position, she is responsible for chemical industry anti-terrorism standards.

Ms. Armstrong served as the Chief of Staff to Assistant Secretary Bob Stephan in a prior assignment in which she was in charge of the daily operations of DHS' infrastructure protection programs. She has also served as Deputy Chief of Staff for the Information Analysis and Infrastructure Protection Directorate. She is formerly Assistant Director of the Immigration and Naturalization Service Internal Investigation Branch. She also served in the State Department's Office of the Inspector General. I am very pleased now to introduce Susan Armstrong. Thank you for being here on such short notice.

MS. SUSAN ARMSTRONG: Thank you very much for your kind introduction. I just had my actual sixth anniversary with DHS. We count the years in dog years, so I have actually been with the Department for 42 years.

I am glad to be here today. This is an important symposium, and you all are practitioners in a very important field to both physical security, cyber security and people security. I think that is one of the most complex challenges that we face in this era of homeland security because we are charged with protecting facilities that house workers, their children, big events, important research, and important scientific discoveries. How do you protect those and keep them economically significant without turning them into fortresses?

My purpose here today is to give you a high level overview of what the Office of Infrastructure Protection at DHS is doing in this area in both voluntary and regulatory space. IP's mission, as I am sure you all know, is to lead and coordinate the national effort to reduce risk to critical infrastructure and key resources [CIKR] posed by acts of terrorism and to enable national preparedness, timely response and rapid recovery in the event of an attack, natural disaster or other emergency – the all hazards environment.

Under the construct of the National Infrastructure Protection Plan [NIPP], we [IP] serve as the Commercial Facilities Sector Specific Agency [SSA]. We work with that sector, which is comprised of a vast array of large and complex facilities designed to house business activities, personal commercial transactions, recreational pastimes and accommodations. These facilities face a set of common vulnerabilities: easy access by a large number of people, accessibility to items of unique value or significance, certain events which guarantee a significant and mobile crowd, and numerous entrances and exits for people and deliveries.

Our goal in IP is to understand the unique nature of different types of commercial facilities and to design protective programs and support tools applicable to the specific vulnerabilities and necessities of each.

The commercial infrastructure sector is literally A to Z – arenas to zoos. There are eight sub-sectors called public assembly, sports leagues, resorts, lodging, outdoor events, entertainment and media, real estate and retail. A few examples of our activities with and in that sector include the publication of protective measures guidance. Over the last few years we have published protective guidance in collaboration with Major League Baseball, Major League Soccer, NASCAR, the National Basketball Association, the National Hockey League (Go Caps!), the National Football League, and the U.S. Tennis Association. We have developed a guide that discusses potential threats, terrorist objectives, current threat streams and applicable protective measures that would be effective for us at sporting facilities and at sporting events. That guide is available to all of our private sector partners that operate in the sporting industry. It is the first in a series of such guidance publications that we are working on with the commercial facilities sector. We are at present working with lodging, retail and the outdoor events sub-sectors on protective measures guides for their facilities.

We have also developed the first mass evacuation planning guide and planning template with NASCAR. The purpose is to allow facilities to assess their risks, reduce their vulnerabilities and increase their level of preparedness should an event requiring evacuation quickly occur. The NASCAR guide is out and we are currently working with the sports leagues and public assembly sub-sectors on guides for their facilities.

We also have the Bombmaking Materials Awareness Program that some of you may have heard about. We developed the "BMAP" in collaboration with the FBI and ATF. The program applies across all 18 sectors and is particularly useful for commercial facilities. The program has particular interest for distributors, wholesalers and warehousers. It helps them educate their employees on careless use of chemicals and other items usable in the fabrication of homemade explosives or improvised explosive devices [IEDs].

I'm sure some of you are aware that in 2005 we developed an online vulnerability identification self assessment tool, particularly aimed at stadiums at that point in time. We called the tool VISAT. The tool enables a facility to conduct its own vulnerability assessment. Based on the assessment results, we send the facility a recommended set of protective measures that takes into consideration the unique characteristics of their site. It could be a convention center like this one, for example.

We have now convened a working group to take VISAT to the next level. The objective is to transform it into a risk self-assessment tool that will address the combination of vulnerability, threats, and potential consequences were a facility to be attacked or suffer a major incident. This is a major effort this year.

Being the prescient agency that we are, in our infancy, in September 2006 we published a pandemic influenza guide for CIKR addressing preparedness, response and recovery in the face of a pandemic. We recently dusted its cover and reissued it as a resource for the H1N1 flu now of concern. Our entire pandemic engagement focuses on defining essential personnel and business continuity planning, particularly in the context of potential large-scale employee absenteeism.

We have also mapped the threat against critical infrastructure. We developed the CIKR information sharing environment [ISE] which is the subcomponent of the larger ISE, and put in place measures to grant facility owners and operators clearances so that they can routinely attend classified threat briefings. We have developed HSIN, the Homeland Security Information Network. The HSIN provides the critical sectors with portals to use as their information sharing platforms. We had some technical difficulties with that system's development. It was delayed a little bit, but now is back on track to be provided to all sectors.

One of our other services for commercial facilities in particular is teleconferencing following high-consequence events. When there is an incident, such as the 2008 attacks in Mumbai, India, we can quickly convene a phone call with the private sector. In fact, the day after that attack, we had a call with over 300 private-sector owners and operators to tell them what we knew, what the intel was, what the implications were, and some recommended protective measures that they could employ should such an attack be attempted here. Also, it has become a holiday tradition for us to, along with the FBI, issue a threat and informational bulletin right around the time of Black Friday for the holiday shopping season.

So these are some ways in the voluntary space that we work with private industry, with CIKR owners and operators to better protect their facilities. You are also going to see a very snazzy video later this afternoon that I am sure will be up on YouTube tomorrow. You are going to hear from one of our protective security advisors, Ollie Gagnon, in the next panel. He is one of a cadre of people that we have deployed across the nation charged with helping to protect their own communities and serving as a DHS representative for tools and materials support and resources in local communities.

Now, in regulatory space we have gone to the dark side. We are implementing the Chemical Facility Antiterrorism Standards [CFAS], which is published as 6 CFR Part 27. This was a culmination of a number of years of discussions and negotiations among the chemical industry, Congress, and DHS over whether voluntary measures were enough within that sector. You probably have heard the – I won't say rhetoric, because I believe it is true – that certain high-risk chemical facilities may constitute pre-positioned targets in the United States. So CFAS came about after a lengthy and spirited debate on Section 550 of the DHS Appropriations Act of 2007, which gave DHS the authority to regulate security at high-risk chemical facilities.

What is unique about CFAS is that it doesn't cover only what you traditionally think of as a chemical facility – a big manufacturing or distribution plant. Rather, CFAS is focused on chemicals of interest in certain screening threshold quantities. There are a number of different types of facilities that fall under CFAS including university and research labs, the traditional manufacturing and distribution community, food and agricultural production facilities, and a host of others, including the semiconductor industry. So CFAS covers a wide array of facilities.

However, there are some exemptions to CFAS which are in play right now as the Congress writes a new authorizing bill for CFAS. The program actually is scheduled to sunset this October, but we are pretty confident that it will be continued.

So what is exempt from CFAS currently? Facilities regulated under MTSA, the Maritime Transportation Security Act, certain facilities regulated by the Nuclear Regulatory Commission, DoD and DOE owned and operated facilities and water treatment and wastewater treatment facilities are exempt. But that leaves us with a fairly decent universe of covered facilities.

We were given six months from the time the legislation was enacted to write our rules and begin to implement them. If you have ever dealt with government regulations,

you know that six months is like a nanosecond in time. But we actually met the suspense. We published our interim final rule on April 19th of 2007, and it went into effect that June. Then we followed it up in November with Appendix A to CFAS. Appendix A scopes the program. It identifies 322 chemicals of interest and their screening threshold quantities. Some chemicals, depending on the security issue they represent, have different screening threshold quantities [STQs].

The security issues that we address with CFAS are: [1] does a chemical represent a release hazard in terms of a toxic explosive or flammable release that could harm surrounding population; [2] do the chemicals represent a theft and diversion concern; that is, are they in and of themselves a chemical weapon or precursor, and could they be easily taken off site and turned into a weapon or an IED? And [3] does the chemical represent a sabotage or contamination concern; that is, is it a chemical that all you have to do is combine it with water and you get a toxic vapor cloud?

Appendix A was published in November of 2007. The next big regulatory deadline was January 22, 2008, the date when the first piece of the compliance tool that we built for CFAS was due. This is what we call the "tox screens." Our compliance tools are all E-compliant. They are all available over a secure web-based portal. We are not a paper regulatory program.

By the due date for the tox screens, we had received a total of 29,453 submissions. What the tox screens basically give us was information about a facility and its chemical holdings. The screen information allows us to do an assessment of its potential consequences.

On June 23, 2008, we notified 7,010 facilities nationwide that they were preliminarily placed into one of four tiers under CFAS; with tier one being the highest risk. They were all given a suspense date to complete and submit our security vulnerability assessment [SVAs]. To date, over 5,800 facilities have submitted their SVAs. We have reviewed the SVA for physical security, chemical security and cyber security content. Based on these reviews, we will make a final hearing risk determination.

You are hearing this first. We are hoping to begin the notification process as early as tomorrow of the final tier one facilities. We will inform these facilities that they are indeed a final tier one and the due date for their site security plan which is the third piece of our compliance tool. I hear my BlackBerry ringing in my purse. I hope that means the White House is OK with our plan. So you are literally hearing this first.

One of the things about CFAS that is unique in the world of major regulatory programs is that, by statute, we cannot prescribe a particular security measure for a facility. That is, I can't state I am not going to accept your site security plan until you build a crocodile filled moat around your facility. It is not the way this program was enacted or designed.

There is a lot of flexibility in CFAS. In fact, we have received over 36,348 tox screens to date. These reflect companies actually thinking about their holdings. This indicates, for example, that university laboratories maybe doing an inventories for the first time in many years and finding that the chemical weapon those grad students made in the '80s may no longer be needed, and thereby increasing overall security.

We have also seen that companies are thinking how they are distributing particular chemicals, such as phosgene or arsine gas, and maybe cutting down on the number of facilities in their supply chain that hold those chemicals. We believe that CFAS is having a big impact on the ground already, even though we have not moved into the site security plan phase right at this moment.

I also want to share with you an example of something that I am afraid we are going to be seeing more frequently as CFAS takes effect, when our inspectors go to check out a site. Recently inspectors visited a site only to find that it had closed. The owner had declared bankruptcy. The site had been deserted since January and there were two large tanks of hydrofluoric acid that had begun to leak, sitting unguarded with the gates open. An elementary school is located about 150 feet away.

In this case we were able to notify EPA, and get them on site the next day to start removing the chemicals from the site. So here is another one of the benefits of CFAS. I am hoping that we don't see lots of closed facilities given the present economic situation.

Currently our universe of covered facilities is 6,407. In our preliminary determination there are 182 facilities in tier one, 680 in tier two, 1,612 in tier three, and 3,933 in tier four. As I mentioned, we are about to make the notification to tier one facilities and they will have 120 days to complete their site security plan [SSP] – another piece of our compliance tool.
I want to say a couple of words about the SSP because number one, I am hoping you are interested and number two, I want to end with a lesson learned that we have incorporated into the site security plan.

As I said, the CFAS is not a prescriptive program. We can't prescribe, "You will do these things." So in writing our rules and analyzing our enabling statute, we sat around and thought about what we can do to help industry comply. How about if we establish risk-based performance standards for the program and allow facilities design their own layered defense or a range of options for compliance with a particular standard?

That is exactly what we did. In concert with putting our SSP template on our website with its instructions, we have produced and are about to issue a very comprehensive risk-based performance standards [RBPS] guidance document. What that does is allows facilities to consider all 18 of the RBPS, which are traditional physical security measures such as restricting area perimeters, securing site assets, screening and control access, deterrence, detection and delay of attacks. They need to address how to deal with shipping, receipt and storage, how to guard against theft and diversion, how to guard against sabotage. The document includes attention to cyber security posture, both in terms of control systems and ordering and invoicing systems. Also, what can you tell us about who and how will you respond if something goes wrong, how do you monitor the facility, how do you train your personnel, what is your personal surety program? What do you do in terms of an elevated threat, how do you deal with specific threats, vulnerabilities or risks, based on your chemical holdings? How do you handle reporting of significant security incidents, how do you respond when there is an incident or a suspicious activity at your facility? Then there are a couple of catchall RBPS's.

Having listed these risk standards for you, I would like to relay to you something that we at IP have learned in both voluntary and regulatory space. That is – no shocker here – you can't do homeland security from Washington, D.C. If you are looking at a complex facility that needs protection, multi-jurisdictional planning is necessary. The right people have to know who is going to respond, who is going to do what, who has what capabilities in the surrounding local jurisdictions or counties that can be brought to bear at a facility. This planning is key.

Several years ago we instituted a program in IP called "comprehensive reviews." We started with nuclear facilities. For the first time, we tried to bring everybody to the table, the owner and the operator, the NRC, the FBI, IP, State and facility-local jurisdictions. We assembled everyone and with the objective of developing a multi-jurisdictional security and incident management plan for the facility that IP has designated worthy of protecting.

What we found back in the 2005-2006 time-frame when we started this was that our called meeting was often the first time the owner and operator and the local fire chief or the local chief of police had met each other. This is significant. We built this process into the RBPS for CFAS on purpose. We want to make sure that facilities know who their first responders are. We want to help them with their security planning. We want to facilitate future exercises involving all of these concerned parties around a high-risk chemical facility.

So that is an important lesson that IP has learned in both voluntary and regulatory space. In your roles as security planners, people responsible for security at a key facility or university or consulting with your clients who want your best advice on how to secure their facility and still remain economically viable – I hope that you will pass this lesson on to them.

Finally, I will mention one thing that you will see as the FY 2010 budget rolls out. I think there are some members of Federal Protective Service here at this symposium. A new move in the FY 2010 budget request is there to move the Federal Protective Service from Immigration and Customs Enforcement to the National Protections and Programs Directorate of which IP is a part. I think it is a good idea to start consolidating the entities that have primary infrastructure protection responsibilities in one place within DHS. The budget will be completed when we go into conference. There is a new development that may come to fruition. I personally hope it does. I see a lot of common ground between IP and FPS that we share on the Interagency Security Committee. This move would improve our abilities to leverage each other and do our jobs better.

At this point I believe we may have a couple of minutes for questions.

QUESTION: Susan, I am Battalion Chief Blair Daley with the Baltimore County Fire Department. I am assigned to the MCAT Center, the fusion center. Our duties are critical infrastructure. So I deal a lot with ACAMS [Automated Critical Asset Management System]. I'm not real happy with it, but is it going to get better? For instance, Friday I am going down to Denton on the Eastern Shore. None of the information is in there yet. The local fire departments aren't in there, the police department, so I am doing that, but it bogs you down.

MS. ARMSTRONG: I will tell my good friend Rick Triggers that you had that comment.

CHIEF DALEY: I don't know how much staff is there, but I'm just wondering if they are going to beef it up.
MS. ARMSTRONG: Yes. IP is literally a startup within a startup organization. We are working hard to staff up, but Rick is in the process of hiring to supplement the ACAMS program. For those of you who don't know what ACAMS is, it is a tool designed in conjunction with the Los Angeles Police Department back in 2005 to help local jurisdictions catalog assets and facilities that are important to them. It provides guidance to build a database of information in case you need to go into incident management mode at one of those facilities. I will take your comment back, and I appreciate it.

DR. STAFFO: Gary Staffo, Department of Energy. How do we balance having performance-based versus requirement-oriented standards? From the perspective that the more we put into requirements, the more information we give out to those who might use them against us.

MS. ARMSTRONG: Yes, I hear your point. One of the things that CFAS does is establish a new information safeguards protocol called CVI, which stands for chemical terrorism vulnerability information. This protocol applies in particular to facilities' submissions to us –their tox screen, their SVA, their SSP and all the correspondence back and forth between us and the facility. The CVI exempts this correspondence from public disclosure.

QUESTION: Just one comment I was going to make in relation to an earlier presentation. I just returned from a visit to the San Francisco Emergency Response Center. I was very impressed with California's ability to do what we were just talking about, to put all this information into a system, to know where all of your assets and resources are, and to be able to use those in a very efficient and effective manner to relay where the needs are. That is a model for HS to look at.

MS. ARMSTRONG: Definitely. With ACAMS starting in Los Angeles, California has become a major user of our tools for their own CIP program. If anybody is interested in learning more about ACAMS, please let one of the symposium facilitators know. We will be happy to get you more information. We are up to 36 or 37 states that are using ACAMS on a routine basis with their police and fire communities.

QUESTION: Susan, I have a question. I am Justine Pontius with Customs and Border Protection. I am working in the Secure Border Initiative, and we are installing communications and detection equipment along the borders. Is anyone in your group looking at the critical infrastructure designation or any of the properties that these sites and various facilities should have?
MS. ARMSTRONG: There are a number of people. IP runs a program called the tier one and two asset list. That is a combination assets nominated by the States. We are looking at those nominations and vetting them against particular criteria to form tier one and two assets. Tier one is a very small subset of facilities or assets that have been named based on credible threat reporting. Tier two is a larger universe of about 3,000 facilities nationwide that we think rise above from a regional economic or national economic or consequence perspective. We use the tier one and two list to prioritize where the Protective Security Advisors [PSAs] visit, in terms of enhanced security and for targeting grant dollars. To answer your question, yes, there are a number of tier one and two assets along the southwest border to include some of the ports of entry.

QUESTION: Hi, Amy Smith with Design and Construction Strategies. Do you see any of these programs that you are working on eventually taking advantage of the Virtual Alabama or Virtual USA platform that has been in pilot phase?

MS. ARMSTRONG: Yes. We have, actually through our infrastructure analysis and strategies division, been part of the pilot of Virtual Alabama. We are looking at it and other GIS-type applications for the tools that we hope to develop and roll out to State and other jurisdictions. We're out of time and I will not keep Mr. Becraft, an old friend, from kicking off his panel. I want to thank you again for the opportunity to be here today.

Panel Three: Facility Protection Case Studies

DR. BAKER: We are now to our final panel of the symposium. The panel will consider selected facility protection case studies. I would like to introduce Mike Becraft, who is heading up this group. Mike is the Senior Vice President of Serco North America. He heads the Homeland Security Division and the Mission Critical Outsourcing Division, a total of 2500 people under his leadership. His customers are Department of Homeland Security, Department of the Army, Department of the Navy, Department of State. Prior to his corporate career, he served as a senior executive in the U.S. Immigration and Naturalization Service, rising to Deputy Commissioner there. He served in the U.S. Army prior to that, and retired with a full career as an O-6 with two combat tours in Vietnam. I should also mention that he was chief of counter-narcotics for the Joint Chiefs of Staff. So Mike has a strong and diverse background in our subject matter today. Mike, you're on!

MR. BECRAFT: I will make one correction. It is not the Homeland Security and Mission Services Group any longer. My group is now called the Federal Civilian Services Group at Serco North America. When we merged SI International with Serco North America in late December of this past year, I now have responsibility for about 5,000 people in the U.S. and Canada.

First off, I just want to mention, although I think Sue has departed, that Sue is what I refer to as a rocky red-hot. She worked for us back at INS when I was the chief of staff and deputy commissioner. She worked in internal audit, and she was a rising star at that time. Clearly you can see today from her performance up here this afternoon that she has room to continue to move up that ladder of success, in my opinion.

Also, I want to mention, my last job at the INS and in DHS was to split the Immigration and Naturalization Service up three ways, and move part of it into Customs and Border Protection, create immigration and Customs enforcement, and split off all our benefit side into what became the Citizenship and Immigration Services. In that process, they decided to give the Federal Protective Service to Immigration and Customs Enforcement, and for the life of us we couldn't figure out why they were doing that. As Susan just mentioned, it looks like they are going to move to a more appropriate location.

We have three great speakers today, very interesting people. I think it will be a good capstone for the panels that you have heard today.

