NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING AGENDA

Tuesday, July 11, 2006
1:30 – 4:30 p.m. ET
National Press Club
529 14th Street NW
Washington, DC 20045

I.	**OPENING OF MEETING**	*Jenny Menna*, Designated Federal Officer, NIAC, Department of Homeland Security (DHS)
II.	**ROLL CALL OF MEMBERS**	*Jenny Menna*
III.	**OPENING REMARKS AND INTRODUCTIONS**	NIAC Chairman, *Erle A. Nye*, Chairman Emeritus, TXU Corp. NIAC Vice Chairman, *John T. Chambers*, President and CEO, Cisco Systems, Inc. *Frances Fragos Townsend*, Assistant to the President for Homeland Security and Counterterrorism *Robert Stephan*, Assistant Secretary, Office of Infrastructure Protection, DHS
IV.	**APPROVAL OF APRIL MINUTES**	NIAC Chairman, *Erle A. Nye*
V.	**FINAL REPORTS AND DELIBERATIONS**	NIAC Chairman, *Erle A. Nye* Presiding
	A. INTELLIGENCE COORDINATION	NIAC Vice Chairman *John T. Chambers*, President and CEO, Cisco Systems, Inc. and *Gilbert Gallegos*, Chief of Police (ret.), Albuquerque, New Mexico Police Department, NIAC Member
	B. DELIBERATION AND APPROVAL OF RECOMMENDATIONS OF FINAL REPORT	*NIAC Members*
VI.	**STATUS REPORTS ON CURRENT WORKING GROUP INITIATIVES**	NIAC Chairman, *Erle A. Nye* Presiding

A. CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT CHALLENGES	*George Conrades*, Executive Chairman, Akamai Technologies, NIAC Member, *Margaret Grayson*, President, Grayson and Associates, NIAC Member, and *Gregory A. Peters*, Former President and CEO, Internap Network Services Corporation, NIAC Member.
B. CHEMICAL, BIOLOGICAL AND RADIOLOGICAL EVENTS AND THE CRITICAL INFRASTRUCTURE WORKFORCE	*Chief Rebecca F. Denlinger*, Fire Chief, Cobb County, Georgia Fire and Emergency Services, NIAC Member, *Martha H. Marsh*, Chairman and CEO, Stanford Hospital and Clinics, NIAC Member and *Bruce Rohde*, Chairman and CEO Emeritus, ConAgra Foods, Inc.
VII. NEW BUSINESS	NIAC Chairman, *Erle A. Nye*, NIAC Members TBD
A. INTRODUCTION OF A NEW TOPIC: THE PRIORITIZATION OF CRITICAL INFRASTRUCTURE FOR A PANDEMIC OUTBREAK IN THE UNITED STATES	*Chief Rebecca F. Denlinger*, Fire Chief, Cobb County, Georgia Fire and Emergency Services, NIAC Member, *Martha H. Marsh*, Chairman and CEO, Stanford Hospital and Clinics, NIAC Member and *Bruce Rohde*, Chairman and CEO Emeritus, ConAgra Foods, Inc.
VIII. ADJOURNMENT	NIAC Chairman, *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Vice Chairman Chambers, Mr. Archuleta, Mr. Berkeley, Chief Denlinger, Lt. Gen. (ret) Edmonds, Mr. Gallegos, Ms. Grayson, Ms. Marsh, Mr. Noonan, and Mr. Thompson.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Chairman Nye, Dr. Barrett, Mr. Nicholson, Mr. Peters, Mr. Rohde, and Dr. Rose.

MEMBERS ABSENT:
Mr. Conrades, Mr. Davidson, Mr. Hernandez, and Commissioner Kelly.

OTHER DIGNITARIES PRESENT:
U.S. Government: Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security/Counter Terrorism (APHS/CT), Ms. Susan B. Reingold, Deputy Program Manager, Information Sharing Environment, Office of the Director of National Intelligence (ODNI), Mr. Robert B. Stephan, Assistant Secretary, Office of Infrastructure Protection, and Ms. Jenny Menna, DFO, NIAC.

I. OPENING OF MEETING

Ms. Jenny Menna introduced herself as the Designated Federal Officer (DFO) for the National Infrastructure Advisory Council (NIAC) and the Preparedness Directorate of the Department of Homeland Security (DHS). She welcomed Ms. Frances Fragos Townsend, APHS/CT, Ms. Susan Reingold, Deputy Program Manager for the Information Sharing Environment at ODNI, Mr. Robert B. Stephan, Assistant Secretary for Infrastructure Protection, Mr. Erle A. Nye, NIAC Chairman, Mr. John T. Chambers, NIAC Vice Chairman, and all Council members present or on the teleconference. She welcomed the members' staffs and other Federal government representatives. Ms. Menna also extended a welcome on behalf of DHS to the members of the press and public. She reminded the members present and on the teleconference the meeting was open to the public and, accordingly, to exercise care when discussing potentially sensitive information. Pursuant to her authority as DFO, she called the sixteenth meeting of the NIAC and the third meeting of 2006 to order. Ms. Menna then called roll.

II. ROLL CALL

III. OPENING REMARKS AND INTRODUCTIONS

NIAC Chairman, *Erle A. Nye,* Chairman Emeritus, TXU Corp.

NIAC Vice Chairman, *John T. Chambers*, President and CEO, Cisco Systems, Inc.

Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism

Robert B. Stephan, Assistant Secretary, Office of Infrastructure Protection, DHS

Chairman Nye welcomed everyone in attendance and on the phone and thanked them for their participation. He also welcomed Mr. Edmund Archuleta, General Manager of El Paso Water Utilities and Mr. James Nicholson, President and CEO of PVS Chemical, Inc. They will bring important sector insight and expertise not currently represented in the NIAC. Assistant Secretary Stephan would swear them in as NIAC members later in the meeting. Chairman Nye noted Mr. Archuleta and Mr. Nicholson could only participate as observers until they were sworn in by the Assistant Secretary.

Chairman Nye then introduced Ms. Susan Reingold, Deputy Program Manager for the Information Sharing Environment, ODNI. Chairman Nye thanked her for participating on Ambassador Ted McNamara's behalf and for their interest in the Intelligence Coordination Working Group Final Report and Recommendations. Chairman Nye asked Vice Chairman Chambers if he had any comments.

Vice Chairman Chambers thanked Chairman Nye, Ms. Nancy Wong and Ms. Menna for the organization and structure they provide the group. He then joined Chairman Nye in welcoming the Council's new members. Vice Chairman Chambers thanked the new members for joining the Council's efforts to improve the security of the nation's critical infrastructure.

The Vice Chairman announced the Intelligence Coordination Working Group would present its recommendations later in the meeting. The Working Group must still work out final details of the report which will be ready in the next few weeks, but they have the recommendations ready for the Council's acceptance. Vice Chairman Chambers also said the Convergence Working Group and the Chemical, Biological, Radiological Working Groups will provide status updates. Vice Chairman Chambers then asked Assistant Secretary Stephan to comment.

Assistant Secretary Stephan thanked Chairman Nye, Vice Chairman Chambers and the members of the NIAC. He also thanked Mr. Archuleta and Mr. Nicholson for their interest in becoming members. The Assistant Secretary praised the NIAC's consistent work that the Department uses to create important critical infrastructure protection policy.

The Assistant Secretary told the Council their sector expertise aided in developing the National Infrastructure Protection Plan (NIPP) Base Plan and will help with the sector specific plans.

Assistant Secretary Stephan expressed his pleasure with the state of critical infrastructure protection in 2006. DHS made fundamental progress at the national level and within each sector. He praised

the private sector for their role in the public-private partnership; with both sides coming together for a common cause, critical infrastructure protection can move forward with a knowledge base within each of the 17 sectors.

The NIAC's recommendations helped create the NIPP Base Plan and the Critical Infrastructure Partnership Advisory Council (CIPAC). The Council continues to produce important recommendations which DHS needs to continue implementing. The NIPP Base Plan is now available in hard copy, and the sector specific plans should come together in the next few months.

In terms of the government's partnership with the private sector, sector coordinating councils continue to meet with their government coordinating councils to focus on the status of critical infrastructure protection within the sectors. Also within each of the 17 sectors, DHS has launched pilots or full-scale deployments of the Homeland Security Information Network-Critical Sectors. Assistant Secretary Stephan detailed the importance of this as a trusted environment allowing DHS to send each sector real-time threat information as well as strategic level threat assessments. The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) develops both tactical products, meaningful and decipherable outside the intelligence community. This allows people inside the infrastructure sectors to better understand what the government is telling them. Most importantly, DHS is developing these assessments with the private sector's help. The Assistant Secretary stated he was close to determining whether DHS may grant Federal Transit Subsidies to private-sector individuals for a one-year tour of duty inside HITRAC.

Additionally, the Assistant Secretary said DHS has been working steadily with the nuclear energy and chemical sectors to ensure that buffer zone protection plans are tied to specific, critical deficiency-focused grant money in areas such as state and local law enforcement capabilities gaps and their connectivity to individually identified high-risk infrastructure sites. Every single nuclear power plant and the tier one, two, and three chemical plants will be covered by the end of 2007. Assistant Secretary Stephan told the group DHS recently announced $400 million in infrastructure-protection-related grants across ports, mass transit systems, rail lines, buses, and individually identified high-risk infrastructures within all 17 sectors, based upon consequences, vulnerabilities, and threat analysis.

According to Assistant Secretary Stephan, DHS has also cooperated with the private sector to prepare for the 2006 hurricane season. Together, they held nine regional exercises across the country where they learned important lessons, gathered results, and identified gaps. The Secretary moved to pre-designate principal Federal officials, Federal coordinating officers and their deputies, and infrastructure liaisons for each of the targeted potential impact zones--Gulf Coast and Atlantic--for this hurricane season.

The last topic the Assistant Secretary discussed was the avian flu. He told the Council DHS officials do not know when or where it will strike but are fairly confident it will strike. No one knows at this point whether it takes a bird-to-human, or human-to-human transmutation variant, but the Department must be prepared for the worst case scenario. DHS partnered with the Department of Health and Human Services (HHS), the Centers for Disease Control and Prevention (CDC) and the 17 Critical Infrastructure sectors and published a pandemic influenza planning guide for critical infrastructures and key resources.

Assistant Secretary Stephan told meeting participants his office is working on distributing the NIPP Base Plan to each sector and hopes to make progress on the sector specific plans. DHS worked with the chemical sector on their sector specific plan recently at their security summit. DHS is also working on the nuclear sector specific plan. Assistant Secretary Stephan concluded by thanking Chairman Nye, Vice Chairman Chambers, and the rest of the Council members for all of their great work.

Vice Chairman Chambers asked members if anyone had comments for the Assistant Secretary. He then told Assistant Secretary Stephan his comments mean a great deal to the Council. He referenced a recent meeting where the Council discussed researching and developing recommendations regarding insurance on critical infrastructure components. He asked the members to consider the issue for a new report topic. Vice Chairman Chambers asked for additional comments.

Hearing no additional comments, Vice Chairman Chambers introduced Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism. Ms. Townsend thanked the Chairman and Vice Chairman for allowing her to address the Council. She told the NIAC the President greatly appreciates all its hard work. The greatest indication of the Council's value is the frequency with which DHS implements its recommendations. The government cannot protect the country's critical infrastructure without an effective public-private partnership. Ms. Townsend said she learned this when the President asked her to perform the *Hurricane Katrina Lessons Learned* study. It became immediately obvious, particularly during a catastrophic event, there will be tasks the Federal government is not positioned to do. The NIAC is a wonderful ongoing example of this partnership working in a non-crisis environment, and the Federal government and private sector need to effectively cooperate in crisis situations. The government needs the help of the private sector to prioritize vulnerabilities because businesses make these decisions every day.

Ms. Townsend reminded the meeting participants the President signed an executive order on intelligence and information sharing in December 2005. Ms. Townsend is very interested in the recommendations of the Intelligence Coordination Working Group. She appreciates that from what she has seen of the draft recommendations, they support the President's intelligence sharing agenda. The Council's research of this topic will help the Program Manager of the Information Sharing Environment at ODNI, Ambassador Ted McNamara. Ms. Townsend described the intelligence coordination effort as a long tedious process. She thanked the Council for its work on the Intelligence Coordination Report.

Ms. Townsend stated she anticipated hearing the status report of the Physical and Cyber Convergence Working Group. She told the Council that Congress expressed interest in the topic. She then thanked the Council for its work on Chemical, Biological and Radiological Events and Critical Infrastructure Workforce study. This is another one of those issues where there is only so much that the federal government can do. The President needs the help of the private sector to accomplish his goal of protecting the country.

Ms. Townsend concluded by reiterating her comments about the implementation of the Council's work. The Council's work on Sector Partnership Model Implementation and the Risk Management

Approaches to Protection have greatly affected recent DHS policy. The Sector Partnership Model helped Secretary Chertoff develop the CIPAC. The Council's recommendations have also helped Assistant Secretary Stephan with the NIPP's development. She said they do not simply read the reports, they use the recommendations to implement policy. Thus, DHS and the White House take the work of the NIAC very seriously. She again thanked the Council for letting her speak with them.