The first speaker is David Achterberg. Besides being an elk hunter, David is also a professional engineer. He is Director of the Office of Security, Safety and Law Enforcement, Bureau of Reclamation, U.S. Department of the Interior. David will first give you a quick overview of the Bureau of Reclamation. Then he will focus on two of his large facilities that he has security responsibility for. You need to know, he has got responsibility for over 350 dams and reservoirs in the Western part of the United States. The two major facilities he will talk about are the Grand Coulee and the Hoover Dam.

The second speaker is John Paczkowski. John is a Distinguished Fellow from the Naval Postgraduate School at the U.S. Department of Homeland Security, where he is working for the Director of Emergency Management and Security within FEMA – this is a part time job for John, it is a year sabbatical. He is also, in reality, the Director of Emergency Management and Security for the Port Authority of New York and New Jersey. That is a big job, a big responsibility.

Our last speaker at the end, the name that you have heard more times today, mentioned by Bill Austin, and again by Sue Armstrong this afternoon, is Ollie Gagnon. Ollie is the Protective Security Advisor, as Sue mentioned, for the Central Florida District, U.S. Department of Homeland Security. In his previous life, he was with the Defense Threat Reduction Agency. He liked that job very much. He got to know Bill Austin there. But the really fascinating assignment he had when he was a career Air Force officer. Ollie served as the Chief of the Presidential Aircraft Security. So he got to ride on Air Force One. He is glad he wasn't on that plane on its latest flight over New York City.

The other disappointment is that the six-minute video that he was going to show today will not be highlights of the Super Bowl game. Ollie had responsibility for coordinating security for this past year's Super Bowl. So he is going to talk about that. As you'll see, he is not going to focus on the stadium, because the security for that event was much broader and required a lot of intense federal, state and local law enforcement coordination.

I want to mention one other thing. Although John Paczkowski got a big job in New York and New Jersey, John was central to the success of turning around the problems in New Orleans post Katrina. John went down there and was every effective in bringing the Port Authority back to life and setting up command and continuity of operations centers.

We will now start with David Achterberg.

MR. DAVID ACHTERBERG: Good afternoon. I am pleased to be here today and get broader insight into the activities the National Research Council. Within the Bureau of Reclamation I have had the pleasure of having a National Research Council review of our security program. I have also had DTRA assessments associated with the facilities I will discuss today. I can attest first-hand to the value of external reviews to a program or to a particular facility in helping to evaluate the potential vulnerabilities and also the single point vulnerabilities that we need to avoid. So I am a fan of both our internal Reclamation programs perspectives and getting that valuable external perspective from organizations like NRC and DTRA.

Within Reclamation, I grew up working in the context of the dam safety program. This program was generated by the Bureau of Reclamation in 1976, following the failure of Teton Dam. Because of a tragic event, we formulated a program that has had major benefits. By approaching a program with openness and with independent review, we

have come through a progression of building a stronger program. Sometimes it is not the most pleasant thing when you talk to that doctor after a physical examination. You say "I know what is back there, but I didn't really want to look at it that close." Likewise, external evaluations of security programs provide value in identifying details where attention is needed to build a stronger security program.

I would first like to give you brief perspective on Bureau of Reclamation. Some folks may know about us – many do not. We are a water resource agency. We operate in the 17 western States. We are split into five regional offices. I work in a headquarters office located in Denver. Reclamation has a very small footprint here in Washington, probably less than 100 people work in our Washington office, so we are really headquartered out of Denver.

In that respect, I have responsibility for the Bureau's security, safety and law enforcement program. But I must tell you, to be able to be effective, I have to rely on the folks who operate those facilities, who take ownership, and have boots on the ground. So I am in a role of administering a program that needs to be pushed out to the field.

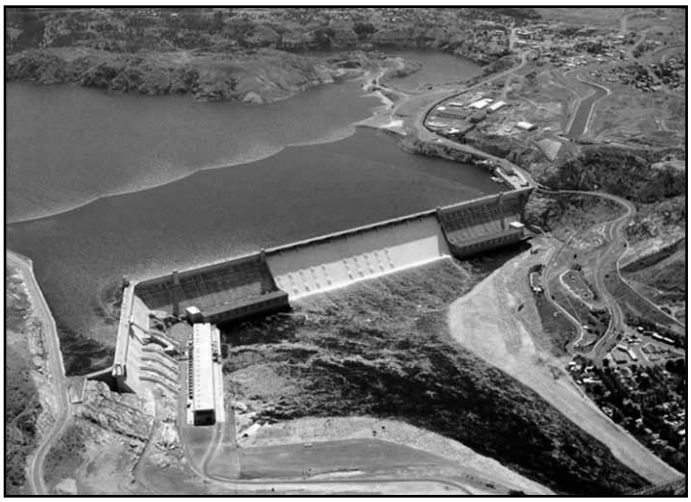
I am striving to administer the security in such a way that we impose no reduction in mission. After 9/11 we made a concerted effort to insure that we continued to deliver water and power from our facilities without compromise as we immediately instituted security measures in response to that event. We have been going through a process to develop credible security methodologies balancing risk with costs. We acknowledge that we must accept a certain level of risk.

One of the things that I have learned over the years, working with the security program and performing many assessments, is that I can always find someone who can tell me authoritatively how they can defeat a given location and tell me the force and means needed to do so. Organizations such as the Special Forces, the Navy SEALs and DTRA are particularly good at this. We train our military very well to be able to defeat facility defenses. In that context we look at design bases to counter the tactics that they identify for us. Our objective is to raise the bar, to raise the amounts of effort and resources a malefactor would need to compromise the mission of any of our facilities.

Now to address specific facilities, I'll turn my attention to the Grand Coulee Dam. It is on the Columbia River at an eastern Washington location. Downstream from Grand Coulee Dam on the Columbia is the Chief Joseph Dam, which is a Corps of Engineers facility. There are other downstream facilities including Wells, Rocky Reach, Rock Island, Wampum and Priest Rapids, that are owned by public utility districts. Further down, on the Lower Columbia, there are several Corps of Engineers facilities. If the Grand Coulee Dam were to fail, there is quite a cascading consequence effect on the many facilities downstream.

Grand Coulee's hydropower production is 650,000 megawatts. Up until a few years ago, Grand Coulee had the largest hydropower production in the world. It has now been surpassed by two facilities, one of which is the Three Gorges in China. To give you just a little perspective, the dam is roughly 500 feet high. At the base it is about 550 feet wide, so it is a very massive concrete structure. From end to end the dam is a mile long.

I need to point out some of the many different assets associated with this dam. Focusing just on the dam itself, you can see the locations of the power plants. The spillway is in the center section of the dam. The spillway includes 11 large gates with the ability to release a little over a million cubic feet per second downstream. An irrigation pumping plant is located on the right-hand side of the dam.



Water is pumped to a height of about 250 foot into a canal. From there, the water flows through the feeder canal to North Dam, and then used to irrigate Central Washington.

The variety of missions performed by this facility poses challenges for security. Recognize that this is not just a just not a big piece of concrete – it is a huge industrial complex. We have over 350 people that work to run the hydropower plant. We also have about 300,000 visitors to the facility throughout the year. One of the advantages related to Grand Coulee is the absence of a major highway

crossing the dam. We do have a major highway through the edge of the complex that provides a public right-of-way adjacent to the facility.

Following 9/11 we asked DTRA to provide a vulnerability assessment. They helped us to identify some single point vulnerabilities – vulnerabilities that would, by themselves, cause loss of mission. Based on the DTRA findings, we determined that we needed to have a comprehensive security system that would enable us to protect the complete point set. Traditional ways of pushing a perimeter out with fencing would have been cost and operationally prohibitive.

We took advantage of the fact that the critical assets are internal into the system. We developed a comprehensive security system that included sensors, door alarms, motion detectors, and camera systems integrated to allow us to be able to monitor all the access points into the facility. Access points are important because once someone enters the facility they have access to over seven miles of galleries internal in the dam. If we don't know who has entered the facility, it would take us a very long time to clear that facility and search to make sure that no bad guys are present. So aggressive, comprehensive monitoring is very important.

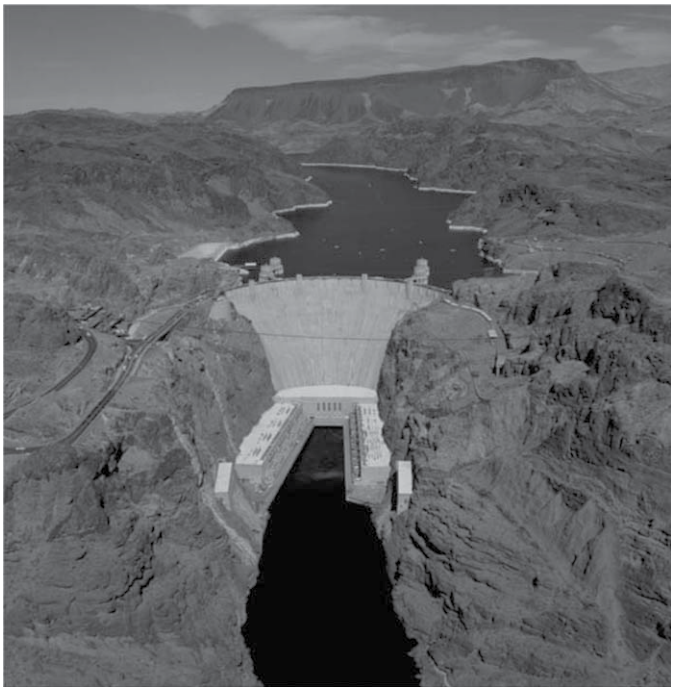
The other thing that we did at Grand Coulee was to develop a federal response team to assist with the job of guarding that facility. These are individuals who are not law enforcement personnel. We heavily leveraged the Department of Energy's training center in standing up this group. The response team was implemented because we are challenged in this part of Washington regarding access to contracts and other resources in time of crisis to protect the facility for an initial period of time until we can get additional outside response. This response force is postured to be able to protect those critical assets until we can get the Washington State Highway Patrol from Spokane and the FBI to the site.

About two years ago, we organized a comprehensive exercise at Grand Coulee in which we asked the Oak Ridge Institute [ORISE] to create a series of scenarios. We conducted an exercise in which we practiced running our incident command and unified command procedures. We then practiced our ability to react and respond at the facility. An important element of that event was exercising our public affairs office ability to interact with the media during the event.

There continue to be challenges regarding security at this facility. A particular challenge is the high turnover rate associated with the guard force. This is a remote part of the country, so it is important that we are able to recruit and retain well-trained individuals. We are evaluating pay and benefit upgrades for the guard force. We recognize that people attracted to response force careers like to shoot, train, and compete. Those are benefits that we can provide. If they enjoy their job, if they enjoy their training, they will be able to work through some of the tedious aspects of guarding and monitoring the facility.

I would now like to turn your attention to the Hoover Dam. Quite often people ask if Hoover is our biggest facility. They are surprised when my answer is no. I just showed you our biggest facility, Grand Coulee. Hoover is actually taller – about 720 feet high. It is considered to be an arch dam. What people don't realize is that the thickness at the base of the dam is about 500 feet. It is almost as thick at its base as Grand Coulee.

As far as hydropower production, there are two power plants – a Nevada Plant and an Arizona Plant that sit on opposite sides of the dam. As far as power production, the amount of water that can flow through either one of these sides is the equivalent to what flows through one power unit at Grand Coulee in the third power plant where they have the big power production units. So that gives you one comparison of scale. Although Hoover produces a lot of power, it is not in the same magnitude class as Grand Coulee.



There is no doubt that Hoover Dam is a national icon. But its most critical mission is water supply. The reservoir behind Hoover holds roughly 28 million acre feet of water. It is a major water supply to Southwest Arizona, New Mexico, and California. The most critical area supplied is California.

Once again, the dam is a large industrial complex that performs many functions. We have spillway intakes. There is a visitors' center at Hoover that serves between 500 thousand and one million people annually. It's quite a different security situation in that the crest of the dam is open for traffic - between 8,000 and 25,000 cars a day cross the dam. It is a very open and public site. On the surface of the dam, we have a very structured tour route. One of the major challenges after 9/11 was re-establishing the tour program so that the public could again visit the plant, recognize what the facility is and does and, at the same time, be subject to appropriate security controls to monitor tours as they move through the facility. We work with our tour guides regarding their presentations to ensure that they are discreet. They need guidance on sensitive information to avoid as they describe the facility to the public and answer questions.

With regard to Hoover, similar to Grand Coulee, there are a variety of access points. Our security is largely focused on monitoring these access points using camera assessment and the motion detection. Any place where Reclamation has a camera in place, there are other sensors including motion detection. The concept of having someone sit and watch an unchanging screen is problematic and wearisome – the guards need an alert on which screen to watch and when an intrusion may be occurring. So as we develop comprehensive monitoring systems, we are including alarms in conjunction with the camera to help us with the assessment.

Once again, Hoover Dam is a major operating industrial plant. Many people need to be moving around inside and outside the plant. So the door alarm and camera assessment are very valuable to enable us to determine who has entered or is moving around the facility.

A major security issue that we had to address after 9/11 is controlling access to the crest of the dam. Truck traffic was curtailed immediately following 9/11. That was not because of the structural vulnerability of the dam, but because of the highly public nature of the site and the large number of people moving through. Prudence dictated controlling the size of the vehicles that moved in and through the facility.

The dam was built in the 1930s. It was not constructed to accommodate today's large semi trailers moving across the dam. We have rerouted that traffic. As some of you may know, a major bridge is being built downstream from the dam. That will have major benefits for our security program. Once the bridge is in place – sometime in 2010 – we will be able to pull all regular traffic off the facility crest. We will continue to keep the dam crest open for visitation. We want the American public on their Western vacation to be able to drive across the dam, but it will be a visitor experience rather than a transportation hassle associated with the facility.

At Hoover we have a backup security system. We have a limited police force on-site. We augment this with contract security guards that work in conjunction with the on-site police force. The contract guards primarily provide deterrence and immediate of response for facility security incidents.

Similar to Grand Coulee, we conducted a major exercise last year at Hoover Dam, working with Clark County authorities out of Las Vegas including their SWAT team, the FBI and others. We worked on a unified command and incident command to be able to manage a response at that facility. These exercises provide major value. Just as with Grand Coulee, the Hoover exercise was an independent event based on ORISE scenarios. We also had an independent assessment of the exercise results.

With that, I thank you very much for the opportunity to present.

MR. BECRAFT: I failed to mention that our next speaker, John Paczkowski, is a retired United States Marine Corps Reserve Colonel.

MR. JOHN PACZKOWSKI: Mike, thanks very much. Thank you for your very kind introduction.

I once had a boss very much like Mike, a handsome, distinguished guy. He gave me some advice before a presentation to the board. In fact, it was my very first presentation. My boss noticed that I was kind of nervous. He said, "John, it's easy – just be good." I started to shrink in my chair. He then said, "Well, if you can't be good, be funny." I shrank even lower. He said, "Well, if you can't be funny, show them a lot of pictures, and if you don't have a lot of pictures, at least be brief. If you can't be brief, be gone."

To show you where I am on that sliding scale of speakerdom, I am going to show you a lot of pictures, and I will attempt

be brief. I will give you a short overview of who we are and what we do. Then I will talk to you about our security challenges and what we have done to secure our critical infrastructure since September 11, 2001. I will conclude by providing you with a sense of the way ahead for the Port Authority.

Of course, New York City is the big show. The two largest attacks from international terrorists in the nation's history occurred here. New York's status as a world class city makes it tremendously vulnerable to terrorism. It is also tremendously vulnerable to natural hazards.

The Port Authority is critical to the lifeline of New York City. We have been around for a long time. We have a mission of transportation, trade and economic development in the New York region, which is a 1,500 square mile jurisdiction. A key factor is that we are self-supporting, largely from business revenue. We get a very small offset from tax revenue to the Port Authority. We receive airport improvement grants, and we receive a small percentage of the homeland security money that comes to the region. However, for the most part, we pay for our own security.

A key statistic here is our total employee base of 7,000. That is down from about 9,000 or 9,500 when I first started in the Port Authority. We have contracted out a lot of our facility operations. We have downsized and improved efficiency. A large percentage of our workforce,

1,600 of that 7,000, are Port Authority police officers. The Port Authority is the 26th or 27th largest police jurisdiction in the country. It pales in comparison to New York City, which employs 37,000 plus. Nonetheless, we have a substantial force that is backed up by a very large contract security force.

We move it all – trains, planes, automobiles. We move data communications through a satellite communications facility in Staten Island. We move garbage through our resource recovery plant in Essex County, New Jersey. So if it moves into, through, around or even under the Port of New York or New Jersey, it probably comes across a Port Authority facility.

Within our 1,500 square mile jurisdiction are about 20 major facilities. These include all the region's major commercial airports, Kennedy, Newark, and La Guardia. We recently acquired Stewart Airport, which is about an hour north of the city as our fourth major jetport. We have the largest general aviation facility at Teterboro in Northern New Jersey. Our jurisdiction includes the interstate tunnels and bridges – the George Washington Bridge to the north, the Lincoln and Holland Tunnels, and the interstate Staten Island bridges. The Verrazano Bridge is not ours because it is wholly within the state of New York.

And of course, we are responsible for the port facilities including Newark and Elizabeth - the largest container facilities on the East Coast, the third largest in the country. In addition to that, we operate Port Authority Trans-Hudson, which is a rapid rail transit system between Newark, New Jersey, downtown Manhattan and Midtown Manhattan. You may recall on 9/11, the south tubes of the Port Authority Trans-Hudson were totally flooded after the collapse of the Twin Towers. We also operate a number of lesser commercial facilities around the region, resource recovery plants and other commercial properties.

We move a lot of goods from a lot of people – our Port serves a ten-state hinterland of 70 to 80 million people. A lot of people depend upon what comes through the port. The Port was closed following 9/11. After two or three days we had governors in New England calling us to get the Port reopened because they were running out of gasoline. The Port is critical, not only to the economic life of the New York City area, but to the entire Northeast.

Our security challenges are not much different from any other major metropolitan area. Many of our facilities are embedded with the local bedroom communities in Northern New Jersey. We are identified as high threat targets. As you might guess, the George Washington Bridge, the Lincoln Tunnel, and the John F. Kennedy International Airport are all signature targets. Like everyone else, we need to balance security with mobility. We like to think of the transportation system as the circulatory system of commerce, and commerce being the lifeblood of the region's economy.

The Port Authority owned and operated the World Trade Center. It was our corporate home for 30 years. We lost 84 Port Authority employees that day, including our

executive director, our superintendent of police and a number of senior corporate staff. In addition we lost 37 Port Authority police officers, the largest single loss of life of any policy agency in the nation's history. Of course, it pales in comparison to the losses of the New York Fire Department, but nonetheless a major loss for our small force.

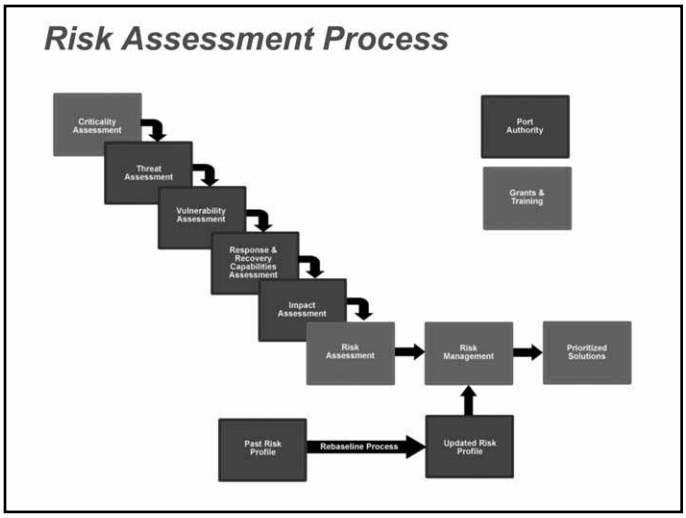
We had no corporate security or emergency management programs in the Port Authority prior to 9/11. We pretty much relied on Port Authority police, with facility police commands, essentially precincts, at each of our facilities to provide us with the needed security over-watch. But we learned very quickly after 9/11 that the game had changed and we needed to change with it.