Vice Chairman Chambers thanked Ms. Townsend for taking time to speak with the Council. The Vice Chairman stated that open communication between the Federal government and the private sector is mutually beneficial.

Ms Townsend agreed, saying that creating collaborative environments was one of the lessons learned from Hurricane Katrina. In situations where work must get done immediately, it will be helpful for the communications between the government and the private sector to route through field command centers where individuals have the authority to provide information to everyone needing it, instead of just a central command. Ms. Townsend said President Bush and the Homeland Security Council are working toward creating this. Vice Chairman Chambers thanked Ms. Townsend and turned the floor over to Chairman Nye for the approval of the April meeting minutes.

IV.	**APPROVAL OF APRIL 11, 2006 MINUTES**	NIAC Vice Chairman, *John T. Chambers* Presiding

Chairman Nye thanked Vice Chairman Chambers. He asked the Council if there were any questions or comments about the minutes. Hearing no corrections or comments, he asked for a motion to approve the minutes. A motion was provided, seconded, and unanimously approved.

Chairman Nye asked Vice Chairman Chambers to introduce the Final Report of the Intelligence Coordination Working Group.

V.	**FINAL REPORTS AND DELIBERATIONS**	NIAC Vice Chairman *John T. Chambers* Presiding
	A. INTELLIGENCE COORDINATION,	NIAC Vice Chairman *John T. Chambers*, President and CEO, Cisco Systems, Inc.. and *Gilbert Gallegos*, Chief of Police (ret.), Albuquerque, New Mexico Police Department, NIAC Member

Vice Chairman Chambers thanked Chairman Nye and asked Chief Gallegos to join him in the presentation of the Intelligence Coordination Working Group's Final Report and Recommendations. He thanked the Chief for his hard work as the Working Group's co-chair. He also thanked Mr. Kenneth Watson from Cisco Systems, Inc. and the NIAC Secretariat for their hard work. He went on to express his gratitude to all those involved in the Working Group, especially Mr. Alfred Berkeley for his help with the CEO interviews. Mr. Berkeley interviewed several critical

infrastructure CEOs, which provided helpful input as the Working Group developed its overall view. Vice Chairman Chambers told meeting participants the Working Group will present the recommendations at the meeting and will have the final report ready in a few weeks. He asked Chief Gallegos and Mr. Berkeley if they had anything to add.

Chief Gallegos thanked the Vice Chairman for allowing him to co-chair this important Working Group. He told the meeting attendees he spent a great deal of time in law enforcement, but this Working Group allowed him to better understand how the intelligence community works with the private sector. Additionally, his law enforcement experience enabled him to notice tremendous recent strides made toward effective intelligence coordination. He then thanked DHS for its efforts in improving public-private information transfer. He also thanked Mr. Watson, Mr. Berkeley, and the Vice Chairman for their efforts on the project.

Mr. Berkeley added that it was an incredible effort by a large number of people from both the private and public sectors. He asserted the Working Group did a great job, and its work will benefit the country.

Vice Chairman Chambers thanked Mr. Gallegos and Mr. Berkeley. He told the participants the Study Group for this topic brought together over 30 experts from both the intelligence community and the private sector. The Study Group approached the task as they would approach a business problem: they began with a purpose statement and broke it down into individual issues. They looked at the topic of sharing the right information with the right people, while keeping critical infrastructure protection in mind. The decision quality at both the executive and operational levels depends upon the information quality provided to the decision makers. The Working Group found early in their research the sectors are very interdependent. Vice Chairman Chambers asked Mr. Watson to provide the specific findings and recommendations of the Working Group to the Council.

Mr. Watson thanked the Vice Chairman as well as Ms. Gail Kaufman and Mr. Robert Beecher, contractors with DHS, for their efforts in pulling together the multiple Study Group reports. He thanked Cisco Systems' Ms. Robin Roberts for her work on the private sector side of the report. At the operational level, Mr. Watson said the Working Group began by defining the problem and concentrating on two key questions. The Study Group held four in-person workshops and weekly conference calls to pull together the recommendations. The Study Group also conducted case studies on four recent information-sharing events to refine the group's findings. Finally, Mr. Berkeley added the CEO interviews to capture the strategic executive level perspective. After this, the Working Group pulled Study Group inputs together and developed findings and recommendations.

Mr. Watson told the meeting attendees the term "information sharing" is overused, poorly defined, and therefore poorly understood. Information sharing holds different meanings for different groups. The Study Group decided to include a definition of information sharing specific to this study to clarify its meaning in the report. There is operational information sharing, which addresses incident managers, tactical decisions, and situational awareness; and there is strategic information sharing, which refers to relationships between CEOs and senior intelligence executives as they move toward long-term resource allocation and investment decisions. Information sharing, preparation,

prevention, mitigation, response, recovery, and restoration all cover the protection effort spectrum. At the first workshop, the Group asked:

- What are the private sector and intelligence community's information needs?
- What kind of information do they already possess?
- What information can each side provide?
- What are the roadblocks?

Study Group members were then asked to write issue papers on specific topics derived from these questions.

They again found differences in vocabulary and standard practices. For example, Mr. Watson stated some private sector groups use the term "confirmed," while the intelligence community rarely does. "Originator Control" also creates problems in sharing information. There were specific examples where DHS wanted to share information with certain groups, but were prohibited from doing so because they were not the originators of the information, and therefore needed to ask permission of the originators. DHS could eventually deliver the information after approval by the originators, but this process delayed the ability of the Department to inform those needing the information.

The lessons learned from the case studies supported the Study Group members' issue papers and added more understanding to each topic. From the blackout, the Group learned the Information Sharing and Analysis Center (ISAC) network effectively shared and disseminated information, especially during the US-Canada joint cyber investigation. The London subway bombing case study reiterated this. Lessons learned from the financial services threat include repositioning sector coordinating councils (SCCs) and the Partnership for Critical Infrastructure (PCIS) to be near the top of the alert warning priority list. Not only can industry experts identify unwarned collocated facilities, they should also be best positioned to know the occupants and managers of named buildings. The public transit alert example highlighted progress since the first of the case studies used. Sharing timely, effective information with the appropriate people vastly improved in the two years separating the first and last case studies. Mr. Watson said the Group found poor that incomplete information on consequences affected the quality of decisions by some incident managers. One example of this was a key decision to turn cell phone capability in tunnels due to a bomb threat—this removed potential triggers for bombs but also any warning or communication ability to evacuate people should an incident occur. Mr. Watson then turned the floor to Mr. Berkeley.