By way of background, immediately following 9/11 we initiated a series of comprehensive security audits like everyone else. Expert security consultants came back to us with a stack of reports about two feet high. There were 23 individual reports that included 1,500 separate recommendations. When our staff added all these up, our rough order of magnitude estimate was one billion dollars of capital investment to implement the recommended security improvements. This figure was way beyond what the agency could afford at that time. We have conducted agency-wide threat and risk assessments to manage down that number. Based on the risk assessment results, we have implemented a five-year security capital improvement program. I will go into some detail on this program a little later in the presentation.

When the security consultant reports came in, management's questions were predictable. Do we understand what it is we are protecting and why? Are all these recommendations really necessary? If we can't pay for it all, what do we do first? How do we know that our capital investments for security will give us a good return for our dollar?

I had the unenviable job of going to the board and asking them to write a check for $500 million with the promise that I would bring back a five-year risk-based security capital investment program. I immediately reached out to the Department of Justice at the time, informing them that I needed help. They authorized five million dollars for technical assistance, and we went to work with SAIC to put together what was then a best practice model for risk assessment for critical infrastructure.

That risk assessment process is ongoing. In fact, we are now moving from risk assessment to an ongoing program of risk management that I will describe in a little bit more detail. It is basically a six-step process. It includes and builds on the basic risk assessment methodology, but with focus on terrorism. It starts with an assessment of criticality, threat vulnerability, response and recovery assets, assessing the overall impact of various attack scenarios, and then coming up with a stratified listing of risk to individual critical assets at the Port Authority. We repeat this process on a two-year cycle that now permits us to measure the buy-down in risk over time. We have overlaid a cost-benefit model to enable us to not only look at the cost effectiveness over the entire risk management program, but look prospectively at planned investments in security and determine their risk reduction potential. We are then able to fine-tune the entire capital security program.



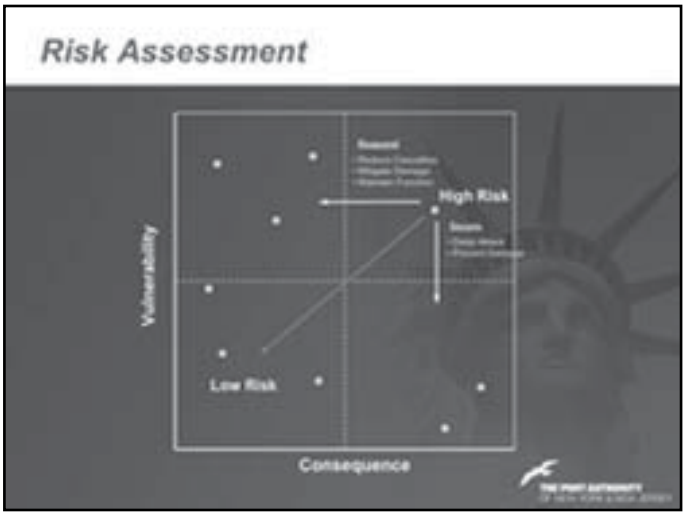
The rubric here is what you have seen elsewhere. Risk is basically determined as a function of vulnerability and consequence. You identify things that the highest combination of risk and consequence and work on those first. There are two ways to buy down risk. You can harden the facilities and prevent an attack from occurring, or you can also improve your response asset. If an attack occurs you can hopefully blunt the attack, and if not, respond quickly to prevent further loss of life.

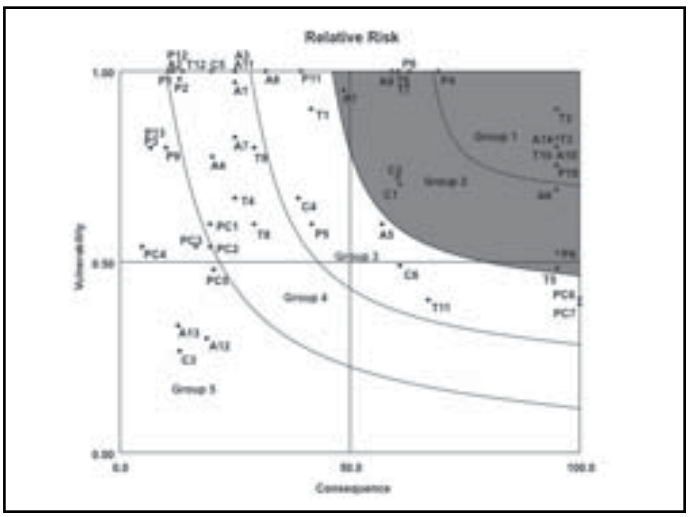
The entire process ends up in something looking like this, which is a very simple risk map. Each dot on that map represents a particular critical asset and an attack type against that asset. So you might find the anchorages to the George Washington Bridge on that map, for example. And the attack type against that anchorage might be a large conventional explosive. This asset/attack combination will show up somewhere on the risk vs. consequences chart. This gives us a visual cue on exactly what we need to pay attention to.

When we repeat the process, we can compare results from one assessment to another and see the movement of those dots from high to low. In some cases we see them return to the high value. With PATH, for example, our Port Authority Tarns-Hudson system, the south tubes were not in operation at the time of our first risk assessment. When we put those into operation, they became an additional asset. They were also the subject of an ongoing investigation because of a plot against the Port Authority Trans-Hudson tubes at the time. Thus, the risk profile for PATH went up, not down. These plots allow us to do is get a good strategic measure of security management performance over time.

Our overall priority initiatives are not unlike those of other organizations – a combination of prevent, protect, respond and recovery strategies.

I have mentioned the Port Authority police department. A lot our investment in the Port Authority police has gone into a tremendously expanded special operations unit. We have integrated not only our emergency services personnel, but our commercial vehicle inspection, our motorcycles and our canine operation, all in the special operation division, so that we can have an integrated capability.





We have expanded our aviation unit as well. We have two Sikorsky S-76 helicopters that provide routine over-watch of our facilities. They have a long-range day and night CCTV downlink capability, so we can send pictures immediately back to our emergency operations center and central policy desk, and also to an incident command post in the field or to other agencies should that become necessary. I've included a few pictures here of that capability.

We invested heavily even before September 11, 2001 in establishing a WMD incident response capability. We had anthrax response cards in the World Trade Center prior to September 11, 2001 as an example of our security upgrades.

My office is the Office of Emergency Management and Security. It is a civilian complement to our uniformed force. I have overall responsibility for everything that is non-law enforcement and security and emergency management related. So our security programs include that ongoing threat and risk assessment program I mentioned. In addition we have programs covering facility security planning, critical infrastructure protection, new technology, and emergency preparedness in terms of emergency operations plans (EOPs). The operations center is mine. Coordination of our executive incident command group is my responsibility. That includes critical incidence management coordination in an actual emergency and working with other regional partners in response to any particular contingency.

We focused an awful lot on the emergency operation center, but I'm not a big fan of brick and mortar EOCs. So we also have established a mobile capability. I have incident response and incident command vehicles that I can deploy that are hot-wired to our Internet at all times. Anything that is on the EOC servers is also replicated in our emergency vehicles. So if my EOC goes down, I can continue operations by moving those mobile assets to a remote site. The large vehicle there can support a 70 work station emergency operations center at an austere site until I can get back into my facility. We also have put a lot into situation awareness tools, but frankly the integration of those tools, GIS, Web OC and the like, still lag tremendously because of the lack of national level standards.

Response operations. Mike mentioned Hurricane Katrina. That was really my unit's baptism of fire to a great degree, other than 9/11. We were asked to provide our mobile satellite communications capability to New Orleans to assist with re-establishing continuity of government down there. We walked into the New Orleans EOC six days after the hurricane hit, one day after the Superdome was evacuated. It had the sign "Unified Command Post" on it. Inside we saw two guys asleep with a hand-held radio and a land line. That was it. There was no federal presence or state presence in the New Orleans EOC. They were operating totally on their own, and they had been awake for six days.

Terry Evert, who is the real hero of New Orleans – the second battle of New Orleans, if you will. He was the homeland security commissioner and in charge of public safety for the City of New Orleans. He had been newly installed the year before. He was awake for six days. He is a former Marine colonel, Vietnam veteran and Navy Cross winner. We told him the last thing that he needed was satellite communications gear right now. We went to work, immediately shifting our focus to help him build an EOC in City Hall. We started with a 30-station EOC and then ultimately moved the entire city's apparatus into the hotel which became a 100-person EOC.

We called in two incident management teams [IMTs], from North Carolina and Arlington, Virginia. Their people moved down to staff the EOC. Then we moved other incident management teams into rotation behind them. Two weeks later we felt the city was basically on its feet. With mission accomplished, we went home. It was a good testament to our ability to move my people to a different location, set up operations and help another city government.

We have implemented a lot in WMD countermeasures. We started very early - before DHS was formed - on radiological detection equipment. We have mobile assets and portal monitors at various facilities. That program became the basis for the" Secure the Cities" program, which is now a NYPD and DHS program to secure Lower Manhattan.

We have devoted a lot of attention to IED [improvised explosive devices] detection technology. We have an active test bed to develop new technologies and the associated CONOPS. It is an important part of Homeland Security. The principal players there are DHS S&T and IP.

With respect to cargo and vehicle security, a lot of our focus in the maritime domain. We are pushing the boundary out away from our Port. We are heavily invested with Customs and Border Protection and the U.S. Coast Guard on things like Operation Safe Commerce and cargo tracking and inspection programs. We have an active cargo vehicle inspection program at Port Authority facilities.

We have improved the security of tunnels and bridges. Principally there has been a lot of physical hardening. We have done a lot of simulation and blast modeling of all Port Authority facilities to identify critical structural members. We have installed access denial and things like bollards and gates based on the blast model results. I think you heard a presenter earlier this morning from Weidlinger talking about the Port Authority's work in this area.

We have done a lot to harden the George Washington Bridge. We have protected the suspender rope cables including anchorage and the inside steel cladding. The bridge is much harder to large conventional explosive devices.

We have also protected the bases of the bridges. On Port Authority Trans-Hudson, we have devoted a lot of attention to access control. Our operations control center was the single point of vulnerability on the system for a long time. We are now building a second, redundant control center. A big focus in transit of course is policing. We have a lot of cops with a lot of dogs all the time.

Tunnel protection is a big issue for us. The tunnels are 100 years old. They are cast iron and extremely vulnerable. They sit under river silt so a major explosion in the tunnel could create catastrophic collapse. This is a big concern to us. We have laser intrusion detection systems that have been deployed in the tunnels to prevent access or at least interdict access to the tunnel portals.

We have a lot of territory to cover relative to Port commerce. You saw the area the Port covers. We are essentially a landlord port, so we rely heavily on the Coast Guard in terms of its work with our tenants and security programs and the maritime security regulations. But we have the overall security command and control center, a CCTV over-watch including very active police patrols.

In aviation, the size of the facilities is a challenge. We have put a lot of effort as a nation into screening passengers, but if you look at major airports around the country, very little effort has gone into perimeter protection. So to get to an aircraft within the airport operating area is a matter of walking a quarter mile down the road and crossing over the fence. If you look like somebody who belongs there you probably won't be challenged when you get to an aircraft. We have over 50 miles of perimeter around our airports that we need to protect. We are using a tremendous

amount of intrusion detection technology that is going in right now. It's a $100 million program. We've installed ground surveillance, and radar systems. Kennedy and La Guardia have a lot of water sites, so we have enhanced police patrol at our aviation facilities. We are installing and using ground surveillance radar and CCTV technology.

With respect to way ahead, we are working very hard to continue to develop our security risk management program. We are now embedding it as a part of our continuous business model, our planning and programming budgeting in the Port Authority. In fact, it is now driving enterprise-wide risk management in the Port Authority writ large.

This year, we are shifting from a security focused risk management program to a multi hazards risk management program. My guys back there are working really hard on five non-terrorist scenarios as part of the security planning. We also have been hit tremendously by the downturn in the economy which has significantly curtailed some of the long term security programs. As a result, our emphasis is on technological and operational integration not only within the Port Authority, but with other jurisdictions.

Now that we have established a very solid base for our internal security program, we are looking at regional interdependencies to address the secondary and tertiary effects of a major regional contingency on the Port Authority and the region we service, both ways. We are now trying to think more in terms of corporate resilience. This requires going beyond the brick and mortar security and working more with our personnel. We are paying increasing attention to the insider threat within our background screening programs.

We continue to recalibrate our risk threshold and to determine how much risk reduction we can afford. The question continues to be what are we willing to trade off in the way of investments in operations to make those security improvements.

MR. BECRAFT: Our next speaker is Mr. Ollie Gagnon who will present the effort involved in protecting the Super Bowl XLII event in Tampa.

MR. OLLIE GAGNON: I was pretty upbeat about coming today until I heard John Paczkowski's scale of speaker qualifications. Now it makes a whole lot of sense why my boss here in Washington told me, "You'd better bring a video, because you are not funny, and you're not good. Bring pictures, but especially bring the video with you."

It is a pleasure to be here. I only have a couple of slides to set the context of my presentation. One is an outreach video that was developed from a series of videos including everything from natural disasters to public outreach to one we did in Philly on national monuments and icons. It is about the outreach efforts going on nationally in relation to the National Infrastructure Protection Plan from the Office of Infrastructure Protection. I am a member of this organization.

The film provides a lot of information on the overall effort went into security for what we consider a very successful Super Bowl. The video also serves as a reprise of today's agenda.

As you watch the screen shots, you see many of things that were discussed today in terms of protecting large venues. You will see our public safety committee that included both private and public sector organizations. You see protection measures that have been installed. You see education and awareness that are such an important part of the overall effort. You will see vulnerability assessments where I was able to include local, state, and federal counterparts.

We get a lot of credit for the Super Bowl. Shortly after the Super Bowl, I had the opportunity participate in Congressional testimony concerning the event. You'll notice that I always say "local, state, federal" in that order. Everything is local, whether it is an emergency, event planning, or protecting a large venue. When we go to a financial institution or we go to a water treatment plant the first thing I tell them is that I'm not the guy who is going to be responding – it will be the other gentlemen and ladies sitting at the table. The local responders always come first. We are in a support role.

As far as the venue, how many people here watched the game? You are probably one of the estimated 154 million that caught some part of the game. Raymond James Stadium is considered one of the crown jewels of the NFL. It is a very modern stadium in all respects including the security measures. The NFL deserves a lot of credit for the stadium features. The existing security features set a good starting baseline.

The footprint of the stadium itself is 1.65 million square feet or 9.2 acres. It usually holds about 65,000 people. That was expanded to 72,000 for the Super Bowl. Obviously it is a large venue. This was my third Super Bowl. I did the last two in Phoenix and Miami, and I will be doing Miami again in 2010 before I am out of the rotation. One thing I noticed during all today's presentations is they provided a great

lead-up to the security effort you will see in the video. As you watch the video, reflect on all the speakers' messages that have come beforehand. Everything presented today, from using a risk-based focus, balanced surveillance, blast effects calculation, modeling, partnerships, cyber security, identifying key infrastructure, to determining single points of vulnerability were integrated into the overall Super Bowl planning, preparation and protection environment. Within DHS, we call single point vulnerabilities "critical nodes" or "significant areas of assets."

Dr. Steger explained that we can't protect everything. We wrestled with this fact during the entire 22 months of planning for the Super Bowl. Although the stadium is one venue, there were probably over a thousand different assets, facilities, and complexes that we considered during the overall process. I am very fortunate to have 80 counterparts around the country. We are here for you. Our consolidated role is to work in an advisory capacity with the public and private sector. So we were able to adopt a lot of existing programs, processes, information, ACAMS [Automated Critical Asset Management System], for the Super Bowl in Florida. One of our major roles is to bring these programs and processes to the state and local levels including both government and the private sector. We then help them to discover potential gaps and weaknesses and to develop an overall protection environment in many different facilities. In the past four years in Tampa, I have visited all types of facilities from dams to water booster stations to blood banks. Critical infrastructure is a big area, and we considered everything related to the operation of the stadium.

I need to briefly mention fences and gates. Gates, fences, and cameras are certainly part of the DHS protection guidance. But DHS has a much more expansive definition of "protection" that includes redundancy and resiliency. Our local, state, federal risk critical infrastructure working group applied this definition as we looked at the many different assets of concern. This working group was instituted under the Public Safety Subcommittee for Super Bowl XLII. We had all our partners, both public and private, working together to evaluate all these different assets.

I will be quite honest with you. NFL has developed a straightforward security plan over the past several years for the stadium itself. It includes everything from a hardened perimeter 300 feet out to gates to surveillance. It is very finely tuned -- I call it an orchestra. They have laid out a security template that they take from city to city. Our working group addressed features including access control, ingress, egress routes, and perimeter control. We also conducted multi-agency exercises including tabletops and our first full-scale exercise at Raymond James Stadium in 2007. That was followed up by our annual emergency preparedness meeting at Raymond James Stadium in cooperation with the Tampa Sports Authority.

We were using the same players. The players I have been dealing with for four years, and that had been together before that, were at the table during the Super Bowl. This is an extremely important point. It is not enough to talk about physical security and the other elements of protection. But organizational and interpersonal relationships in the case of Tampa and what I have seen across the country and in my particular district are the key in achieving overall success. As you can imagine, the event was a highly special event, level one visibility. This helps to bring a lot of automatic attention to the venue site.

When we talked about the Super Bowl in terms of facilities and complexes, there were basically seven primary venues overall. At the stadium we were dealing with two team practice venues – the University of South Florida and the Tampa Bay Buccaneers. We had to address the team hotel, the NFL headquarters hotel and the media center, which was the Convention Center. These are considered the primary venues. Every Super Bowl has them, and they are very important.

We have a scatter diagram of the entire infrastructure that we assessed in relation to the Super Bowl event. We looked at everything from water control structures on bypass canals that provide water to dams, to water treatment plants, to blood banks to bridges. We looked at the entire infrastructure. People at your level with your experience and the environments you work in realize that it is not necessary to go to an event to disrupt the event. Because of infrastructure interdependencies, I can disrupt an event, for instance, by interfering with the dam and water sector. There are eighteen critical infrastructure and key resource sectors that could be used to disrupt the event three days out. There are many different infrastructure targets.

We had several means of assessing this suite of interdependent infrastructure. We leveraged the relationships within Tampa making sure we had all the key players at the table. This also helped us to leverage technology. Tampa, for example, uses a site profile for the critical infrastructure program that they obtained under a Department of Justice grant after 9/11. The state has adopted the automated critical asset management

system, ACAMS, using data matching in order to share the information among the key players. That risk enterprise model was already in place. We were able to build on all the work that had been done over several previous years. We examined the entire infrastructure based on failure consequences – explicitly how failure of a given infrastructure would impact the event. As part of this, it was important to consider how failure would affect not just the event, but the day-to-day life in the Tampa Bay area.

As you might guess, the infrastructure of concern required us to visit and assess many, many different facilities. I don't know how many different water treatment plants we visited in the city and surrounding areas.

As an example, every city has a lot of hotels. We screened the overall hotel list and were able to narrow down the list to about 20 hotels that we considered the higher consequence assets. These included the two team hotels and the NFL headquarters hotels. Just as with Phoenix last year, the teams decided they wanted to change hotels three days before the game.

There were over 760 bridges and overpasses in the Tampa Bay area. Our critical infrastructure protection committee was able to reduce the number to thirty based on consequence of failure. These included the primary bridges over Tampa Bay, and the three or four bridges that cross Hillsborough River between the stadium and the medical treatment facility that also have high commercial value. These decisions could only be made by having the right players at the table.

We had to address an entire region of complexes and facilities. The same approach applies to your facilities. We identified assets spanning several critical infrastructure sectors including water, transportation, and energy. We needed to determine which substations fed our venues of concern. These were assigned higher priority in terms of vulnerability and consequences.

We started with a large collection of assets and narrowed it down. At this point we began to look at the facilities in detail to identify their critical nodes, and single points of vulnerability. We focused our attention on these.

There is never enough money to go around. Action may be limited to helping the asset owners understand what is important. In cases of limited resources, it is important to have the right people present from the facilities of concern. This has been true in general – not just with the Super Bowl. The right people talking and working together can mean the difference between success and failure. Problems arise when security does not talk to the facility management and the facility manager doesn't talk to emergency manager or the emergency manager is not talking to IT. It is important to get the right players together. That is what I really appreciate about the balance of the vulnerability assessment process – they facilitate communication among the people who can make a difference.

How well did Tampa succeed in the overall endeavor? They used a risk-based approach including the basic consequence, vulnerability and threat equation. As Denise Crawford, who is our federal coordinator said, it is a three-hour game. It is a level one event that involves a series of week long events culminating in a three-hour game. The protection environment creation starts way out in advance. The most important part of the process is coordination and collaboration. The event planning took 22 months from the first meeting to the actual event.

We derived major benefit because Tampa is pretty progressive when it comes to disaster planning. They deal with hurricanes. It is not much of a stretch to move their normal public safety environment associated with a natural disaster to a special event environment like the Super Bowl. Tampa has a lot of special events and natural disasters, so they had a foundation we could build on. And they have been progressive in protecting their critical infrastructure protection as well. With Tampa's foundation, we were able to hit the ground running for those 22 months.

More than 85 percent of infrastructure is privately owned. We had private sector members that were already part of the critical infrastructure protection committee and part of the air and maritime security committee long before the event. Key players included CSX for rail and the Tampa Port Authority.

I am using the words "coordination" and "collaboration" for a reason. Coordination is people bringing their individual capabilities to the table and integrating these into the planning process. They may work brilliantly together. It doesn't mean they are going to accomplish anything. The real part comes when you are working towards a common goal. In our case it was ensuring a safe event overall. So there has to be that external-internal focus, multidisciplinary approach, and then leveraging available tools and technologies.

The last thing I want to leave with you is the post-event evaluation. How do can we determine what a successful

event is? In the public safety community and probably most of you in this room, the primary measure is the absence of any major incidents. During the Super Bowl event there were 26 arrests. (This is actually a small number. When the Red Sox played the Rays last year, we ejected 58 Red Sox fans during the first game.) We had four planes intruding into the exclusive air space, none of them hostile. There were ten counterfeit arrests. A DUI woman hit a police horse. These stats are quite acceptable for a level one event. There were over 100,000 visitors in Tampa during the event. $261 million was spent for advertising. That is a record for the networks. The game reached the largest audience ever. Super Bowl XLII was the second most viewed television event of all time.

There was an article that came out about a month ago that addressed the fact that Tampa had budgeted one million dollars for public safety during Super Bowl XLII. That is a low number. The last two Super Bowl cities allocated about four million. Tampa ended up getting a third of their money back. How did this happen? We had relationships that enabled us to leverage the tools, the technologies and the process very effectively. The effort to coordinate organizations' efforts to support the event made all the difference in achieving an effective protection environment.

I'll stop here to make sure we stay on time. Thank you.

MR. BECRAFT: I want to say, I think these were fantastic presentations. I give them another round of applause. We are open to your questions, so please, be brave.

PARTICIPANT: One more question about ACAMS [Automated Critical Asset Management System]. We have played with it now for close to a year. Did you see real good results? Did everybody buy into it?

MR. GAGNON: Actually, I had a very big role in bringing in ACAMS including the pilot program and the whole structure. I became a trainer and trained the first 150 in the State. In my opinion it has great potential. When it started we were at a crawl – now we are up and walking. We will soon be issuing version 2.3. There is a great case study in Phoenix, Arizona. The city uses ACAMS exclusively in their fusion center. During Super Bowl XLII, it was very widely used in terms of the overall identification, prioritization and protection of critical infrastructure. So I see great things. The system is under constant improvement including integration of additional elements. For example, there is a new geospatial mapping feature along with a 3D visualization – the Integrated Common Analytical Viewer [ICAV] next generation.

PARTICIPANT: I'm Amy Smith with Design and Construction Strategies. This is for the gentleman from the Port Authority. You mentioned that in doing your security planning you used a lot of different simulation software. Can you talk a little bit more about which ones you used and which of those you found most effective?

MR. PACZKOWSKI: A lot of the work was actually done through third parties including Weidlinger Associates. I am not sure which software package they used. I do know they did a lot of the computer simulation and blast analysis on a number of our structures including the George Washington Bridge. In addition to Weidlinger, we worked with Lawrence Livermore National Labs, the Port Authority, and the Trans-Hudson Tubes. I don't know if they used commercial packages or not. I do know they did a lot of specialized modeling, not only in terms of the structure, the cast iron, but also relatively new modeling of the under-river silt and the impact that an explosion would have once the cast iron fractured on that silt and the resulting liquefaction. There were some very startling results that came out of that very sophisticated analysis. They found that that once the liquefaction took place and the displacement of the silt occurred, you would get daylighting of water up to the bottom of the river. We initially assumed that we would just get oozing of the silt into the tunnel. That modeling that was later backed up by some physical modeling done by Rensselaer Polytechnic Institute and then physical blast modeling at New Mexico Tech. We also performed physical simulation and a centrifuge of a tunnel section at RPI. We blew up both recently fabricated and then old 100-year cast iron tunnel rings to validate our assumptions. When we did the physical destructive testing of the tunnel rings, we found that the cast iron was actually much more fragile than our initial assumptions incorporated in the computer modeling. So again, I don't know what modeling packages were used. I could have somebody follow up with Weidlinger and Lawrence Livermore, but those were quant jocks that do things way beyond my capacity. We were pretty happy with the results that they gave us.

MR. BECRAFT: I have a question. How do you see protection challenges and solutions changing in the future? Anyone?

MR. PACZKOWSKI: A lot of our focus across the country has been analogous to filling sandbags when the flood is coming. You just get out there and start doing things. There is a lot of focus on individual facilities. We have not focused nearly enough on facility and critical infrastructure interdependencies. I am encouraged that this situation is changing. We need to be looking not only at interdependencies in networked infrastructure,

but interdependencies in networked systems. We must address the reliance of one set of infrastructure on another set of infrastructure.

I am particularly concerned about the interdependencies issue relative to transportation in the New York area. There are secondary and tertiary impacts in certain scenarios that we have yet to even begin to contemplate. Right now, we are extending risk assessment into bringing back critical infrastructure after a major event like Hurricane Katrina. We are not only using risk assessment now to think about how to protect those facilities, but people are now beginning to think about how to use risk assessment before an event to consider the impact of response and recovery strategies and the best sequence to use in restoring infrastructures. There is major benefit to be derived from addressing interdependencies and networked infrastructure.

MR. ACHTERBERG: A significant challenge that we are seeing out West is the cost of security programs and its effect on our task of progressively addressing risk reduction throughout the agency inventory. I showed you some of our big facilities where it was fairly easy to make decisions to reduce risk. We continue to be challenged within our agency as we compete for security budget dollars with O&M. As the memory of 9/11 recedes, there will be significant challenges to maintain focus on what those risks are. To address this problem, I am reaching out more to other organizations. We are looking at the design basis that others are using to reduce risks and trying to benchmark my dam infrastructure with other critical infrastructure. I am looking to DHS to help me in this activity. That is one of the things I have been stressing in the DHS sector coordination process. It has been helpful in reaching out to industry to look at what are they protecting against at what levels. It is unfair for the dam sector to take on a level of protection beyond what others are addressing if the risks are commensurate. So my strategy is to leverage more of what others are doing. We are finding it easier to communicate between sectors now with regard to comparing strategies and progress.

MR. GAGNON: I am seeing a lot of progress with state and local organizations working in concert with the federal level. People are taking a more consequence-based view. Previously, under the national criteria, a chemical plant and a nuclear plant would carry almost the same weight in terms of protection priority. The approach has improved to consider regional-level consequences leading to a much more realistic set of priorities. People are assessing the cascading effects of losing the water treatment plant, the bridge, or the chemical site, for example. A lot of work is being done to explore the consequences of infrastructure loss both downstream and upstream. There is also increased attention to the recovery process – what is involved in bringing the infrastructure back.

PARTICIPANT: My name is Bradley Provancha. I am the Acting Director of the Defense Facilities Directorate, Washington Headquarters Services in the Pentagon. I have a couple of questions and a couple of comments. We serve about 60,000 folks in the National Capital region, DoD personnel at the Pentagon, as well as in about 120 leased buildings. I was very impressed with some of the risk assessment models presented today. One that I am familiar with was used a few years ago at the National Institutes of Health. The model incorporated the types of threats, both natural and manmade, the likelihood of them occurring, the projected extent of damage and then the degree of preparedness and mitigation required. The model allowed us to prioritize based on the most realistic threats that would have the greatest damage for which we were the least prepared. In resource constrained environments, based on experience, I think that such models are quite useful. The model came from Susan McLaughlin, who runs a company by that name.

I want to highly recommend subject matter experts in the area of protecting digital control systems. Scott Schwartz is fairly widely published in the literature. He is with the Department of the Navy at the Navy Surface Warfare Center in Dahlgren. We have used him in some of the activities at the Pentagon. We are about to undergo a DTRA BSA and a second round of follow-up exercises. Another expert is Dr. Tom Slaussen. Dr. Slaussen is with the Corps of Engineers Research Lab at Vicksburg. His area of expertise is ballistic material testing. His concepts have been battle tested in both Iraq and Afghanistan. The ballistic materials are well-suited for mobile systems – easily moved, installed, and demounted.

One of the consultants that we have used at the Pentagon, in addition to Weidlinger and others, is a group called Rogers Marvel based in New York. They have recommended some protection technologies for our consideration. I wondered if the panel has had any experience with the technologies that they are recommending, including the collapsible concrete systems as well as the turntables with the built-in bollards that are based on the old technology of turning train engines around. These can be used for vehicles of various types. Have the panelists had any experience with these technologies?

MR. PACZKOWSKI: Some of the collapsible concrete technology has its origins in airport runway overrun

aprons. We have had a lot of experience with that technology relative to stopping aircraft in relatively short distances. We have actually considered that around our airport perimeters as an access denial strategy but we have not employed it yet.

PARTICIPANT: Marvel has it in place at two locations in New York.

MR. PACZKOWSKI: The collapsible concrete technology works.

MR. BECRAFT: Thank you for your question and advice. Are there any other questions? We're out of time. I need to thank you in the audience for hanging in there. There is always a decline in the numbers in the afternoon, and we still have another keynote address, so I'm sure George would like us all to stay for the duration. And could we have another round of applause, please, for this panel.

DR. BAKER: We are coming down the home stretch. It is my pleasure this afternoon to introduce our final keynote speaker, John Stevens. He is the Deputy Director of the Centers for Disease Control and Disease Prevention for Security and Emergency Preparedness. He also serves as Special Agent in Charge of Counter Intelligence and Counterterrorism at CDC. John has been in charge during a period of major security upgrades that CDC, which has made his job quite interesting. I should say just from my own experience of doing vulnerability assessment there, the CDC has made huge strides in upgrading their protection. We have a lot to learn from their experience. Prior to CDC, John has years of experience as an Indianapolis police officer and at the FBI. He supervised the Crisis Management Team with the Critical Incident Response Group at the FBI. He also was supervisor of the Atlantic Joint Terrorism Task Force. So please join me in welcoming John Stevens to the podium.

Afternoon Keynote Address

MR. JOHN R. STEVENS: Thank you, Dr. Baker. I also want to thank James Madison University and the Academies for having me here. Our director, Dr. Richard Besser was originally scheduled to speak but couldn't make it today due to the present demands of flu pandemic preparedness. He wanted me relay his apologies and to be sure to thank you for the invitation to speak. I am no stranger to D.C. I lived here while working for the FBI. In the FBI, if you rise up in rank, you are required to get your lobotomy at the D.C. headquarters. So I was here for two and a half years before returning to a field assignment.

I must apologize in advance. After 27 years in the government, as most of you govies understand, my vocabulary has become a bit acronymical. If I use a contraction that you don't understand, please raise your hands and I will decode the acronym or explain that I just made it up. There are many acronyms in the government, so please bear with me.

I have a little story that goes along with the acronym problem. George mentioned that one of my positions in the FBI was the coordinator of the Domestic Emergency Support Team. For those of you who may not know what that is, it is a team that is flown first to the location of a WMD incident. I had an office at Andrews Air Force Base. We do many different things. One day I was put in charge of a territorial incident that had occurred. It involved the Army, the Navy and the Marine Corps. They put the team together and the operational plan and asked me to execute the plans and run the command post. I agreed. We do this kind of operation all the time and we rehearse this type of scenario. I was in the Situation Room at the White House and supposedly in charge. Being in the FBI, you generally are not in charge of anyone other than FBI agents – especially not the military. However, that was my job as coordinator for the Domestic Emergency Support Team. There were so many acronyms floating around the room – things that sounded like jock, tick and tock. To prevent confusion, I informed the team that the next time I heard an acronym I would make the offender stand up. We went on to another issue. A fellow from the Air Force informed me that a certain task was going to be handled by "glick." I ordered him to stand up for his acronym violation and asked him to decode the "glick" word. He informed me that he was referring to Scott Glick from the Department of Justice who was sitting next to me.

What Dr. Baker said is true. Over the last decade we have totally revamped the security at CDC. Before the attacks on 9/11, CDC headquarters was more like a university campus – maybe not a campus of today, but a campus prior to 9/11. It was an open and inviting environment. People came and went with no constraints.

Many of you know about CDC and its mission. We have and study almost every select agent there is. The term "selected agent" refers to dangerous agents – tularemia, smallpox, plague. These are substances that need to be carefully contained, that professionals need to handle, and we don't want a bad guy getting them.

After 9/11 the security structure went sky high. The anthrax attacks were of particular concern to CDC and

Fort Detrick. Fort Detrick is one of the other bio labs in the country that store and use level-four bio agents – the most dangerous agents.

The day after I became the supervisor of the FBI Joint Terrorism Task Force, I had 1,500 biological bags stacked up outside my office. Three women in the office were pregnant. They wanted the bags removed, threatening to sue the FBI and walk off the job. This was right after we discovered the anthrax during the 9/11 period through the work of Mr. Stevens out of Florida.

In determining how to respond, I called the WMDO, Weapons of Mass Destruction Division, at headquarters. They advised me to work with the CDC. We had 1,500 leads a day coming in on the 9/11 anthrax case. The Atlanta Division handled all of them, because we had just finished the Olympic Park bomb follow-up and we had all the necessary infrastructure set up. I called the CDC and spoke with the Director of the CDC on behalf of the Director of the FBI. We determined that the best course of action was to get the State involved.

We called the State authorities and within about five hours we came up with a national protocol for handling biological evidence. It is still the protocol that is used today. It is a very simple approach that I don't have time to explain. The point I want to make is that we never really worked together with the CDC. When we investigated the anthrax attacks we were at loggerheads with the CDC because of the different approaches used between the epidemiological investigation and the criminal investigation which were occurring in parallel. The problem was that, during this type of investigation, interviewing someone twice by two different agencies will nullify the evidence obtained. So we came up with a cooperative arrangement that involved a forensic epidemiology approach.

At the CDC we have 15 different field locations with 85 different facilities in Atlanta alone. I am responsible for the security of the national stockpile, which is distributed at various locations around the country. We have select agents in three different locations around the country. As of today, we have distributed 25 percent of our pandemic-related resources to the States. This is mainly Tamiflu.

We practice transporting agents over and over again – there are many security implications. We are operating from locations that are basically hidden in plain sight. And we are transporting materials that, if they are needed, may involve panic scenarios - crisis in the street. Such situations are very challenging from a security standpoint.

The original security department at the CDC headquarters in Atlanta included about three people. We had unarmed guards who basically controlled parking – and that was about it. We spent a lot of money to fix this.

Many of you probably know that the Patriot Act changed security requirements. For example, if you have a select agent in your facility – it doesn't matter if it is a university or a bio level-four laboratory – there are certain standards that apply. The CDC both regulates these standards – and, of course, uses them as well.

In the post 9/11 world, the government started assessing its vulnerabilities and needs as well as appropriating and transferring funds for security improvement. The government also began to establish security and emergency management mandates. The needs assessment showed that we needed a comprehensive security approach, security awareness training with emphasis on our employees, upgraded force protection, improved access controls, personnel screening and an emergency preparedness program.

We also needed an intelligence analyst program. Based on my FBI background, when I was assigned and transferred to the CDC, I saw a clear need to develop intelligence as part of our security profile. We were able to fuse security intelligence with the medical intelligence program.

We also needed law enforcement liaison – real police, basically. Options include armed guards, special agents of the FBI, or other folks who are involved in personnel security or intelligence operations. But if something happens, real police are needed to lock up the offender. My office provides the physical security liaison with local, state and federal police.

We needed classified programs and controls. There is a lot of information related to materials and threats that must be protected. We built a SCIF, a special compartmentalized information facility capable of handling information up to the SCI [special compartmentalized information] level. CDC routinely handles top secret information and we have classified network access up to the secret level. We manage all of our secure operations, which include the SCIF operation and maintenance.

The classified information handling capability is also important because without it, some countries won't share information with us. Obviously they don't want to be embarrassed. SARS is a case in point.

This is our vision. In harmony with what you've heard from earlier panelists, achieving this vision will require a multifaceted approach. We need to structure our security programs so that they work together within and among our many institutions. The following slides will give you an example of what I mean by overlapping security at our major institutions.

I know that the folks here involved in security at institutions of higher learning have experienced strong resistance to security. Academics are open-armed about their research – they want to help people. They don't want to be closed in or gapped in because security restricts open sharing of some information. A big challenge for us was to overcome this inherent resistance.

We started screening every employee that entered the fence. We inspected everything they brought in. The complaints continued for months. After three years, we noticed that the Pentagon and the State Department dropped their employee screening process. Employees with the appropriate security ID were allowed access without screening. So we followed suit and amazingly, for the following three months we heard nothing but complaints. People asked "Why aren't you checking us? What about this person down the hall?" So the point is, with time, our employees dropped their resistance to strict screening to the point where they were concerned when we stopped the practice. In response to employee concerns we implemented a random check process which turns out to be an acceptable compromise. Every now and then when we pull someone's car off to the side we'll find a weapon that the driver "forgot was there."

We take personnel security very seriously. When a person is hired to work at CDC, as a U.S. government employee, we conduct a prescribed background check. These checks are not as comprehensive as a Top Secret Clearance; rather their purpose is to determine if you are generally fit for duty. We look at credit history, arrest record, felony background and other factors. This is done out of my office. We have the complete system with about 20 employees involved in background checks. The select agent program is also handled within my office. We worked with the Department of Justice to help develop the special background check for our select agents. DOJ performs these checks.

Universities have been affected by the Patriot Act. At the time that Patriot Act was passed, there were about 1,500 universities with select agents doing research for CDC. In the wake of the Patriot Act this number dwindled to 325. This number is now headed back upwards to its previous level.

The Clifton campus at the CDC has gone through millions of dollars of security renovations. Dr. Baker was involved in the early assessments that resulted in these changes. We have added popup bollards and wedges. We have positioned armed security guards at the gates. The gate system provides two layers of physical security. We work in cooperation with the local DeKalb Police. We contract with off-duty police officers and have found their presence to be invaluable.

We have a countermeasure program that involves working with the local police to identify businesses around our properties. We make contacts with the businesses and arrange casual meetings (that may include dinner) to what goes on at our facility. In most cases, through these contacts, we are able to identify "trusted agents." We get calls, probably every other month, from a nearby business, informing us of strange behavior or potentially threatening activity. As an example, a nearby hotel manager called to report a guest who asked for a room that overlooked the CDC. In this case, our investigation determined there was no threat presented. But we greatly appreciate the trusted agent relationships and view these as an important part of our countermeasure program.