Mr. Berkeley said the Working Group formally interviewed about a dozen CEOs. He said he also had informal discussions with another 18 to 20 critical infrastructure CEOs. Mr. Berkeley's interviews resulted in multiple findings, including the importance of resiliency. The private sector and government cannot protect against everything. Additionally, the CEOs understood the Federal government cannot single-handedly protect all critical infrastructure; it needs the help of the private sector.

Vice Chairman Chambers thanked Mr. Berkeley and Mr. Watson for their presentations. He stated if the private sector had better access to the information or understood why the government asked for certain information, they would be better able to provide the specific help needed. He told the

Council that although executives are more willing to share information with those they know and trust, it's important to develop an architectural approach to institutionalize that trust and minimize dependence on personalities that may come and go.

The Vice Chairman moved to the Working Group's recommendations. Mr. Chambers said CEOs must better prioritize resource investments to benefit from more strategic information relationships. Law binds companies to protect employee privacy. However, if an insider is found to be a terrorist or another criminal, executives can be held accountable.

Mr. Berkeley said CEOs wished to communicate with government officials who have the same decision-making authority. They believe they can work best with senior intelligence officers to find out what assistance their sector or company could provide. Mr. Berkeley said CEOs are willing to invest time and corporate resources to educate analysts with thorough, industry-specific knowledge of their industry. This would help the government have a better understanding of each sector's point of view.

Vice Chairman Chambers said implementing the Working Group's recommendations would take time and effort, but he is confident that the government will agree with the recommendations and work to implement them. The private sector and Federal government have made progress, but there is still no overall national capability to fuse all-source information. Additionally, the government and private sector need to establish state-by-state and national awareness. DHS created the sector specialist role within the Department. The Working Group commends this approach and recommends expanding it. The Intelligence Coordination Working Group recommends all intelligence agencies involved in critical infrastructure protection provide information at operational and executive levels. Ongoing training and career development should be built into the sector specialist role, because, without current skills, their ability to interface with their private sector counterparts could grow stale. The private sector needs a repeatable process to request and receive information from the intelligence community. Vice Chairman Chambers asked Ms. Susan Reingold, Deputy Director for the Information Sharing Environment at the ODNI, to comment on the Intelligence Coordination recommendations.

Ms. Reingold thanked the Chairman, Vice Chairman, and the members of the Council. She began by saying the Intelligence Reform and Terrorism Prevention Act of 2004 established the office of the Program Manager for the Information Sharing Environment at ODNI and provided it with government-wide authority. While the office is housed in ODNI, they have government-wide authority to coordinate, implement and manage the terrorism information-sharing environment. Ms. Reingold told the group the information-sharing environment is actually a collection of processes, protocols, and systems supporting the sharing of terrorism information among federal, state, local, and tribal governments and private-sector entities. It is designed to support all those responsible for preparing and protecting communities from terrorism and responding should an attack occur. The Program Manager's purpose is to utilize existing resources and systems already in place.

Ms. Reingold then addressed the work of the Intelligence Coordination Working Group. She believes the recommendations are valuable and will make a difference. The CEO perspectives provide specific data, not just anecdotal data. Additionally, the four case studies provide a private-sector perspective of each of these potential critical infrastructure crises.

She said the report clearly articulated the problems with the current system, while providing analysis and specific recommendations to remedy each problem. The Working Group also recognizes the similarities between the views of the state and local governments and the private sector, which actually allows for the identification of solutions that can be applied across state, local, tribal, and the private sector with the understanding that there are a number of solutions that are going to have to be tailored to specific sectors. Ms. Reingold said the Working Group's recommendations emphasized the importance of creating and maintaining trust. She agreed trust would help solve many of the problems preventing effective intelligence coordination. Ms. Reingold said her office anticipated working with the NIAC and with other members of the CI/KR sectors through the CIPAC. She thanked the members of the Council and told them she looked forward to future interactions.

Chairman Nye thanked Ms. Reingold for her comments and told the Working Group he appreciated its hard work on this important topic. He said he believed the report is an outstanding work product. He noted there needs to be a few minor changes made to the report before it can become final, but the changes will not affect the recommendations.

Vice Chairman Chambers asked for a motion to accept the recommendations of the Working Group. He received a motion that was seconded. The motion carried unanimously.

VI	**STATUS REPORTS ON CURRENT WORKING GROUP INITIATIVES**	NIAC Vice Chairman, *John T. Chambers* Presiding
	A CONVERGENCE WORKING GROUP	*George Conrades*, Executive Chairman, Akamai Technologies, NIAC Member, *Margaret Grayson*, President, Grayson and Associates, NIAC Member, and *Gregory A. Peters*, Former President and CEO, Internap Network Services Corporation, NIAC Member

Vice Chairman Chambers introduced the Convergence Working Group status update by asking Ms. Margaret Grayson and Mr. Greg Peters, two of the Working Group Chairs, to take the lead on the presentation.

Mr. Peters thanked the Chairman and the Vice Chairman. He then thanked the Convergence Study Group for its diligence thus far. He began by telling the meeting attendees the Working Group is on track to complete its report and recommendations by the October 2006 deadline. The team held conference calls nearly every week since the effort began in October 2005. Numerous subject matter experts from the intelligence community, the private sector, and educational enterprises have presented their research to the team and significant progress has been made in defining and focusing the scope of the objectives and subsequent recommendations to ensure a positive impact.

Mr. Peters continued, saying Ms. Grayson would present the specific progress made to date and the Group's next steps forward, but first he would present an overview of the Working Group. The

mission of the Working Group is to investigate the important questions and recommendations regarding the protection of SCADA and process control systems from cyber security threats. In order to put this into perspective and provide a framework, the Group first defined five framework questions. The first question was security as an enabler:

1. How do we position cyber security as a contributor and an enabler to achieving reliability, availability, and safety goals for the management of SCADA and process controls systems?
2. What are the market drivers required to gain industry attention and commitment to research and product development?
3. How do we best generate executive leadership awareness to assist in creating a culture and an environment that values the protection of SCADA and process control systems from cyber threats?
4. What are the appropriate federal government leadership roles and priorities in identifying threats, vulnerabilities, risks, and solutions?
5. What are the obstacles and recommendations for improving information sharing about process control systems and SCADA threats, vulnerabilities, risks, and solutions? Mr. Peters then asked Ms. Grayson to present specific details of the group's recent actions, observations, and next steps.

Ms. Grayson thanked Mr. Peters**.** She began by saying the Group must lay out a path allowing them to consolidate and move the recommendations forward towards drafting the final report. The information gathered and the work performed over the last three months allowed the Group to drill down into some of the critical framework questions. The Group's work included reaching out to multiple organizations and subject matter experts, some of which came from within DHS. The Group had the chance to reach out to executives at the Process Control Systems Forum in June. This gave the Group an understanding of the needs, requirements, and necessary environments for a comfortable level of communication between private industry and the government. Much of what the Group learned is that these process control operators and managers have shareholders and profit requirements. As operators of very critical systems, they recognize the impact of downtime in an environment that must operate continuously. These owners/operators want to help, but need assurance the government understands their need for a platform based on trust, anonymity, and the ability to come forward with sensitive information that can make these systems stronger, more secure, and safer. The Group developed a questionnaire for outreach into the control systems community that allowed the Group to consolidate the initial outcomes into nine specific recommendations. One of those recommendations looks at an outreach format with the University of Georgia, Department of Risk Management. Ms. Grayson said Mr. Peters would be able to explain this area and provide some information about the Malcolm Baldridge Award.

Mr. Peters said the Department of Commerce's National Institute of Standards and Technology manages the Malcolm Baldridge Award Process and Program. The Baldrige Award is given by the President of the United States to businesses—manufacturing and service, small and large—and to education and health care organizations that apply and are judged to be outstanding in seven areas: leadership; strategic planning; customer and market focus; measurement, analysis, and knowledge management; human resource focus; process management; and results. Not only do many Fortune 500 companies pay close attention to and also participate in the award program, many of the Fortune 2000 companies use its criteria to self-evaluate their own organizations even if they do not

participate in the evaluation. In addition, sixty-nine global and national organizations use the Malcolm Baldridge criteria as a model for their own evaluations. This program has significant and global influence. Through the Working Group's interaction with the University of Georgia's Terry School of Business, they identified the Dean, Dr. George Benson, as the Chairman of the Board of Overseers for the Malcolm Baldridge Award Program. The Working Group discussed its work with Dr. Benson and he embraced its goals. At a recent Board of Overseers meeting he suggested the Baldridge criteria be revised to include the Working Group's recommendations wherever possible. With the concurrence of the NIAC members, the Group intends to work closely with the Baldridge team over the next few months to ensure convergence security criteria is reflected in the next criteria revision planned for December 2006. Mr. Peters said the Working Group believes this effort would reflect serious U.S. government leadership as well as additional CEO awareness for this very important issue.

In framing the questions they used for CEO information gathering**,** Ms. Grayson said the Working Group was able to draw on the expertise of Mr. Scott Borg and the US Cyber Consequences Unit's work evaluating risks and consequences. This allowed the Group to take the framework and provide information for CEOs to use to establish a baseline for the convergence of both physical and cyber security. Ms. Grayson stated the Working Group can now take information they gathered and move forward in shaping final recommendations.

Ms. Grayson said the Working Group looks to government leadership for the ability to communicate, share information, and cooperate with systems the government is installing for threats and alerts in a way that will allow owners/operators to communicate safely and anonymously. The Working Group perceives that there is a desire for cooperation on the part of both the private sector and the government. Business and government best practices could be merged, and the Group hopes to work those into the recommendations. Additionally, information sharing in all sectors, both public and private, is critical. The desire to protect and make these critical infrastructures safe and secure is shared on both sides. Ms. Grayson stated the Group senses a need for collaboration, communication, and cooperation to ensure that systems function correctly. Many are public companies with regulatory and rate-based constraints, which provide unique parameters around how they manage customer requirements. Public utilities also must interact with the Department of Homeland Security for government requirements. In the next three months, the Group will consolidate gathered data and information to begin forming a final report. Ms. Grayson stated the Group plans to have the Final Report ready by the October 11, 2006 meeting.

Vice Chairman Chambers told the Convergence Working Group they had made significant progress on such a complicated issue. Vice Chairman said as technologies and industries converge, beginning to think about physical and cyber infrastructures as one as opposed to separate is the only way this issue can be addressed.

B CHEMICAL, BIOLOGICAL AND RADIOLOGICAL EVENTS AND THE CRITICAL INFRASTRUCTURE WORKFORCE WORKING GROUP

Chief Rebecca F. Denlinger, Fire Chief, Cobb County, Georgia Fire and and Emergency Services, NIAC Member, *Martha H. Marsh*, Chairman and CEO, Stanford Hospitals and

Clinics, NIAC Member, and *Bruce Rohde*, Chairman and CEO Emeritus ConAgra Foods, Inc.

The Vice Chairman then moved to discuss the Chemical, Biological and Radiological Working Group. He asked Ms. Martha Marsh and Chief Rebecca Denlinger to present a status update on their Working Group.

Chief Denlinger thanked the Chairman and Vice Chairman for the opportunity to present. Within the context of this update, she will provide some specifics on the body of work the Group has accomplished to date. The presenters will give more detailed indication of the problem statements assessed and provide some indication of the initial findings developed to this point.

Chief Denlinger said the CBR Working Group began by focusing on the higher probability biological threat. Within this context, they studied many aspects of biological threat and vulnerability scenarios and focused a portion of their resources and research on the potential impact of a biological event. These biological scenarios included a potential pandemic influenza outbreak, so the benefit of this is that the Group can leverage some of the work already accomplished to address the new topic of resource prioritization during a pandemic flu. She said Chief Gallegos offered his assistance to the Group, now that the Intelligence Coordination Working Group has concluded its work and presented its findings.

While the body of work accomplished to date will not completely apply to the new pandemic study, Chief Denlinger suggested elements of the work accomplished over the previous months retain some relevance and much of the primary research conducted as part of the assessment is directly applicable. The Chief said the CBR presentation will provide an overview of findings identified as part of the initial CBR study as well as the groundwork for the application and relevant findings within the CBR study to the pandemic Working Group. Chief Denlinger asked Study Group member Mr. Scott Blanchette to present the Group's overview.

Mr. Blanchette thanked the Chief and told the meeting participants the NIAC asked the Working Group to study the ability of the critical infrastructure worker to prepare for and respond to a biological event and assess the efficacy of the tools, training, and equipment supporting preparation, planning, response, and recovery efforts. Within this context, the NIAC tasked the Working Group to perform the following:

- Identify critical infrastructure personnel
- Identify biological emergency requirements
- Assess the current response to biological needs
- Identify planning, preparedness and response capability gaps
- Make recommendations to ultimately address these existing vulnerabilities.