As part of our COOP program we have outfitted two vehicles for top secret information retrieval and real -time information communication through satellite. We manage and maintain the COOP vehicles. If a situation requires execution of our COOP plans, it will be important to continue to operate the CDC as a national government asset. An important task is to move the Director to a safe location and enable him to maintain communication. We have two separate COOP facilities and five different laboratories that we can use for COOP activities. Plans are in place to use these facilities for continuing the business operations of the CDC. There are north and south locations to circumvent problems associated with varying plume vectors.

Our organization was established on May 7th, 2002. I transferred to the CDC in August of that year. We consolidated the necessary personnel and functions. We basically drew in a big lasso and pulled related assets and personnel as we established a security office. Our organization included personnel, security functions, emergency planning functions, the select agent program from the CDC's Office of Health and Safety, and the stockpile security functions from the Strategic National Stockpile Division. One of the things that saved me was that I was able to recruit Phil Joyner, a 32-year veteran of the DeKalb police department. He was the Assistant Chief of Police, and very capable. He is respected by the

community, familiar with the general area, and gets things done in a way I could never get done.

Another major asset is Tammy Hammady who serves as our Chief of Intelligence and Communications Security. She had 18 years of experience as an FBI intelligence analyst. I have worked with hundreds of analysts and must admit that she is the best analyst I've encountered. I've also been very grateful to recruit a career Army officer who had worked in the field of personnel suitability and select agent compliance for six or seven years. Our emergency management team includes a Presidential management intern.

Managing our contract guard force is not easy. Our budget for contract guards is $20.5 million a year. Government procurement does not simplify this task.

Everybody who comes into our facility must have an ID, unless they are escorted as a visitor. We have 7,000 visitors a month. So you can imagine the issue with this operation. I don't know how many people here have been involved with Homeland Security Presidential Directive 12 also known as HSPD 12. Now everyone in the government will have the same ID implanted with their bio and clearance information. It has been very difficult for CDC to switch from our own card key access program into the HSPD 12 program – a veritable nightmare. As an example, at one of our facilities we have 2500 readers that will not read the new cards. We will end up having to replace all of these readers. You can imagine the cost and complexity involved.

Our physical security office also conducts assessments of our facilities. From time to time we also request other agencies do independent security assessments at our locations. The information from these assessments is very helpful. We use the results when we make requests to GSA, OPM and other regulatory agencies for addition security personnel and infrastructure protection. We have uniformed and plain-clothes security personnel. They are all highly trained. Training emphasizes the importance of customer service first. Training also addresses officer safety and how to identify and resolve security issues.

Our physical security department is responsible for all the operations which they coordinate through our operations center. The center is reminiscent of James Bond. We have 1500 cameras at the Clifton location alone. Due to the Patriot Act and its definition of the select agent, we are required to have a camera on every freezer, a biometric reader, and also a card reader. A scientist that needs to get select agent out of a freezer can't just remove the uranium. They must access the freezer through the security mechanism. Operation of the security devices requires that the scientist's name is in the system associated with their particular grant and select agent.

My office processes requests for 7,000 visitors a month. Foreign nationals must submit their requests ten days in advance to give us time to check their visas. This process has caused us much difficulty. We don't allow visitors with diplomatic immune passports.

Another challenge is security for the many leased spaces that we are responsible for. We are involved in planning meetings for new buildings from day one. One of the design features we have been able to influence is the use of collapsible posts. In the event of a detonation, this feature allows for a natural collapse of the building rather than all the floors collapsing. Our presence in the planning process for new buildings from the onset is important due to the tendency to design without considering security. Security is one of the first features to be reduced in the face of limited resources. Actually, designing in security from the beginning reduces the cost of security. If the wire installation necessary for security networks is not included in initial design and construction, it is be very expensive to retrofit.

Our personnel security operation performs the employment suitability investigations that I talked about. This involves approximately 6,000 investigations each year. On average about 1600 of these investigations lead to issues that require additional processing. As an example, we will investigate cases where an applicant claims to have a degree that can't be corroborated with the issuing institution. This is a very serious issue at CDC. We also coordinate the drugfree certification program including random testing of employees. Our investigations include compliance in the select agent program. We obtain the information necessary for the investigations of all the people who will have access to the select agents. We also conduct the bi-annual inspections prescribed by select agent program regulations. These cover bio-security, bio-safety, emergency response and chemical hygiene.

Our intelligence group provides intelligence support, including the threat analysis, to the CDC Director and the coordinating directors. We meet with the Director every week and talk about the threat analysis around the world as far based on the latest medical intelligence. We conduct mandatory security briefings for our cleared employees who are traveling to other countries. We provide a mandatory State Department out briefing, and then we debrief them when they return. We provide liaison

to external entities and supplement activities including DoD, FBI, CIA, NSA and the Department of Homeland Security. One important point I want to make relative to CDC is that most of the intelligence, threat analysis, risk analysis and security operations that we do – even after our facilities are secured and hardened through this layered approach – comes back to the trusted employee.

We schedule frequent meetings with groups of individuals who may work in very sensitive areas, such as smallpox. We meet with this group together and as individuals. We'll ask them about their concerns, their work, their thoughts on their environment and contacts, and if they've received any unusual threats or offers. We develop guidance on what to do if they are threatened or extorted to provide select agents or classified material. We have developed code words and response procedures in place in conjunction with the FBI as well as the local police for such contingencies. We also manage all of our classified document storage.

We are responsible for emergency management of the CDC. This includes our COOP operations and internal crises. An internal crisis could be a terrorist with an automatic weapon, a suicidal employee or a fire. We have developed an IEMP, which is the integrated emergency management plan. We also are coordinating with the new National Emergency Management System and whatever will come up next year out of the national emergency response groups.

In the short time remaining, I'll highlight some of the improvements we are working for the future. These fall into the categories of better training for guards, enhanced perimeter control, X-ray magnetometers, embedded security in building and campus design, improved card key access, and the use of biometrics.

We have a short time available for questions. If you need further information after today, please call me. Thanks for your attention.

PARTICIPANT: Ben Delp, James Madison University. My gym in Harrisonburg, Virginia, which is also a community center, uses a fingerprint scan for access. That seems to be a bit more common these days. You mentioned biometrics and also fingerprint security. Can you go elaborate on your experience with biometric technologies, including iris or retina scanning?

MR. STEVENS: We include iris scanning in addition to the fingerprint scan. Employees entering restricted spaces have card key access but are also required to use a fingerprint and iris scan. These procedures allow for positive identification before allowing access through particular doorways.

PARTICIPANT: I am Carroll Highsmith, with D.C. WASA Security. Would you go into more detail about how you deal with foreign nationals who want to visit your facility?

MR. STEVENS: We have a standing policy. The most important thing is to have a well-defined policy approved at the executive level. We require the visit request information ten days in advance. We provide the information to the FBI and the State Department who then run background checks. Although they don't give us a yes or no, they do advise us about any concerns they have. If they have no concerns, then we allow them visitor access. We generally restrict foreign visitor access from certain areas.

Symposium Recap

DR. BAKER: We've heard many talks today and now want to recap – to look for major themes in what has been presented over the course of the symposium. We are very pleased to have Doug Hall from the Federal Facilities Council and Dutch Thomas from the Institute for Infrastructure and Information Assurance to provide their summary of today's proceedings. Some brief introductions are in order.

Doug Hall is the Associate Director of Protective Services at the Smithsonian. He is responsible for the Smithsonian's physical security, antiterrorism and risk management programs. Doug oversees the design, construction and maintenance of physical security elements for the Smithsonian at all their locations worldwide. He chairs the Federal Facilities Council's Steering Committee on Physical Security and Hazard Mitigation.

Dutch Thomas has 26 years of professional management experience in security and emergency management. He guided the National Guard Readiness Center in developing their emergency preparedness program. The program he designed has become the prototype for the National Guard's nationwide effort. During his military service, he coordinated DoD support to civil authorities for all declared disasters, and was Chief of Military Support to the National Guard while at the National Guard Bureau. As a very fitting capstone to his career, while at FEMA, he was James Lee Witt's liaison with the Department of Defense.

So Doug and Dutch thanks and now, over to you.

MR. DUTCH THOMAS: Thank you, George. Where is our Super Bowl man? I am a Kansas City Chiefs fan and the only bowl that my team knows about has cereal in it. I grieve. You brought all that to my mind with your presentation. Doug, will you lead off?

MR. DOUG HALL: You bet, Dutch. First, George, I expected either to speak an hour ago or an hour from now. You've done an excellent job in facilitation and time keeping. It is a very, very difficult job, and I really appreciate it.

One thing Dutch and I realized as we got together earlier to talk about this wrap-up is that there has been a tremendous amount of information presented on many different topics from highly qualified experts. Although we don't have time to cover each talk, there are some central themes that we want to begin with here I think were important. We also want to get opinions and comments from you, the audience, about items you believe to be important take-aways.

One subject that jumped out from every presentation was the concept of risk assessment and risk management. In some cases the speaker covered risk in an overt manner – for instance the Port Authority expert in presenting his very sophisticated assessment and management process. Other presentations that may not have addressed risk assessment and management in an overt fashion pointed to the importance of these disciplines. In each case, risk factors including the threats, the consequences, the vulnerabilities and the management of risk were clearly important. What are your thoughts on themes, Dutch?

MR. THOMAS: Two short imperatives: "Don't be afraid" and "be ready." During the discussion of the New York Port Authority, I was reminded of the disabled aircraft landing without warning in the harbor. The rescue was conducted by boat operators in accordance with lessons they had learned in a well-exercised plan, if I am not mistaken. A Coast Guard captain found that his familiarity with the exercise and plan made all the difference in executing the rescue in a calm and effective manner. Coordination among local, state, and federal authorities and the interface between the private and the public sectors were required during the operation. We were all amazed at Captain Sully's grace and skill in his water landing with no one even seriously injured. They were rescued as a result because of a well-exercised plan. "Don't be afraid – be ready."

MR. HALL: The challenge associated with threat definition was a theme today as an important part of the risk assessment process. It is clear from the talks today that the identification and analysis of threats are difficult tasks. Austin Smith addressed the problems they have encountered and Bob Smilowitz emphasized the importance of developing a design-basis threat. Which threats to include in the design basis and how to deal with threats that may be impractical from a protection standpoint came through as major issues. The message is the importance of identifying all potential threats. We must avoid the temptation to bury our head in the sand, vis-à-vis the more difficult threats.

An important part of risk assessment is determining the consequences of specific threats. We saw a number of different approaches to determining these consequences. Bob Smilowitz discussed vulnerability assessment tools that they are using and their modeling capabilities used to quantify consequences.

Today, we were exposed to a wide variety of approaches to risk assessment culminating in Susan Armstrong's presentation on the approach DHS uses to categorize risk relating that specifically to chemical facilities.

MR. THOMAS: Institutions take steps to mitigate risk and risk consequences, but what responsibility does the individual have? That has been a theme implied in many of today's presentations. Individuals have an implied responsibility.

The potential threat to civil liberties was also an important theme. Federal-level programs need to balance security and civil liberties. When we talk about such things as the Patriot Act, there must be a balance. It is inherent in our system of governance. We must keep in mind that as we prepare for the asymmetrical terrorist threat, we must define it. Is it a terrorist, a criminal act, or an act of war? What is it? How do we adjudicate it? At the same time we must protect the individual liberties that make this nation unique and strong and our democracy viable. This goes back to the Domenici legislation.

Maintaining the national security and maintaining civil liberties as coequal objectives came through as a key point.

MR. HALL: On the same point, Dr. Steger emphasized the importance of balancing risk reduction and the impacts on our individual rights including privacy, the public right of way and other factors. This is an aspect of risk management that has major implications. It is similar to cost-benefit analysis although the cost is not easily quantified. It is not enough to determine the most protection that can be achieved based on dollar cost alone. Dr. Steger and others emphasized that there are liberty-related aspects

of cost to be considered in how we manage risk. It is also important to recognize that the cost criteria will vary by institution and agency.

MR. THOMAS: It is important we define threats as best we can. This is not easy. It has been difficult to be able to articulate the threats from asymmetrical terrorism, aging infrastructure, and climate change. There are other threats that are more easily quantified such as fire, weather, and seismic related events. In this regard, the all-hazards approach makes sense. I commend the categorization of threats presented today in terms physical, cyber, people, and security. This is key.

The cyber threat category scares me. It scares a lot of people, because it affects systems we use on a daily basis but we don't fully understand. What is inside a computer is a mystery to most people. If our computers and networks fail, who fixes it? How do we re-establish the services that are computerized? How do we re-establish that system? Although the systems are a mystery to most of us, we must pay attention. Richard Clark, as our past cyber security czar, provided great service in explaining the dimensions of this threat. The cyber panel was an important part of today's agenda in helping us understand the threat, the enormous potential consequences and the latest countermeasures including security procedures and software.

MR. HALL: I also wanted to comment on the all-hazards approach that Dutch mentioned. There are some important cost-benefit issues here related to risk management.

Earlier, Rich Little alluded to the problem of determining how much investment is appropriate for facility protection. Are we spending enough? Are we spending too much? How can we analyze this? One of the lessons that was apparent from the DTRA experience which Bill Austin related, is that their assessments don't consider specific threats. Rather they look at single points of vulnerability and realizing that these points are vulnerable to multiple hazards. This is an important lesson on how to approach risk from a balanced standpoint. This approach was mentioned by several different speakers looking at very different types of facilities and locations.

It is important to spread our limited dollars as far as possible – to maximize the return on our investment. If we can identify fixes that protect against multiple hazards that engender the same consequences, this greatly helps us stretch our dollar.

MR. THOMAS: I was pleased to see risk acceptance as a common issue today. Because of the IRA threat, the City of London removed trash cans from their public transit stations. However, prior to 9/11, they had not installed metal-detecting magnetometers in their public places. If you visited the Tower of London, you were not frisked or scanned by a magnetometer. My point is, they had accepted a level of risk. At that time, they were willing to accept the risk of a criminal or terrorist explosives attack.

If you read our National Response Plan on page 25, you will find the only mention of accepting a level of risk. But many of our speakers today, much to their credit, talked about the need for establishing a level of risk acceptance. People living in Tornado Alley accept a certain level of risk in order to remain there. People that live next to the seismic zone down by New Madrid have accepted a level of risk from an earthquake. We need to articulate and incorporate this principle in our assessments.

MR. HALL: An excellent point that relates to the final step in the risk management process. Austin Smith's presentation on new federal criteria piqued my interest. Formalizing the risk acceptance process for federal facilities using the IFC criteria represents a major milestone. Whether we realize it or not, as individuals, we are constantly assessing risk. People in Tornado Alley are doing it. But they are not doing it in any formal way.

Unfortunately, the same applies to many of us responsible for major facilities… we don't do risk management in any formal way. We don't have enough money. Often, we back into risk acceptance without putting it down on a piece of paper. Unfortunately, if something bad happens, there is a price to pay. So I am very interested as we go forward and as the IFC goes forward, how the process will be formalized within the federal world. I am also quite interested in whether and how the commercial world will formalize their approach.

Just to finish my risk soapbox message here – we are seeing a lot of risk-based criteria and countermeasures standards coming out. It is difficult to implement standards in the security world. Standards work best if the risk is the same from place to place. We all know that is not the case. To address this issue, DHS is identifying some regulatory measures that are risk-based. The new IFC criteria we heard about today are risk-based. As we develop solutions, we must keep this in mind.

In conclusion, the spirit of risk management was the central theme running through today's agenda whether overtly or inadvertently.

MR. THOMAS: Thank you, Doug. Security is multifaceted and must address resilience. We can't stop all of the events, all of the potential threats. Hurricanes will hit, earthquakes will happen, and Mt. St. Helens could erupt again. In the face of these threats, we need to be prepared – we need to be resilient. We have to be able to cope with the consequences and get on with our life and the life of our communities. We are a tough people. We can do it.

My final point is that disasters are local. They begin and end at the local level.

MR. HALL: Thank you. I'd like now to turn to the audience. Are there any other comments or big ideas that need to be captured?

PARTICIPANT: One key principle worth mentioning is the importance of education. Any successful security plan must incorporate education, whether it relates to physical protection or cyber protection. It is important to make sure that your employees understand that they can't put critical information on their computers. They should use encrypted thumb drives for very sensitive information. People at the local level need to understand the importance of informing citizens about precautionary measures such as storing supplies or sealing windows. Education is key to effective security.

MR. THOMAS: If I may reinforce your point, who lives at the local level? People. It all begins and ends with people, not systems, not machines, but people, human beings.

MR. HALL: Thank you.

DR. BAKER: On behalf of the Federal Facilities Council of the National Academies of Science and the Institute for Infrastructure and Information Assurance of James Madison University, I want to thank everyone involved in making today's symposium a success. Special thanks to our panel moderators, our panelists and you in the audience for your presence, questions and comments. I saw a tremendous amount of interaction. It has been a very productive day.

Now I would like to close, and hope that you will find that what happened today will be useful in your endeavors to protect our large facilities and facility complexes. Thank you very much.

Dr. Charles W. Steger
President, Virginia Tech

On January 7, 2000, **Dr. Charles W. Steger** became Virginia Tech's 15th President. Dr. Steger's ties to Virginia Tech span four decades. He has been student, teaching faculty, academic department head, college dean, vice president, and now president. While a faculty member, he won two teaching excellence awards. He authored a portion of a textbook that has been adopted by 230 universities and is now in its 7th edition. When he became dean of the College of Architecture and Urban Studies (CAUS) in 1981, he was the youngest dean of any college of architecture in America. For his contributions to the profession in the field of architectural education and research, he was inducted into the College of Fellows of the American Institute of Architects (AIA) in 1990, and received the Distinguished Achievement Award of the Virginia Society of AIA in 1996.

Dr. Steger has played an active role in shaping the future of the university. He chaired the Committee on Strategic Planning, which developed the institution's process for strategic planning, and was a member of the committee which developed the first core curriculum for Virginia Tech in 1981. In 1989, he chaired the University Committee on the Impact of Digital Technologies on the Teaching-Learning Environment. This report was highly regarded by the State Council of Higher Education for Virginia (SCHEV) and described by the past president of EDUCOM as a seminal work in the field that underpins many instructional technology efforts.

In Dr. Steger's previous position as Vice President for Development and University Relations, he directed the university's successful campaign, which raised $337.4 million, exceeding the $250 million goal by 35 percent. It was the most successful fundraising effort in the university's history. Over 71,000 donors and 500 volunteers participated in this six-year nationwide effort led by Dr. Steger.

Dr. Steger has been appointed by two governors of Virginia to serve on various study commissions and work groups. The most recent was the Governor's Commission on Population Growth and Development, where he served on the executive committee of the Commission. He also was a member of the Board of Trustees of Hollins University. In addition, he currently serves as president of the Endowment Foundation for the Western Virginia Foundation for the Arts and Sciences (known as Center in the Square) in Roanoke. Dr. Steger also is a director on the Boswil Foundation in Zurich, Switzerland. He received the Outstanding Fund Raising Executive Award given by the First Virginia Chapter of the National Society of Fund Raising Executives at its 1999 National Philanthropy Day Awards Dinner.

Most recently, he has been asked by the Swiss Ambassador to the United States and The World Bank to serve on a committee to establish a foundation in the United States to conduct research on mitigating global natural disasters.

Symposium Introductions

Dr. John B. Noftsinger, Jr., Vice Provost for Research and Public Service, James Madison University, and Executive Director, IIIA

Dr. Noftsinger serves as Vice Provost for Research and Public Service, Executive Director of the Institute for Infrastructure and Information Assurance, and Professor of Integrated Science and Technology and Education at James Madison University. He has primary responsibility for facilitating external grant and contract funding, homeland security research programs, economic development, technology transfer, and academic public relations and service programs for JMU. He has led the development of an innovative bachelor's program in Information Analysis at JMU and is actively engaged in developing economic acceleration policy and programs within the mid-Atlantic region through the Accelerating Innovation Foundation, Virginia Technology Alliance, and the Shenandoah Valley Technology Council, all of which he co-founded. He is a founding member of the Executive Committee of the Virginia Institute for

Mr. John R. Stevens, Jr.
Deputy Director
Centers For Disease Control and Prevention
Office Of Security and Emergency Preparedness (OSEP)

Mr. Stevens became the Deputy Director and Special Agent in Charge of Counterintelligence-Counterterrorism of CDC's Office of Security and Emergency Preparedness in August 2002. Following the September 11, 2001 terrorist attacks, CDC expanded OSEP's responsibilities from mostly physical security to developing, implementing, and managing a comprehensive security program—personnel suitability and select agent compliance, medical and public health intelligence, communications security, physical security, and emergency management—at CDC facilities throughout the country. John was hired to engineer and oversee much of the new program.