To more clearly study the problem statement, the Study Group defined specific scope boundaries. The Study Group focused on biological awareness, preparedness, and planning efforts. They also studied tools, technologies, and training efforts that enhance response capabilities. While not

specifically identified in the charter, the Study Group also assessed service continuity and recovery capabilities. The Group did not focus on specific threats or threat vectors for two reasons:

1. The magnitude of the threat problems statement is a tremendous undertaking and would have consumed equally tremendous Study Group resources to more clearly articulate.
2. There are bodies outside of the NIAC with greater expertise, experience, and credibility within the world of biological threats and threat vectors that could and should take ownership of this question.

Finally, the Study Group opted to look at the biological problem from a strategic and tactical perspective, recognizing key interdependencies across all levels of the preparedness, planning, response, and recovery spectrums.

To focus Study Group efforts and develop some consistency across their sector-specific efforts, the Group gravitated towards the following questions:

- Do CEOs in the organizations have awareness, planning, and preparedness programs in place today?
- If the Group wanted to understand market incentives in order to invest in biological response preparedness, what financial metrics would they use to justify investments depending on the magnitude and seriousness of an event?
- Are there sufficient communications infrastructure in place to support response scenarios in a biological event?
- Has the Group looked at tools and technologies to support a response capability?
- Are the tools and technologies that are in place today effective or sufficient?

Next, the Study Group looked in some detail at the sufficiency of coordination between Federal, state, local, and private-sector entities. They surveyed respondents to address the question of what the federal government can do to encourage or facilitate enhanced preparedness or response capabilities. They used this to address key interdependencies. Interdependencies became a very key theme, because interdependency management is going to be a huge challenge at the Federal, State, and local government levels, as well as in the private sector. Finally they asked if there were three or four critical vulnerabilities facing organizations today.

Within the framework of these questions, the group was not as broadly represented as the Pandemic Working Group will need to be. They enjoyed fair representation across multiple critical sectors, though, especially in emergency services, telecommunications, and food and agriculture. In addition to the sector-specific focuses, the Group had a number of less linear contributors ranging from DHS and HHS to private-sector organizations to private companies to academia.

The Group identified three positive trends over the course of its study:

1. The Study Group found that this was not the first time that organizations had heard about a biological threat problem statement.
2. Organizational leadership has shifted its focus to identifying specific principals responsible for response and preparedness planning activities either as a primary or secondary function of their job.

3. Trendlines remain positive in terms of the number, frequency, and extent of biological planning and preparedness exercises on a national level. Sustained response capabilities in excess of 72 hours are highly dependent upon uninterrupted provisioning of electric, water utilities, and a functioning logistics infrastructure.

Many organizations surveyed indicated some degree of comfort in their ability to respond to a biological event for a short period, but the effort became increasingly complex and risky at longer intervals. The ability to deliver services directly correlated to the health and welfare of the responders and the providers. A common theme was concern for the health and welfare of responders' immediate family members. The Study Group also centered on communications. While industry has experienced significant improvements in its operability spectrum, there are still some risks in terms of responders and other interdependent entities. Regarding response coordination, a tremendous number of questions still exist today around who is responsible for what. Since the Study Group began its work, Assistant Secretary Stephan's organization has released a virtual library of new information addressing coordination questions.

Vice Chairman Chambers thanked the Group for their impressive progress and asked if there were any members willing to assist the Working Group in its efforts.

New NIAC member, Mr. Edmund Archuleta, volunteered to help the Working Group.

The Vice Chairman thanked the CBR Group for their hard work and flexibility. He asked if there were any comments before the meeting moved into new business.

Assistant Secretary Stephan told the Council DHS needs their help in rolling out the next phase of the NIPP. DHS is hoping for individually tailored plans for each sector by December 31, 2006. The Assistant Secretary asked the NIAC to provide sector leadership to help set each of the plans into motion.

Vice Chairman Chambers moved the discussion to NIAC new business, introducing a new Working Group topic.

VII	**NEW BUSINESS**	NIAC Chairman, *Erle A. Nye*, NIAC Members, *TBD*
	A. INTRODUCTION OF A NEW TOPIC: THE PRIORITIZATION OF CRITICAL INFRASTRUCTURE FOR A PANDEMIC OUTBREAK IN THE UNITED STATES	*Chief Rebecca F. Denlinger*, Fire Chief, Cobb County, Georgia Fire and Emergency Services, NIAC Member, *Martha H. Marsh*, Chairman and CEO, Stanford Hospital and Clinics, NIAC Member and *Bruce Rohde*, Chairman and CEO Emeritus, ConAgra Foods, Inc.

Chairman Nye began by telling the meeting attendees that President Bush recently unveiled the administration's National Strategy for Pandemic Influenza to begin preparing the country for a

possible pandemic. As with any risks facing the nation, including natural disasters or terrorist attacks, it is imperative all segments of society be prepared for such a serious threat. In June, Chairman Nye received a letter from Secretary Chertoff and HHS Secretary Michael Leavitt requesting the Council study and provide recommendations on critical infrastructure prioritization for a pandemic. Secretaries Chertoff and Leavitt asked the Chemical, Biological and Radiological Working Group to suspend their current work and begin a study with the following desired deliverables:

1. Identifying and defining "critical services" that must be maintained in a pandemic;
2. Establishing criteria and principles for critical service prioritization;
3. Defining critical services priorities with principles for variation if necessary;
4. Identifying critical employee groups in each priority critical service;
5. Building a structure for communication and dissemination of resources; and
6. Identifying principles for effective implementation by DHS and HHS.

Given the importance of this study, the Secretaries have asked the newly formed Pandemic Working Group to complete its study by the October 10, 2006 NIAC meeting, where its recommendations will be presented. To assist the Working Group, a Study Group of subject matter experts will be utilized and to ensure that all critical infrastructures are represented, Chairman Nye asked the Partnership for Critical Infrastructure Security, through its Chair, Mr. Stuart Brindley, to provide subject matter experts for the study from each of the sectors. Further, he asked Mr. Duane Ackerman, Chairman of the National Security Telecommunications Advisory Committee (NSTAC), to provide subject matter experts. Both of these organizations have enthusiastically and positively responded.

Chief Denlinger, co-chair of the new Pandemic Working Group, asked Study Group member Mr. Scott Blanchette to present the framework for the Pandemic Study Group.

Mr. Blanchette told the Council the Working Group's charge is to make recommendations on critical infrastructure prioritization in an influenza pandemic event, which the Study Group is supporting. There is broad recognition that a severe pandemic could significantly affect the critical infrastructure and have severe negative economic, health, and social impacts. Secondly, there are existing countermeasures in place: for example, vaccinations; but supplies will be limited and prioritization of those supplies will be critical in any response scenario. Finally, defining priorities around this will allow the Group to better allocate those very limited resources and preserve some societal function and order in a pandemic event.