Prior to working with CDC, John spent more than 20 years in law enforcement, including 5 years as an officer with the Indianapolis Police Department, and 15 with the Federal Bureau of Investigation.

During his time with the FBI, John served in a number of critical positions. Most notably, he was a supervisor in the Critical Incident Response Group, Crisis Management Unit; coordinator of the US Domestic Emergency Support Team; and supervisor of the Atlanta Joint Terrorism Task Force.

John has also assisted at several Olympic games where he served as the case agent for counterterrorism planning for the 1996 Olympic Games in Atlanta; Identification Team supervisor for the Olympic Games in Salt Lake City; and Olympic security representative in Barcelona, Lillehammer, and Nagano.

John graduated from Indiana State University in 1980 earning a Bachelor of Science Degree in Criminology. He continued his education and earned a Master of Science Degree in Criminology in 1982.

Defense and Homeland Security and Deputy Chairman of the University of Virginia's Critical Incident Analysis Group (CIAG) Steering Committee. Dr. Noftsinger is also a member of the Critical Infrastructure Roundtable at the National Academy of Sciences. He serves as a Senior Fellow at the George Washington University Homeland Security Policy Institute (HSPI). In 2002, Dr. Noftsinger's statewide leadership was recognized when he was appointed by Governor Mark R. Warner, and reappointed by Governor Tim Kaine, as co-chair of the Virginia Research and Technology Advisory Commission (VRTAC), which advises the Governor and General Assembly of Virginia on appropriate research and technology strategies. He was also appointed by Governor L. Douglas Wilder as Deputy Secretary of Education for the Commonwealth from 1993-1994. He holds a Bachelor of Science in political science and public administration from James Madison University, a Master's of Arts in higher education administration and student affairs from The Ohio State University, and a Doctorate in higher education administration from the University of Virginia.

Ms. Lynda Stanley, Director of the Board on Infrastructure and the Constructed Environment (BICE) of the National Research Council (NRC), National Academy of Sciences

Ms. Stanley has been the Director of the Board on Infrastructure and the Constructed Environment (BICE) of the National Research Council (NRC) since 2005. The NRC is the operating organization of the National Academies of

Sciences and Engineering and the Institute of Medicine. The BICE addresses questions of technology, science, and public policy applied to the relationship between the constructed and natural environments and their interaction with human activities. Ms. Stanley served as the Director of the Federal Facilities Council (FFC) of the NRC from 1995-2005. The FFC is a cooperative association of 27 federal agencies whose mission is to identify and advance technologies, practices, and policy for the improvement of federal facilities from planning through disposal.

At the NRC, Ms. Stanley has served as the study director on a series of reports on federal facilities-related issues. These include Stewardship of Federal Facilities: A Proactive Strategy for Protecting the Nation's Public Assets; Outsourcing Management Functions for the Acquisition of Federal Facilities; Investments in Federal Facilities: Asset Management Strategies for the 21st Century; Core Competencies for Federal Facilities Asset Management Through 2020: Transformational Strategies. She has also been involved with the NRC studies on the New Orleans Regional Hurricane Protection Projects, Assessment of the Bureau of Reclamation's Physical Security Program, and Assessment of the Results of External Independent Reviews for U.S. Department of Energy Projects.

Prior to joining the NRC, Ms. Stanley was the Director of the Planning Division in Fairfax County, Virginia. She holds a Bachelor of Arts in political science and American history from the State University of New York at Albany and a Masters in city and regional planning from Harvard University.

Panel One: Physical Protection Problems and Approaches

Moderator: Mr. Richard Little, Director, The Keston Institute for Public Finance & Infrastructure Policy, USC

Mr. Little is a Senior Fellow in the School of Policy Planning and Development and Director of the Keston Institute for Public Finance and Infrastructure Policy at the University of Southern California. Mr. Little teaches, consults, conducts research, and develops policy studies aimed at informing the discussion of infrastructure issues critical to California and the nation. Prior to joining USC, he was Director of the Board on Infrastructure and the Constructed Environment of the National Research Council (NRC) where he directed a program of studies in building and infrastructure research. He has conducted numerous studies dealing with life-cycle management and financing of infrastructure, project management, and hazard preparedness and mitigation and has lectured and published extensively on risk management and decision-making for critical infrastructure. Mr. Little has almost forty years experience in planning, management, and policy development relating to public facilities, including fifteen years with local government. He has been certified by examination by the American Institute of Certified Planners, is a member of the American Planning Association and the Society for Risk Analysis, and is Editor of the journal "Public Works Management and Policy." He holds a Bachelor of Science in Geology and an Masters of Science in Urban-Environmental Studies, both from Rensselaer Polytechnic Institute. Mr. Little was elected to the National Academy of Construction in 2008.

Mr. Bill Austin, Chief, Balanced Survivability Assessments Branch, Defense Threat Reduction Agency (DTRA)

Mr. Austin is the Chief, Balanced Survivability Assessments Branch, of the Defense Threat Reduction Agency, Fort Belvoir, VA. DTRA safeguards America and its allies from weapons of mass destruction (chemical, biological, radiological, nuclear and high yield explosives) by providing capabilities to reduce, eliminate and counter the threat and mitigate its effects. His branch is responsible for the conduct of detailed multi-disciplinary, performance–based survivability assessments of critical National mission systems and architectures. He holds a Bachelor's degree in general studies from Louisiana State University and Master's degrees in personnel counseling and guidance and in management from Troy State University. He joined federal government service after he retired from the United States Army. He is a graduate of the United States Army Command and

General Staff College and the United States Army War College.

Mr. Austin Smith, Executive Director of the Interagency Security Committee (ISC)

Mr. Smith is Executive Director of the Interagency Security Committee (ISC), a collaborative body focused on improving physical security and protection of federal civilian facilities. Chaired by the Assistant Secretary for Infrastructure Protection (IP), the Interagency Security Committee was created by Executive Order 12977 in 1995, following the bombing of the Alfred Murrah Federal Building in Oklahoma City. Its mandate is to assess physical security vulnerabilities, develop and publish security standards and best practices, and oversee implementation. The ISC plays a critical role in the Department of Homeland Security's (DHS) mission to protect the nation's critical infrastructure and key resources. As Executive Director, Mr. Smith works with the ISC Steering Committee to develop priorities, facilitates numerous Working Groups and publication of Standards, and oversees outreach and engagement with industry, senior federal officials, Congress, and the public.

Since he joined the ISC in August 2007, Mr. Smith directed the development of the new "Facilities Security Level Determinations of Federal Facilities" (March 2008) which specifies updated criteria for rating the security level of all federal buildings and serves as the foundation for implementing a broad range of countermeasures. Currently, Mr. Smith is leading development of "Physical Security for Federal Facilities," a comprehensive Standard, to be published later this year, which will specify countermeasures to be implemented at all civilian Federal facilities (government-owned, leased, to be constructed, modernized or purchased).

Mr. Smith served as an Associate at Booz Allen Hamilton, leading numerous strategic real property and facilities projects for federal clients including the Federal Bureau of Investigation, the Environmental Protection Agency, the Department of the Army, the General Services Administration, and the Department of Justice. He began his career in commercial real estate at the Costar Group.

Mr. Smith received his Bachelor's Degree in Government and Politics from the University of Maryland and completed additional study at Georgetown University and the Federal Law Enforcement Training Center.

Dr. Robert Smilowitz, Principal, Applied Sciences Division, Weidlinger Associates

Dr. Smilowitz is a Principal in the Applied Sciences Division of Weidlinger Associates and Adjunct Professor of Engineering at the Cooper Union. He received a Ph.D. from the University of Illinois at Champaign-Urbana. Dr. Smilowitz has over thirty-one years' experience participating in the protective design and vulnerability studies of numerous Federal Courthouses, Federal Office Buildings, Embassy Structures, airline terminals and commercial properties.

He has also analyzed the World Trade Center underground parking garage slabs in response to the 1993 bombing; analyzed the Khobar Towers, in Saudi Arabia, in response to a terrorist vehicle bomb attack; served as a member of the ASCE/FEMA World Trade Center Building Performance Study; and developed protective design retrofits of the Pentagon facade related to the aircraft impact of September 11, 2001. Dr. Smilowitz also has participated in the explosive testing of full-scale curtain-wall systems and is a principal developer of analysis software for evaluating curtain-wall response to an explosive terrorist threat. He is a GSA National Peer Professional, a National Associate of the National Academies, and a registered professional engineer in New York and California.

Panel Two: Cyber Protection Problems and Approaches

Moderator: Ms. Darlene Quackenbush, IT Planning/Information Security Officer, JMU

Ms. Quackenbush serves as James Madison University's Information Security Officer, where she is responsible for information technology planning and policy

development. In these roles she performs strategic planning, facilitates development of the university's information security program and administers technology policy formulation. At JMU and in the broader higher education community, she promotes information security education and risk management, contingency planning and strategic creativity in the use of technology. With over twenty-five years experience applying technology within public and higher education, Ms. Quackenbush has assisted a variety of successful initiatives and groups including the Virginia Alliance for Secure Computing and Networking (VASCAN) and the Association of Collegiate Computing Services (ACCS) of Virginia. She holds a Bachelor of Science degree in Education/ Business from Virginia Tech and a Master of Business Administration from James Madison University.

Mr. Wayne Martin, Information Systems Security Officer, University of Virginia Health System

Mr. Martin is the Information Systems Security Officer with the University of Virginia Health System. He has thirty-five years of experience in the healthcare industry, with twenty-one years in computer technology. His personal and professional research interests focus on strategic information systems planning, unified theory of acceptance and use of technology, and the potential of information technology in the healthcare industry. He is also interested in the relationship of organizational culture, relationships, and dynamics in creating agile and flexible information technology security processes and practices to align with and support business objectives. He earned his Master of Science in Computer Information Systems from the University of Phoenix.

Mr. Baird McNaught, U.S. Department of Homeland Security, Security Control System Program Manager, Idaho National Lab

Mr. McNaught has supported the DHS Control Systems Security Program since its inception in May of 2004. He has contributed to the development of many cyber security products, which the Program shares with the control systems community to promote the implementation of sound cyber security practices. Most notably, Mr. McNaught led the team which developed the initial version of the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). Recently, he led a Chemical Sector working group that drafted the Roadmap to Secure Control Systems in the Chemical Sector. Mr. McNaught currently supports the Control Systems Security Program in multiple areas of industry coordination and security awareness.

Dr. Joy Hughes, Chief Information Officer and Vice President for Information Technology, George Mason University

Dr. Hughes has been CIO and VPIT at George Mason University for twelve years. Computerworld named her one of the top 100 CIOs in the nation in 2008. Rider University named her to its Science Wall of Fame and she has been honored by the Information Security Executives Association, the March of Dimes and by Women in Technology. She was formerly the CIO at Oregon State University and SUNY-Potsdam. She chairs Microsoft's Higher Education Advisory Group. For three years she co-chaired the EDUCAUSE/ Internet 2 Computer and Network Security Task Force.

She is a member of the boards of two wireless television companies which provide specialized television services to the Washington D.C region and which have returned many millions of dollars to the university.

She earned her Ph.D. in information systems from the Union Institute, an MS in computer science

from the New Jersey Institute of Technology, and an Master of Science in mathematics from Rutgers University.

Panel Three: Facility Protection Case Studies

Moderator: Mr. Mike Becraft, Senior Vice President, Federal Civilian Services Group, Serco North America

Mr. Becraft is responsible for the Mission Services Group at Serco, where he leads two business units, the Homeland Security Division and the Mission Critical Outsourcing Division. With a combined strength of over 2,500 personnel, his Group provides direct support to customers that include the Department of Homeland Security, Department of State, Department of the Army, Department of the Navy, National Institutes of Health, and the Drug Enforcement Administration. Mr. Becraft joined SI International (acquired by Serco in 2008) as Senior Vice President of Homeland Security in July of 2003, after more than thirty-five years of federal civilian government and military service. Prior to joining SI International Mr. Becraft served for ten years in the United States Immigration and Naturalization Service (INS) starting first as an Expert Consultant in October 1993. In February 1995, he was appointed Chief of Staff of the INS as a member of the Career Senior Executive Service. On September 11, 2001, he was appointed Acting Deputy Commissioner. During his tenure the INS grew from 17,000 personnel with a budget of over $1B, to an organization of almost 38,000 men and women world wide and a budget of over $6B. He played a key role in fostering the development of the Entry/Exit System (now US VISIT), the Student and Exchange Visitor Information System (SEVIS), and the INS Enterprise Architecture Plan. Mr. Becraft worked closely with senior U.S. government officials and officials from numerous countries on critical immigration and security issues. One of his last major responsibilities was to manage the restructuring and transition of the agency from the Department of Justice into the new Department of Homeland Security. Mr. Becraft is the recipient of the Presidential Meritorious Rank Award for 2002.

Mr. Becraft also served a career in the United States Army. Commissioned as an Armor Officer in 1966, Mr. Becraft served two combat tours of duty in the Republic of South Vietnam, as well as in various command and staff assignments of increasing responsibility in the United States and in Europe. Before retiring from the Army as a Colonel in September 1993, he served as Chief of the Counternarcotics Operations Division, the Operations Directorate (J3) of the Joint Staff, the Pentagon. In this position, he was responsible for overseeing the daily management of military operations in support of the War on Drugs. Mr. Becraft is the recipient of several U.S. military awards for valor, achievement and service including the Silver Star Medal for gallantry in combat, two awards of the Bronze Star Medal with "V" Device for heroism in combat, the Defense Superior Service Medal, the Legion of Merit, the Purple Heart; and the Combat Infantryman's Badge.

His academic credentials include a Bachelor of Arts in Social Science from Niagara University, a Master of Arts in Political Science from Appalachian State University, and an Master of Business Administration from Marymount University. He is also a graduate of the United States Army Command and General Staff College at Fort Leavenworth, Kansas, and the National War College in Washington, DC.

Mr. David Achterberg, PE, Director, Office of Security, Safety and Law Enforcement, Bureau of Reclamation, U.S. Department of the Interior

Mr. Achterberg of the Bureau of Reclamation was appointed to the position of Director for Security, Safety, and Law Enforcement in August 2006, after having served as the Assistant Director since September 2003. This office is responsible for a variety of risk management programs throughout Reclamation which include Dam Safety, Building Seismic Safety, Security, Law Enforcement, Continuity of Operations, Emergency Operations, and Emergency Disaster Recovery.

Mr. Achterberg began working for Reclamation in 1975 performing construction inspection activities throughout eastern South Dakota during the

summers while attending college. He permanently joined Reclamation in 1980 where he performed dam spillway and outlet works design, and concrete dam design at the Engineering and Research Center in Denver, Colorado. His activities included dam safety analysis, dam safety modification designs, and designs for several new dams. In 1994, he became the Chief of the Dam Safety Office where he administered an annual program of $70 to $90 million and was responsible for monitoring, inspection, analysis, and dam safety rehabilitation for Reclamations 248 high and significant hazard facilities. Mr. Achterberg was appointed to be Reclamations Security Coordinator after September 11, 2001, where he was responsible for a variety of new security initiatives within Reclamation and with other major Federal dam owners and regulators.

Mr. Achterberg served as the Department of the Interior representative to the Interagency Committee on Dam Safety, (ICODS) from 1994 through 2002, and as the Chair for the ICODS Subcommittee on Research from 1997 through 2001. He is a member of Association of State Dam Safety Officials, (ASDSO), and United States Society on Dams, (USSD). He also served as the Vice-Chair for the Dam Safety Committee for USSD from 1997 through 2003 and as a Co-Chair for the National Dam Safety Program Security Task Force.

Mr. Achterberg currently serves as a Department of the Interior representative on the Dams Government Coordinating Council which is led by the Department of Homeland Security. In these positions, Mr. Achterberg has kept Reclamation in a leadership role on dam safety and security within the Federal government and the dam industry.

Mr. Achterberg is a registered professional engineer in the state of Colorado and holds a Bachelor of Science degree in Civil Engineering from Colorado State University where he also attended graduate school and studied river mechanics, sediment transport, water quality, and dam design.

Mr. Ollie Gagnon, Protective Security Advisor, Central Florida District, U.S. Department of Homeland Security

Mr. Gagnon was appointed by the Department of Homeland Security as a Protective Security Advisor on March 21, 2005. In this capacity, he assists state and local efforts to protect critical assets and provide a local perspective to the national risk picture. Prior to assuming his present position, Mr. Gagnon traveled worldwide on behalf of the Department of Defense's Defense Threat Reduction Agency conducting comprehensive physical security assessments of critical infrastructure complexes, facilities and systems. He also served in the United States Air Force for twenty-two years in the various physical security, law enforcement and training positions. In his final military assignment, Mr. Gagnon exercised security decision-making authority affecting the protection of the President of the United States as the Chief, Presidential Aircraft Security. In this position, he personally directed security aboard Air Force One during 200 trips transiting all 50 states and 65 countries in support of President William J. Clinton and President George W. Bush.

Mr. John Paczkowski, Distinguished Fellow, Naval Post Graduate School at the U.S. Department of Homeland Security; Director, Emergency Management and Security, Port Authority of New York and New Jersey

Mr. Paczkowski has worked for the Port Authority of New York and New Jersey since 1978, holding a variety of executive level positions in planning, policy and operations. In December of 2001, he was appointed director of emergency management and security, where he is responsible for oversight of agency-wide critical infrastructure protection and emergency readiness programs for the Authority's aviation, transit, tunnel and bridge, and maritime cargo facilities. On September 11, 2001, he was the Authority's assistant director for operations and managed the agency's emergency operations center coordinating response and

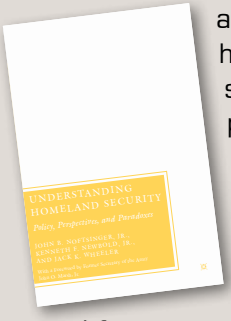
recovery functions following the attacks on the World Trade Center. The Authority owned the World Trade Center and it was its headquarters for over thirty years.

As director, Mr. Paczkowski has supervised comprehensive security assessments of all Port Authority facilities, implemented new security and emergency management practices and technologies, prepared consequence management and business continuity plans for the Authority's corporate headquarters and line businesses, and has spearheaded several national-level projects with the U.S. Department of Homeland Security. This included a ground-breaking critical infrastructure risk management program that has guided over $1 billion in new security capital investment by the Authority and $207 million in federal grants. In September of 2005, he led a Port Authority team that assisted the City of New Orleans in reestablishing incident command and continuity of government less than a week following Hurricane Katrina. Also in 2005, Mr. Paczkowski retired as a colonel with thirty-three years of active and reserve service in the U.S. Marine Corps as both an infantry and combat engineer officer.

Mr. Paczkowski holds a Bachelor of Science in industrial engineering and a Master of Science in engineering management from the New Jersey Institute of Technology, an Master of Science in organizational psychology from Columbia University, and an Master of Science in security studies from the Naval Postgraduate School (NPS), with a concentration in homeland defense and security. On graduation from NPS, he received the prestigious Butch Straub Award for leadership and academic excellence from the Center for Homeland Defense and Security. In addition, he is a graduate of the Marine Corps Command and Staff College, and his military awards include the Legion of Merit Medal. Named a Distinguished Fellow by the Naval Postgraduate School, Mr. Paczkowski is currently on a one-year assignment with the Department, where he is serving with FEMA's National Preparedness Directorate.

Understanding Homeland Security Textbook

Understanding Homeland Security: Policy, Perspectives, and Paradoxes by John Noftsinger, Kenneth Newbold and Jack Wheeler of James Madison University is the first comprehensive academic text regarding homeland security. As a text for students of homeland security, public policy and terrorism studies, "Understanding Homeland Security" explores the complex issues within the emerging domestic protection framework, providing current and future practitioners with a thorough view of the social, psychological, technological and political aspects that have shaped the growth of this movement. *Understanding Homeland Security is published by Palgrave Macmillan (http://www.palgrave-usa.com).*



Poster Presentations in the Exhibit Area (Rm 147A)

The following research projects and highlighted partnerships are featured in the Poster Session in the Exhibit Area (Room 147A). Please visit with the researchers during session breaks and lunch.

Electromagnetic Pulse Commission (EMP Commission)

The Congressionally chartered Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP Commission) recently reported its findings to the Congress, identifying electronic vulnerabilities in the interlocked and interdependent critical systems that sustain our civil society. The Commission's recommendations focused on the civilian infrastructures are available as an unclassified download from the Commission's web site and included measures that confer multiple benefits by improving the resilience and operability of the power grid and mitigating a variety of threats including cyber and potentially significant natural disasters such as Katrina-class solar storms.

Contact: Dr. George Baker, 540-568-8767, bakergh@jmu.edu

Hosting a Cyber Defense Competition

On September 6, 2008, JMU hosted an all-day Cyber Defense competition for students. Approximately thirty students participated divided into five teams. The teams were pitted against a team of 8 attackers comprised of employees from Computer Sciences Corporation, Gemini Security, and one JMU alumni working at Lockheed Martin. The competition was a great success according to all participants.

Contact: Dr. M. Hossain Heydari, Department of Computer Science, James Madison University, (540) 568-8745, heydarmh@jmu.edu; and Dr. Brett Tjaden, Department of Computer Science, James Madison University, (540) 568-2771, tjadenbc@jmu.edu

Analysis of Perceptions toward the Use of Modeling for Emergency Preparedness Planning

A long term project of the modeling team at the Institute for Infrastructure and Information Assurance at JMU is to create a framework for developing models that simulate potential catastrophic events and the impact on infrastructures. As an extension of this project, this project explored the use of modeling and simulation technology for emergency management and planning by surveying a potential user population of this kind of technology. The research identified key attributes of the intended users, their experiences in emergency planning, and their attitudes toward using modeling technology in their planning efforts. The information gathered in this study is intended to support the Institute's modeling team in the development of this project, and to also increase the usability, application, and acceptance of homeland security technologies in the community.

Contact: Ms. Allison M. Smith, MSISAT Graduate Student, smith6am@jmu.edu; Ms. Patricia E. Higgins, 540-568-1727, higginpe@jmu.edu; and Dr. Steven P. Frysinger (Adviser), 540-568-6440, frysinsp@jmu.edu

U.S. Intelligence Failures Analyzed Through Analyst's Notebook

Graduate and undergraduate students at James Madison University conducted research for the Officer of Warning of the National Intelligence Center. This project included researching, modeling, and analyzing information on classic U.S. Intelligence failures. The goal was to identify when and under what circumstances the US made the same intelligence failures. The Intelligence failures that were studied are 9/11, the Berlin Blockade, the Iranian Revolution of 1979, the Soviet Invasion of Czechoslovakia in 1968, the Tet Offensive, the Arab Israeli War of 1973, the Cuban Missile Crisis, the Indian Nuclear Testing of 1974 and 1998, Iraq's invasion of Kuwait, the attack on Pearl Harbor, and Sputnik.

Contact: Ms. Patricia Higgins, 540-568-1727, higginpe@jmu.edu; and Ms. Leigh Ferraro, Undergraduate Student, 732-947-8988, ferrarle@jmu.edu

Office of Technology Transfer

The Office of Technology Transfer (OTT) is responsible for managing the intellectual property (IP) assets of James Madison University, including inventions, copyrights for software and printed materials, and outgoing Material Transfer Agreements for biological materials.

The OTT provides the following services:

- Informs campus researchers about the technology transfer process
- Advises faculty on IP issues
- Solicits and analyzes invention disclosures from faculty, staff, and students
- Analyzes the IP space of the invention for commercialization feasibility and patentability
- Fosters inventor participation in the technology transfer process
- Licenses tangible research property for commercial use
- Licenses patents and copyrights for commercial use
- Connects inventors and venture creation resources

The OTT seeks to build a working relationship with researchers and inventors to facilitate the awareness of the technology transfer process.

Contact: Ms. Mary Lou Bourne, Director of Technology Transfer, 540-568-2865, bourneml@jmu.edu

Offshore Wind and Virginia

This research examines offshore wind turbine and wind farm technology and address's questions that pertain to the technical, environmental, and economic feasibility for such projects off the Virginia coastline.

Contact: Mr. Ryan Geary, Graduate Student, gearyrd@jmu.edu

Functional Mapping of Disease Mitigation Strategies

Picture a computer's map of the world as evidenced by public health professionals who are fighting the spread of various diseases. This "constructed landscape" is proportional to the likelihood of immunization. Locations with similar patterns of disease protection are close to one another, and locations with dissimilar patterns of protection are far apart. For example, if New Zealand and America are next to each other in such a constructed chart, then these two locations would be similar in the effectiveness of their homeland security. Conceptually similar maps can be made of how various diseases spread (we have done this for West Nile Virus). If constructed charts based on the likelihood of pandemic spread from one place to the next are similar to charts constructed from the prevalence of immunization, then we would know that we are optimally fighting the outbreak.

Contact: Dr. Lincoln Gray, 540-568-8154; graylc@jmu.edu

2009 Homeland Security Symposium

Protecting Large Facility Complexes

Electromagnetic Pulse Commission (EMP Commission)

SUMMARY

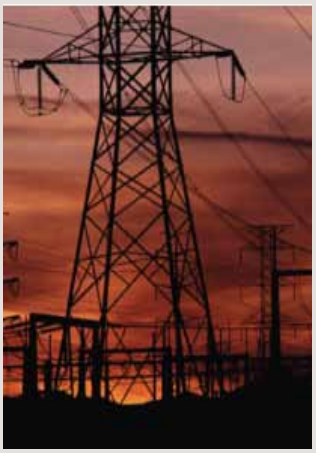
The Congressionally chartered Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP Commission) recently reported its findings to the Congress, identifying electronic vulnerabilities in the interlocked and interdependent critical systems that sustain our civil society. The Commission's recommendations focused on the civilian infrastructures are available as an unclassified download from the Commission's web site and included measures that confer multiple benefits by improving the resilience and operability of the power grid and mitigating a variety of threats including cyber and potentially significant natural disasters such as Katrina-class solar storms.

DESCRIPTION

The Commission's identification of vulnerabilities and recommendations address aspects of all the critical infrastructures, but it is the power grid which is the single most important component of our national system of systems. A few of the steps recommended by the Commission to protect this crucial asset include selective hardening and special grounding to assure functional operation for critical components, increased battery and on-site generator fuel, installation of black start units, exercise of national and regional restoration plans, establishment of Installation standards, a revised system architecture to separate the present interconnected systems into several non-synchronous connected sub-regions or electrical islands. Implementation will also decrease the likelihood that the system, and our personal well being, may suffer catastrophic loss from the inevitable 100–year geomagnetic solar storm that is surely coming

MARKET SIGNIFICANCE

The development of alternative energy sources from sources such as wind farms also envisions the simultaneous development of new extremely high - megavolt class – electrical transmission systems. Such new systems also introduce new vulnerabilities which need to be addressed by approaches such as those embodied in the Commission's recommendations. Some of the concerns over cyber are addressed by still other recommendations. (in the Commission's view, vulnerability of the system to electronic upset at low levels of EMP insult is a neglected component of the cyber threat). There are thus opportunities to improve the resilience and operability of the existing system while reducing vulnerability to a spectrum of threats.



STAGE

These recommendations were developed in response to a Congressional concern about a particular threat. They have broader implications but have not yet been realized in either hardware or operational implementation.

KEYWORDS

electromagnetic pulse
power grid
geomagnetic storms
cyber
resilience
recovery

CONTACT INFO

Dr. George Baker
540.568.8767
bakergh@jmu.edu

Institute
for Infrastructure
and Information Assurance
at James Madison University

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

JAMES MADISON UNIVERSITY

2009 Homeland Security Symposium

Protecting Large Facility Complexes

Hosting a Cyber Defense Competition

SUMMARY

On September 6, 2008, JMU hosted an all-day Cyber Defense competition for students. Approximately thirty students participated divided into five teams. The teams were pitted against a team of 8 attackers comprised of employees from Computer Sciences Corporation, Gemini Security, and one JMU alumni working at Lockheed Martin. The competition was a great success according to all participants.

DESCRIPTION

The competition provided students with great experience and many important lessons. Perhaps the most valuable is what it is like to defend systems in a realistic environment while balancing business requirements with security. One team learned not to all leave their computers unlocked and go to lunch as the attackers came in, sat down, and compromised all their machines while they were away.

To prepare for the competition, we spent the summer preparing the team packet, setting up and configuring the hosts and networks the students would administer and defend, creating and testing the business injects that were used during the competition, and developing the scoring software used throughout the competition. The team packet (which was provided to the teams in advance) describes the machines and network layout that the teams defended, the rules of engagement for both competing teams and the attackers, the scoring rules, and the event schedule.

The network that participants managed was comprised of many standard services including e-mail, a web server, and a firewall. These were all functioning (though not necessarily securely) at the beginning of the competition. Several business tasks were given to the teams throughout the competition. Teams were asked to perform such tasks as installing new services (e.g. FTP) on their hosts and block spam on their mail server. There was a heads-up display of the score board at the front of the room so that each team could see the status of their network and which of their services were available. At the end of the competition, over dinner, the attackers made a presentation and discussed some of their successful attacks with the teams. They recommended specific things that the teams could have done to better protect their machines. The competition ended with the announcement of the winners and everybody feeling exhausted, overwhelmed, and a whole lot wiser. The winning team (and several other participants) joined JMU's Cyber Defense Club which recently won the Mid-Atlantic qualifying round of the National Collegiate Cyber Defense Competition.

MARKET SIGNIFICANCE

Hosting this competition strengthened our ties with several industry partners (including Computer Sciences Corporation and Gemini Security). This has resulted in increased intern and employment opportunities for our students with these companies. Even companies that didn't participate in the competition have shown great interest in hiring our students because they have had such "real world" experience in this area. Having hosted a competition once, we feel that there are numerous opportunities to expand upon this work.

STAGE

We believe the next steps for this work include hosting a competition for high school seniors on a day when prospective students are coming to campus. Such a unique opportunity could very well attract high caliber students interested in Science, Technology, Engineering, and Mathematics and interest them in JMU's Information Security and other STEM programs. Also, foresee hosting competitions for state or private I.T. professionals to practice and refine their Cyber Defense skills. We have already had inquiries from as far away as Delaware about the possibility of running a Cyber Defense Competition for a group of employees.

KEYWORDS

Cyber Defense Competition
Information Assurance
Network Security

CONTACT INFO

Professor M. Hossain Heydari
Department of Computer Science. James Madison University
(540) 568-8745
heydarmh@jmu.edu

Associate professor Brett Tjaden
Department of Computer Science. James Madison University
(540) 568-2771
tjadenbc@jmu.edu

Institute for Infrastructure and Information Assurance
at James Madison University

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

JAMES MADISON UNIVERSITY

Modeling Pandemic Flu for Hospitals

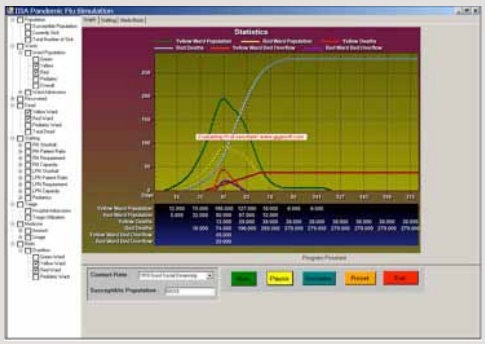
IIIA Wins! 2008 COVITS Governor's Innovative Use of Technology in Higher Education Award*

SUMMARY

... In January of 2007, a team of researchers from James Madison University's Institute for Infrastructure and Information Analysis collaborated with medical professionals at a semi-rural hospital in Virginia to develop a tool to aid the hospital staff in understanding the **full impact of a influenza pandemic on the hospital, its staff, and the hospital capacity.** The tools developed from this effort demonstrate the impact on scarce resources during a flu pandemic at a rural hospital. The resources include nursing staff requirements, medications, and hospital beds. The model produces various graphs, providing a more holistic view of the impact of an influenza pandemic on a hospital.

DESCRIPTION

The model has several useful implications as a **decision support tool for pandemic surge planning.** In addition to the physical space available for the patient surge, understanding how to manage patient care with reduced staffing and limited supplies is essential to reducing mortality and improving patient outcomes during a pandemic. This model enables the hospital's medical personnel to examine the changes in the availability of medication, staff, and beds, based on the number of patients seeking care during an influenza outbreak. Four scenarios were created to aid the hospital with decision making. Three of the scenarios are grounded in historic data: the 1918 Spanish flu, 1957-58 Asian flu, and the seasonal flu. The fourth scenario is a hypothetical "Category 3" pandemic flu scenario based on the CDC's "flu severity index" that would manifest as less severe than a 1918 Spanish flu scenario, but more severe than a 1957-58 Asian flu scenario (Centers for Disease Control, 2007).



MARKET SIGNIFICANCE

In the light of the current **Swine Flu Pandemic**, interest has grown in preparing for and planning for Flu Pandemics of any kind or morbidity. In the event of a flu pandemic, federal assistance will likely not be available for localities. Each will be responsible for implementing its own community surge preparedness/response plans. This tool supports planning and decision making for medical facilities during a flu pandemic.

STAGE

This model was developed specifically to answer the questions of a hospital in the Shenandoah Valley. Augusta Medical Center was the application, designed to be used by hospitals with service populations of less than 300,000, is available for licensing. Further research into other aspects of health related surge capacity problems are under consideration – e.g. managing a flu outbreak at a University, impacts of the flu on the economy of the community, etc.

***Winner:** James Madison University with August Medical Center and the Virginia Department of Health

For: Pandemic Flu Modeling Partnership

Preparing for response to a health related crisis such as a wide spread flu outbreak requires prior coordination and planning. James Madison University, Augusta Medical Center, and the Virginia Department of Health have developed a unique partnership to provide solutions to surge capacity issues impacting regional hospitals. The software enables hospital management to understand the ramifications of a patient surge. Hospitals can use the model to explore different scenarios and the impact a surge can exert on the standard level of care at a particular hospital. The model demonstrates staffing levels of various nursing competencies, hospital bed and medicine availability.

KEYWORDS

influenza pandemic
community surge assessments
agent-based modeling
system dynamics
hospital preparedness

CONTACT INFO

Patricia Higgins, Associate Director for Modeling & Information Assurance, IIIA, 540-568-1727, higginpe@jmu.edu

Cheryl J. Elliott, Assistant Director for Marketing & External Relations, IIIA, 540-568-4442, elliotcj@jmu.edu

Institute for Infrastructure and Information Assurance at James Madison University

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

JAMES MADISON UNIVERSITY

2009 Homeland Security Symposium

Protecting Large Facility Complexes

Analysis Of Perceptions Of Emergency Preparedness Modeling

SUMMARY

A long term project of the modeling team at the Institute for Infrastructure and Information Assurance at JMU is to create a framework for developing models that simulate potential catastrophic events and the impact on infrastructures. As an extension of this project, this thesis explored the use of modeling and simulation technology for emergency management and planning by surveying a potential user population of this kind of technology. The research identified key attributes of the intended users, their experiences in emergency planning, and their attitudes toward using modeling technology in their planning efforts. The information gathered in this study is intended to support the Institute's modeling team in the development of this project, and to also increase the usability, application, and acceptance of homeland security technologies in the community.

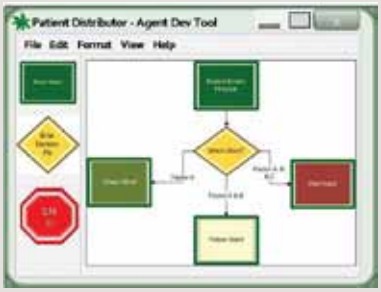


Figure 1 is an example of a "Patient Distributer" decision tree, which determines the ward of the hospital a patient will be routed to depending on the degree of illness. The patient may 'encounter' the Patient Distributor several times as the patient gets better or worse.

DESCRIPTION

The proposed modeling framework is currently envisioned to be supported by several core components including a JMU-developed agent-based model engine, subject matter expertise knowledge acquisition, and, and various methods for output definition based on problem specifications and client needs. Agents will be defined and their rules or decision trees will be crafted in the modeling tool.

METHOD AND SAMPLING... An anonymous survey was constructed using JMU's electronic survey tool subscription, Qualtrics, in order to understand perceptions toward modeling for emergency preparedness planning. The survey was distributed to local and regional officials involved in emergency management, planning, or response. Specifically, the target population included: attendees of JMU's Catastrophic Event Resource Planning workshop, members of the Commonwealth Preparedness Working Group, members of the All Hazards Consortium, and regional coordinators with the Virginia Department of Emergency Management. The survey consisted of a total of 41 questions pertaining to the participants' area of work, their current planning efforts, and their attitudes and interests in using modeling and gaming technology for preparedness planning.

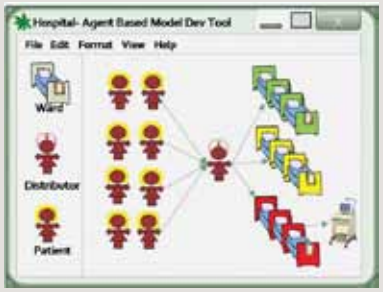


Figure 2 is an example of how connections will be made between various agents. Each agent will be "laid out" in an environment showing general interactions. In this figure, for example, patients first encounter the Patient Distributor which then routes them to a Bed (an agent) in each Ward. In this example the Bed Agent would monitor the patient's illness and possibly send a patient getting worse back to the Patient Distributor.

SUMMARY OF RESULTS...A total of 32 participants responded to the anonymous survey. This population believes modeling technology is useful and would be valuable in their emergency planning efforts. Overwhelmingly, the participants agreed that having a tool that could allow them to realistically address different concepts and scenarios, understand human behaviors, and understand multiple aspects of a crisis situation would be beneficial in their emergency planning positions.

Figure 3 is an example of an output the Patient Distributor model could produce. The graph models all the patients in each ward at a given point as well as the number of patients that are 'distributed' per day.

CONCLUSIONS... The survey aimed to gain perceptions toward the use of modeling for emergency preparedness planning produced excellent feedback from a population of potential users of the agent modeling tool. Overwhelmingly, the participants agreed that having a tool that could allow them to realistically address different concepts and scenarios, understand human behaviors, and understand multiple aspects of a crisis situation would be beneficial in their emergency planning positions. Cost was a factor that was frequently mentioned throughout the survey. While some saw using this technology as cost-effective for planning and training staff, many reported that their limited budgets might inhibit the use of such tools.

Some quotes from participants:

- *Computer modeling tools would allow our organization the benefit of more precise results. We welcome better technology however funding has been an obstacle for us.*
- *If you have to maneuver thru realistic scenarios kind of like Sim City it would be very helpful. Especially if State regulations and policies could be utilized within the game.*
- *Most planning scenarios are too scripted. There is nothing better than "free play" to scope scenarios more completely and effectively.*
- *I believe that computer modeling tools would help us identify weaknesses in our current planning efforts, thereby helping us improve our quality of response. I would also want to expand our breadth of scenarios which we could model and develop response strategies for them. Perhaps computer modeling could also assist with developing chain of command structures.*
- *I would welcome the ability to make decisions in a controlled format. Gaming gives you the opportunity to make mistakes and learn from them.*
- *It could simulate situations to see how they play out, add understanding of each individual's or group's roles, and provide insight into improving our planning.*

Future DIRECTIONS

Since participants were engaged throughout the survey and provided thoughtful feedback, this indicates they would be receptive to further usability testing. The IIIA modeling team will continue to work with these individuals and seek others in similar positions in order to further develop the agent modeling tool framework. The Institute for Infrastructure and Information Assurance has the ability to build and maintain strategic alliances, and its modeling team has the ability and to develop a homeland security tool that could (and would) be accepted and applied within the community. The next step is to harness these abilities and support our local and regional emergency management officials in their preparedness planning.