Mr. Blanchette said the Working Group broadened the participation in the Study Group to ensure that they have contributions from all of the critical infrastructure sectors. They have been working through the PCIS to ensure they have representation of all of the critical infrastructures. Also, as the Chair alluded to, Mr. Duane Ackerman from the National Security Telecommunications Advisory Council (NSTAC) provided some augmentation from its member companies. Finally, The Department of Health and Human Services has provided a number of subject matter experts on pandemic influenza. Another source of support for this initiative comes from multiple directorates within DHS. Through Chief Denlinger, the Study Group has been able to reach the state and local

level to provide subject matter expertise and contributions focusing on pandemic influenza, preparedness, and response scenarios at a state and municipal level.

To provide some context on the current pandemic scenario, there are three continents currently infected with the H5N1 Avian Influenza. As of June 20, 2006, there have been 228 documented cases with mortality rates exceeding 50 percent; current case mortality and morbidity rates are extremely high. Mutation recombination of genetic material poses some problems for those studying it as well. Complications in planning and response scenarios, stockpiling of available vaccinations, or applicable vaccinations becomes increasingly complex through this mutation. In a pandemic resembling the severity of the 1918 Spanish Flu, estimates surpass two million potential deaths in the U.S., not to mention numerous other extremely severe side effects. One of the other key data points within the contextual scenario is that absenteeism is expected to exceed 40 percent at the peak of infection across the critical infrastructure, clearly a point of immense concern for the Study Group. There are existing countermeasures currently in place--vaccinations do exist, they are ready for distribution, and many resources have been applied to building and expanding stockpiles. But again, recombination and mutation could reduce the effectiveness of current and developmental vaccines, making this an extremely challenging problem statement for the country. There are antiviral drugs and plans for social distancing to address infection control and health care measures as well.

Mr. Blanchette said the Group recognizes the new charter's timeline presents unique challenges. It is possible the magnitude of this question might be a trailblazing event for the NIAC.

Vice Chairman Chambers thanked Chief Denlinger and Ms. Marsh for taking on this responsibility. He believes they can accomplish their work in that time and doing so will benefit the Country.

Chairman Nye agreed with the Vice Chairman about the importance of the Working Group. He encouraged other members of the NIAC to become involved in the Group to include their sectors in the Pandemic issue.

VIII ADJOURNMENT

NIAC Vice Chairman, *John T. Chambers*

Vice Chairman Chambers thanked everyone for their contributions at the meeting. He offered a special thanks to DHS for continued support of NIAC their part in the public/private partnership. He thanked Chairman Nye and told the Council Chairman Nye would lead the next meeting in October. Vice Chairman Chambers then adjourned the meeting.

I hereby certify that the foregoing minutes accurately represent the discussion and events that transpired at the meeting held on the date first noted above.

By: /S/ Erle A. Nye_____ Dated: _10/10/06_____
Erle A. Nye, Chairman

ATTACHMENT A

Public-Private Sector Intelligence Coordination

National Infrastructure Advisory Council (NIAC)

Intelligence Coordination Working Group

John T. Chambers
President and CEO
Cisco Systems, Inc.

Gilbert G. Gallegos
Retired Chief of Police
Albuquerque, NM

Overview

- Purpose
- Guiding Principle
- Methodology
- Case Studies
- CEO Interviews
- Findings
- Recommendations
- Q&A

Purpose

- Improve coordination:
  - Between private sector owners/operators and
  - The Intelligence Community
  - To protect critical infrastructures

Guiding Principle: Diversity

- Critical infrastructure sectors have different:
  - Needs
  - Complexity
  - Regulatory environments
  - National boundaries
  - Organizations
- "One size fits all" solutions don't work well
- Nation benefits by allowing for sector differences
  - Architecture approach
  - Process-based trust relationships
  - Information protection

Methodology

- Big picture
- Individual issues
- Case studies
- CEO interviews
- Consolidated findings
- Recommendations

Big Picture

- How can the IC help critical infrastructures?
- How can critical infrastructures help the IC?
- "Information Sharing" at the core of the issue

Individual Issues

- Timeliness
- Requests for Information
- Classification
- Handling restrictions
- Understanding of sector uniqueness
- Collaborative analysis
- Existing mechanisms
- How to ask the right question
- Who are the decision makers?

Case Studies

- August 2003 Blackout
- July 2004 Financial Services Threat Alert
- July 2005 London Bombings
- October 2005 New York Public Transit Threat Alert

CEO Interviews

- Al Berkeley conducted
- Supported by Staff, Contractors
  - John Tritak
  - John MacGaffin
  - Gail Kaufman
- Valuable input
  - Executive decisions demand different information than operational level

Findings

- Trusted relationships key to successful information sharing
- Intelligence analysis often flawed due to lack of critical infrastructure expertise
- Getting information to the decision makers inconsistent
- Private sector information sharing mechanisms vary widely
- Protecting sensitive information vital to building trust
- No single clearinghouse for information
- No common process to request or receive information
- Classifications and inconsistent handling instructions impede information flow

Recommendations

- Develop senior executive information sharing architecture
- Clarify law: privacy vs. insider threat liability
- Leverage existing mechanisms
- Develop national-level information fusion capability
- Create “Sector Specialist” positions in intelligence agencies
- Train and develop “Sector Specialists”
- Develop formal, objective intelligence and information requirements process
- Standardize markings and handling instructions[11]

Questions and Answers

ATTACHMENT B

Convergence of Physical and Cyber Technologies
and Related Security Management Challenges

National Infrastructure Advisory Council (NIAC)

Convergence Working Group

Status Report
July 11, 2006

George H. Conrades
Executive Chairman
Akamai Technologies

Greg Peters
Managing Partner
Collective IQ Partners

Margaret Grayson
President, Grayson and Associates

Overview

- Purpose
- Status of *Next Steps* from Last Meeting
- Timeline
- Actions
- Directional Recommendations
- Next Steps

Purpose

- Mission: The Convergence Study Group will investigate important questions and make recommendations regarding the protection of SCADA and Process Control Systems from cyber threats.