CONTACT INFO

Patricia Higgins, James Madison University, Institute for Infrastructure and Information Assurance, 540-568-1727, higginpe@jmu.edu

Allison M. Smith, Graduate Student, JMU ferrarle@jmu.edu

Dr. Steven P. Frysinger, Adviser 540-568-2710; frysinsp@jmu.edu

Institute for Infrastructure and Information Assurance at James Madison University

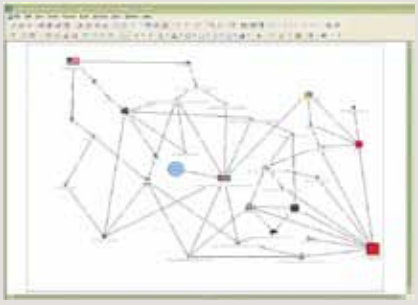
This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

JAMES MADISON UNIVERSITY

U.S. Intelligence Failures Analyzed through Analyst's Notebook

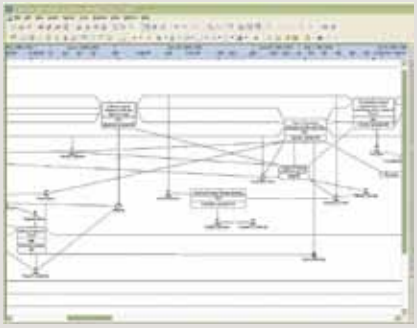
SUMMARY

Graduate and undergraduate students at James Madison University conducted research for the Officer of Warning of the National Intelligence Center. This project included researching, modeling, and analyzing information on classic U.S. Intelligence failures. The goal was to identify when and under what circumstances the US made the same intelligence failures. The Intelligence failures that were studied are 9/11, the Berlin Blockade, the Iranian Revolution of 1979, the Soviet Invasion of Czechoslovakia in 1968, the Tet Offensive, the Arab Israeli War of 1973, the Cuban Missile Crisis, the Indian Nuclear Testing of 1974 and 1998, Iraq's invasion of Kuwait, the attack on Pearl Harbor, and Sputnik.



DESCRIPTION

Through the use of Analyst's Notebook, the students were able to represent the events around the Intelligence failure. The students developed a failure matrix to show the common errors that U.S. Intelligence community made during these incidents. The failures fell into two catagories: Miss-assessment of Opponents Actions or Propensity to Act and Failures of Conveyance (see table for full list and examples) The most common types of failures were bias/groupthink, failure to take each warning seriously ("cry wolf"), failure to address alternative scenarios or dissenting opinions, and failing for denial and deception activities.



Type of Failure	Failure Description	Example
Miss-assessment of Opponents Actions or Propensity to Act	Bias or Groupthink	
	Failing for Denial & Deception Activities	
	Failure to Take Each Warning Seriously ("Cry Wolf")	
	Applying Mirror-Image Thinking or a Rational Actor Model (Overconfidence)	
	Failure to Offer Alternative Scenarios or Dissenting Opinions	
	Ignorance of the Situation	
	Overestimation of Target	
Failures of Conveyance	Unavailability of Information due to Bureaucracy or Resource Hindrances	
	Failure of Inter-Agency Cooperation in Information Sharing	
	Decision Makers Distracted by Other World Events	

MARKET SIGNIFICANCE

The significance of this research is two-fold; it examined the usability of using timelines for complex problems (see diagrams) and it identified and catagorized failures that are seen across intelligence work (see table). The latter provides an alternate way to teach intelligence failures (failure type vs. case studies).

STAGE

The next step for this research is to apply the methodology to classified, and more recent, failures.

KEYWORDS

Intelligence failures
Analyst's Notebook

CONTACT INFO

Patricia Higgins, James Madison University, Institute for Infrastructure and Information Assurance, 540-568-1727, higginpe@jmu.edu

Leigh Ferraro, Undergraduate Student, James Madison University, Information Analysis, Institute for Infrastructure and Information Assurance, 732-947-8988, ferrarle@jmu.edu

Institute for Infrastructure and Information Assurance at James Madison University

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

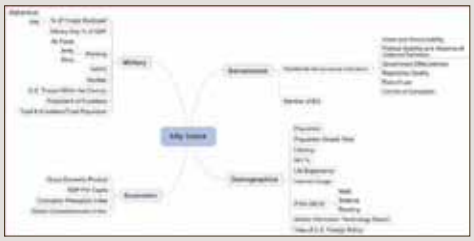
JAMES MADISON UNIVERSITY

Could Lithuania Be A Valuable U.S. Ally? (A Comparative Statistical & GIS Analysis)

SUMMARY

Using two "Ally Indices" - Statistical and GIS – this Master's Thesis determined if Lithuania should be prioritized as an U.S. strategic partner. Lithuania's geographical location is ideal for U.S. economic and defense initiatives. There is an increased need for U.S. allies in the Eastern European region based on the following recent events:

- War between Russia and Georgia.
- Russia's increasing strong relationships with China, Iran, and Venezuela.
- Deteriorating relationships between U.S., Russia, and NATO.
- The planned U.S. missiles in Poland and radar installation in the Czech Republic.
- Russia's threat of placing Iskander missiles in Kaliningrad.
- Russia's recent "flexing" of their muscles.


Statistical Index


GIS Index

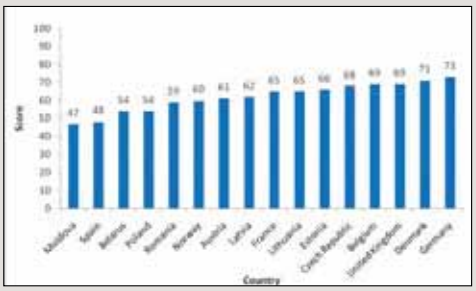
DESCRIPTION

Classic approaches to determining alliances have not always been statistically rigorous and currently do not include analysis based on quantitative GIS analysis. Two "Ally Indices" were developed: one from traditional statistical factors and one from GIS based factors.

Infrastructure of Lithuania


Distances to Capitals of Europe

The Statistical and GIS "Ally Indices" were combined to form a Final "Ally Index" (Below) with a score out of 100. Lithuania scored 65 which placed it higher than Poland (where the U.S. is currently planning to place missiles). This index indicates that Lithuania is a viable and potentially valuable U.S. ally.



Final Ally Index

MARKET SIGNIFICANCE

New methods in Intelligence Analysis are crucial to the future success of the defense of the U.S. Utilizing methodologies like this will enable U.S. decision makers to develop more informed and holistic defense policies.

STAGE

Research and development of the methodology is complete. Further refinement and testing against other methodologies is the next step. This Index could be modified to assess additional countries for potential foreign policy initiatives.

KEYWORDS

Foreign Policy
GIS
Lithuania
U.S. Allies

CONTACT INFO

Daniel Kitchie, (518) 225-5496, kitchie33@yahoo.com
Dr. Robert Kolvoord (advisor), (540) 568-2752, kolvoora@jmu.edu

Institute for Infrastructure and Information Assurance at James Madison University

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

JAMES MADISON UNIVERSITY

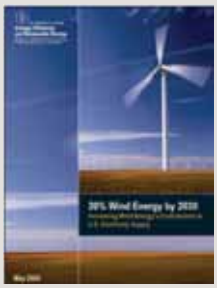
2009 Homeland Security Symposium

Protecting Large Facility Complexes

Offshore Wind and Virginia

SUMMARY

This research examines offshore wind turbine and wind farm technology and address's questions that pertain to the technical, environmental, and economic feasibility for such projects off the Virginia coastline.



DESCRIPTION

The Virginia coastline and specifically the Virginia Beach area are prime locations for the installation of offshore wind farms. Before these wind parks can be installed comprehensive and thorough studies must be completed in order to determine the environmental and economic impacts on the surrounding area. This research reviews the Department of Energy's 20% Wind Energy by 2030 report and in particular the projected contribution from Virginia.

The study analyzes the applicability of these technologies in Virginia's waters to determine whether they are commercially and economically viable and if the current energy infrastructure is capable of supporting the added generation. The findings from this research are being compiled to assess the efficacy of offshore wind technology and whether Virginia will meet the goals for wind described in the 20% report. With the DOE's goal of providing 20% of the energy in the U.S. through wind by 2030 the construction of offshore wind parks would allow Virginia to move forward with its goals in meeting its projected contribution. This research covers issues such as environmental impact mitigation, offshore turbine foundations, offshore to onshore electrical grid interconnection, and a timeline for the construction of these parks in order to meet the Virginia and DOE goals.

MARKET SIGNIFICANCE

There are many advantages to having offshore wind brought to Virginia. The development of this industry will not only provide clean renewable energy to Virginia but it will also serve to create jobs and move the United States one step closer to energy independence.

STAGE

The stage of the wind industry has changed drastically over the last several decades. With new technological achievements and a steady decrease in cost wind developers have been able to expand their operations to almost anywhere in the United States. Their efforts have been motivated in part from increasing interest by Federal, State, and local governments in clean renewable energy. Many States have already taken the first steps in conducting feasibility studies and offering tax incentives for developing companies. As development continues to move forward developers will see decreased cost in construction and maintenance. Newer and more efficient technologies will also help relieve government uncertainties over environmental impacts.

KEYWORDS

offshore wind
wind turbine
wind farm
grid interconnection
alternative energy
energy independence
wind energy

CONTACT INFO

Ryan Geary
Graduate Student
James Madison University
Gearyd@jmu.edu

Institute for Infrastructure and Information Assurance at James Madison University

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

JAMES MADISON UNIVERSITY

2009 Homeland Security Symposium

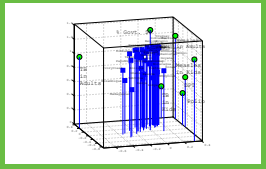
Protecting Large Facility Complexes

Functional Mapping of Disease Mitigation Strategies

SUMMARY

Picture a computer's map of the world as evidenced by public health professionals who are fighting the spread of various diseases. This "constructed landscape" is proportional to the likelihood of immunization. Locations with similar patterns of disease protection are close to one another, and locations with dissimilar patterns of protection are far apart. For example, if New Zealand and America are next to each other in such a constructed chart, then these two locations would be similar in the effectiveness of their homeland security. Conceptually similar maps can be made of how various diseases spread (we have done this for West Nile Virus). If constructed charts based on the likelihood of pandemic spread from one place to the next are similar to charts constructed from the prevalence of immunization, then we would know that we are optimally fighting the outbreak.

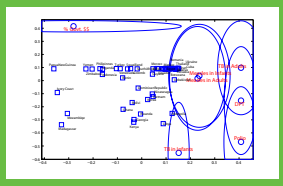
The following graphic represents a functional map of vaccination rates for 7 vaccinations in 49 developing countries. The squares represent different countries. Countries that are close together have similar vaccination rates. The circles represent different vaccines. Circles that are close together indicate similar patterns in these two vaccinations in the developing countries. The closer a country is to a circle the higher that vaccination rate in that country.



DESCRIPTION

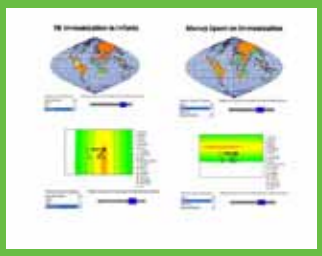
Vaccination rates are mathematically modeled as if they "spread" across developing countries. A technique that had previously been used to model the spread of diseases effectively models the spread of disease prevention. Multidimensional scaling successfully summarizes complex patterns in vaccination rates in developing countries using a "constructed chart." Countries that have similar vaccination rates are close together in this functional map, and countries that have different rates are far apart, regardless of the physical distance between the countries. A statistically significant ($p<0.001$) map was made of seven different vaccination rates (diphtheria, polio, measles in adults, measles in infants, tuberculosis in adults, tuberculosis in infants, and total percent of routine epidemic vaccines financed by government) in 49 developing countries (Belarus, Belize, Benin, …Vietnam, Yemen, and Zimbabwe). See **http://www.csd.jmu.edu/csdsquared/** for more explanation and details.

Figure 2 shows the two-dimensional functional map of the same data as is represented in figure 1. The prevalence of immunization is indicated by distances from "centers" for each disease. Note that the relationships are more difficult to understand when represented in this way.



An interactive visualization tool for this kind of analysis is available at http://www.csd.jmu.edu/csdsquared. A visitor to the interactive Web site first selects a disease, one of the seven vaccines from the menu at the lower left. The visitor then moves a slider to advance the model, and the predicted prevalence of immunity is depicted as changing colors.

The left half of the figure below contains screens from the physical and functional (top and bottom, respectively) predictions of TB immunization in infants. The right half has similar physical and functional versions of the predicted percentage of public money.



MARKET SIGNIFICANCE

This technique of "Constructed Cartography" has been generally useful for depicting complex patterns in data as a simple "map" when typical presentations of those data (such as tables) make it difficult to "see the forest for the trees". The method provides statistically and clinically significant interactive and visual summaries of how oral and breast cancers metastasize, how pandemics spread, and how humans migrate. Here we see that the SAME technique that can model the spread of a disease can ASLO model our attempts to mitigate that threat. The technique is valuable for identifying unusual events and for dealing logically with missing data.

STAGE

The investigator is interested in finding partners for an SBIR/STIR: perhaps someone interested in public health, homeland security, or health-care insurance – anyone interested in finding patterns in "messy" medical data.

KEYWORDS

Data mining
medical informatic
pandemic protection

CONTACT INFO

Dr. Lincoln Gray
540-568-8154
graylc@jmu.edu

Institute for Infrastructure and Information Assurance at James Madison University

This research was supported [in parts] by the Critical Infrastructure Program under Grant #60NANB2D0108, by the National Institute of Standards and Technology. The views expressed are those of the authors, and do not necessarily reflect those of the sponsors.

JAMES MADISON UNIVERSITY

IIIA Advisory Board

The mission of the IIIA is to facilitate development, coordination, integration, and funding of activities and capabilities of the James Madison University academic community to enhance information and critical infrastructure assurance at the federal, state, and local levels. The Institute is guided by an advisory board that includes a distinct group of individuals representing business, industry and government.

Mike Becraft, Serco North America
Daniel Caprio, DC Strategies, LLC
Grant Cooley, Global Strategies Group, Mission Systems
Raghu Dev, Oracle Corporation
Kevin Esser, Analytic Solutions, Inc.
Chaz Evans-Haywood, Harrisonburg and Rockingham County
Helen Franks, Cisco Systems, Inc.
Jacqueline Gamblin, Ingenium Corporation
Gene Garlick, Northrop Grumman Information Technology
Mike Hutton, National Counterterrorism Center
Matthew Keller, Corsec Security, Inc.
Michael King, Northrop Grumman Information Technology
Ken Knight, Office of the Director for National Intelligence
Peter Lejeune, Strategic Analysis, Inc.
Richard Little, University of Southern California, Keston Institute for Infrastructure
Sadaat Malik, Cisco Systems, Inc.
Skip Maupai, Dominion Group, Ltd.
Louis McDonald, Virginia's Center for Innovative Technology
Bill McGilvery, i2 Inc.
Don Parr, Bearing Point
Jeffery Payne, Coveros, Inc.
Brendan Peter, LexisNexis Special Services, Inc.
Ben Plowman, Luna Innovations, Inc.
John Rice, DDL Omni Engineering
Jim Rigney, CACI
Kyndra Rotunda, Chapman University School of Law
Joe Rozek, Microsoft Corporation
Dutch Thomas
Jay Willer, Blue Ridge Home Builders Association

Federal Facilities Council

Lynda Stanley
Director, Board on Infrastructure and the Constructed Environment
National Research Council
500 Fifth Street, NW, Room 943
Washington DC 20001
Phone: 202-334-3374; Fax: 202-334-3370;
lstanley@nas.edu
www.nationalacadmies.org/bice

Institute for Infrastructure & Information Assurance at James Madison University

MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-4442; Fax: 540-568-3521
www.jmu.edu/iiia

Dr. John B. Noftsinger, Jr.
Vice Provost for Research and Public Service; Executive Director, IIIA
MSC 4107, Harrisonburg, VA 22807
Phone: 540-568-2700; noftsijb@jmu.edu
www.jmu.edu/research

Dr. George H. Baker
Technical Director, IIIA
MSC 4102, Harrisonburg, VA 22807
Phone: 540-568-8767; bakergh@jmu.edu

Mr. Benjamin T. Delp
Assistant Director for Administration and Public Policy, IIIA
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-1661; delpbt@jmu.edu

Ms. Cheryl Elliott Wilkins
Assistant Director for Marketing and External Relations, IIIA
MSC 3804, Harrisonburg, VA 22807
Phone: 540-568-4442; elliotcj@jmu.edu

Dr. M. Hossain Heydari
Associate Director for Information Assurance, IIIA
MSC 4103, Harrisonburg, VA 22807
Phone: 540-568-8745; heydarmh@jmu.edu

Ms. Patricia Higgins
Associate Director for Information Analysis and Modeling, IIIA
MSC 3804, Harrisonburg, VA 22807
Phone: 540-568-1727; higginpe@jmu.edu

Mr. Kenneth F. Newbold, Jr.
Director of Research Development
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-1739; newbolkf@jmu.edu

Mrs. Rebecca L. Rohlf
Fiscal Technician
MSC 4111, Harrisonburg, VA 22807
Phone: 540-568-3640; rohlfrl@jmu.edu

IIIA Graduate Fellows:
Lynne Murray, Avery Daugherty, Blase Etzel, and Ryan Cornett

About Your Hosts...

The **Federal Facilities Council**

www.nationalacademies.org/ffc/

The Federal Facilities Council (FFC) was established in 1953 as the Federal Construction Council. It operates under the auspices of the Board on Infrastructure and the Constructed Environment (BICE) of the National Research Council, the principal operating agency of the National Academies and the National Academy of Engineering.

The FFC's mission is to identify and advance technologies, processes, and management practices that improve the performance of federal facilities over their entire life-cycle, from planning to disposal.

- develops and disseminates facilities-related information through networking, conferences, workshops, and studies;
- provides a forum to identify government-wide issues regarding facility planning, design, construction, operation, maintenance, and management;
- convenes standing committee meetings to promote networking and information sharing among sponsor agencies;
- deploys its findings through its reports published by the National Academy Press.

The **Institute for Infrastructure and Information Assurance**

www.jmu.edu/iiia/

Institute
for Infrastructure
and Information Assurance
at James Madison University

The Institute for Infrastructure and Information Assurance (IIIA) facilitates development, coordination, integration and funding of activities and capabilities of the James Madison University academic community to enhance information and critical infrastructure assurance at the federal, state and local levels. IIIA emphasizes collaborative interdisciplinary research that focuses on developing technologies with student participation that have potential for public benefit and commercialization.

Further, the Institute focuses on the integrative, interdisciplinary nature of real-world problems and strives to bridge traditional academic departments to develop solutions to the critical security problems facing our nation. IIIA partners with George Mason University on the Critical Infrastructure Protection Program (CIPP). IIIA Vision is a society strengthened and enriched by increasingly dependable infrastructure fostered by a strong university role in leadership, interdisciplinary education, research and problem-solving.

JAMES MADISON UNIVERSITY

James Madison University is a comprehensive university that is part of the statewide system of public higher education in the Commonwealth of Virginia and is the only university in America named for James Madison. Established March 14, 1908, the university offers programs on the bachelor's, master's and doctoral levels with its primary emphasis on the undergraduate student. JMU provides a total education to students — one that has a broad range of the liberal arts as its foundation and encompasses an extensive variety of professional and pre-professional programs, augmented by a multitude of learning experiences outside the classroom. The university has been a coeducational institution since 1966.