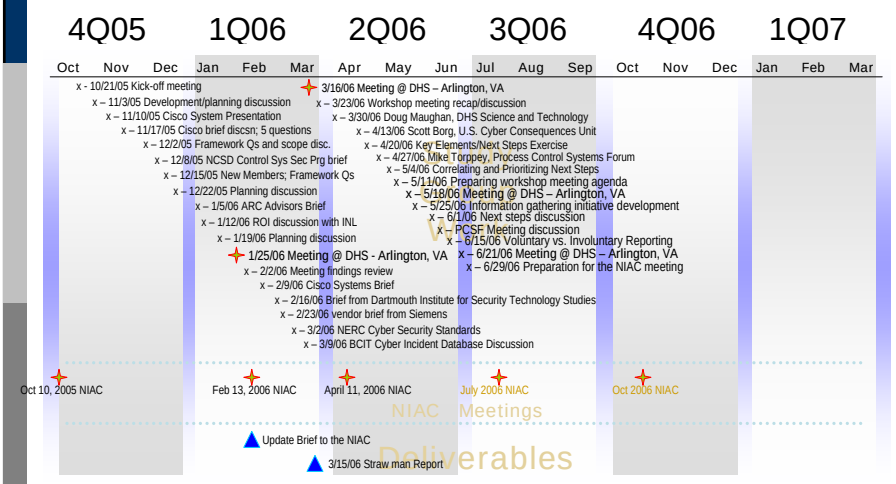
The Five Framework Questions

- ***Security as an Enabler*** **-** How do we position Cyber Security as a contributor and an enabler to achieving reliability, availability and safety goals in the management of SCADA and Process Control Systems?
- ***Market Drivers*** **-** What are the market drivers required to gain industry attention and commitment to research and product development?
- ***Executive Leadership Awareness*** **-** How do we best generate executive leadership awareness to assist in creating a culture and environment that values the protection of SCADA and Process Control Systems from cyber threats?
- ***Federal Government Leadership Priorities*** **-** What are the appropriate Federal Government leadership roles and priorities in identifying threats, vulnerabilities, risks and solutions?
- ***Improving Information Sharing*** **-** What are the obstacles and recommendations for improving information sharing about Process Control Systems and SCADA threats, vulnerabilities, risks and solutions?

Status of *Next Steps* from Last Meeting

- ✓ Address consequences element with Scott Borg, US-CCU
  - Integrated consequences into recommendation for improving Executive Leadership Awareness, informed discussions on Improved Information Sharing
- ✓ Conduct CEO information gathering
  - Attended Process Control Systems Forum Spring Meeting, interviewed eight executive level participants to validate initial findings
- ✓ Further develop potential recommendations
  - Identified 9 draft recommendations to address key elements/framework questions
- ✓ Consult University of Georgia Department of Risk Management
  - Collaborating with Malcolm Baldridge Award board of overseers to communicate SCADA/ PCS cyber security message.

Time Line



Actions

- Held 11 weekly conference call discussions with subject matter experts to address key issues identified during the discovery process
- Held third and fourth face-to-face workshop meetings at DHS
- Used the Five Framework Questions to identify key elements of the desired end states
- Developed process to interrogate the key elements of the framework questions
- Attended the Process Control Systems Forum Spring Meeting to gather executive level perspective on the study's initial findings
- Developed 9 draft recommendations for identified key elements

Directional Recommendations

- Executive Leadership Awareness:
  - Advocate the dissemination of information on threat, vulnerabilities and economic impacts to owner-operators, vendors and government executives in CIP
  - Recommending specific plan in final report based on findings
- Government Leadership:
  - Evaluate recommending a study to investigate the potential role of Sarbanes-Oxley in ensuring the protection of SCADA and PCS from cyber threats
  - Working with Malcolm Baldridge board of overseers to communicate SCADA/PCS cyber security message
  - Recommending that government R&D funding coordinate based on priorities identified by cross-agency CSIA IWG annual reports
  - Recommend funding to accelerate and promote Control Systems Security Program's Vulnerability Assessment Tool to improve owner-operators security posture

Directional Recommendations *(continued)*

- To Improve information sharing:
  - Recommend collection of incident data through protected, trusted mechanism with CERT/CC to provide for more accurate CIP risk assessments
  - Provide CERT/CC program with the necessary resources to rapidly ramp up their SCADA/Process Control Systems training and engineering consulting services needed to build the trusted relationships that will facilitate incident information sharing
  - To get the right information to the right people at the right time, recommend acceptance of and collaboration in efforts to develop the Congressionally-mandated and President-directed Information Sharing Environment.
  - Recommend drafting formal request to intelligence community (RFI) to assess the cyber threat to SCADA and Process Control Systems and communicate that information with Critical Infrastructure owner-operators

Next Steps

- Investigate outstanding key elements
- Investigate the role of the Malcolm Baldridge Quality Award in raising executive awareness and government leadership in security of SCADA and PCS
- Continue executive information gathering to validate draft recommendations
- Finalize recommendations
- Draft the Final Report for October submission to the NIAC

Discussion

- Questions?

ATTACHMENT C

Chemical, Biological and Radiological Events and the Critical Infrastructure Workforce

National Infrastructure Advisory Council (NIAC)

NIAC Chemical, Biological and Radiological Events and the Critical Infrastructure Workforce

Status Report
July 11, 2006

Martha H. Marsh
President and CEO
Stanford Hospital and Clinics

Chief Rebecca F. Denlinger
Fire Chief
Cobb County, GA Fire and Rescue

Bruce Rohde
Chairman and CEO Emeritus
ConAgra Foods, Inc.

Overview

- Objective/Scope
- Assumptions
- Key Questions
- Critical Sectors Represented
- Findings
- Transition to Pandemic Working Group
- Discussion

Objective and Scope

- **Objective:**
  - Provide recommendations for keeping those who work in and maintain areas considered Critical Infrastructure (CI) prepared for a biological event and ensure they have the tools, training, and equipment they need to identify, respond to, and recover from a biological emergency

- **Scope of the activity:**
  - Identify CI operating personnel and biological emergency requirements
  - Identify how needs are currently handled; Identify vulnerabilities in preparedness and response capabilities
  - Identify gaps and solutions

Assumptions

- Scope:
  - Will focus on biological preparedness, training, awareness, response processes, response tools and technologies, response coordination, etc.
  - Will focus on post-incident continuity and recovery capabilities
  - Will *not* focus on specific threats or threat vectors
  - Will focus on high-risk critical infrastructure, key inter-dependencies, and public-private sector linkages
  - Will address both strategic and appropriate tactical issues
    - Example: strategic awareness issue across an entire critical infrastructure sector vs. lack of tactical communications capability between local and state first responders

Key Questions

Focus on common set of data points to collect across critical sectors; contributes to trending/consistency

- Do CEOs and their organizations have employee awareness, preparedness and response training programs?
- Is there a market incentive to invest in biological preparedness and response programs?
- Is there sufficient communication infrastructure in place to respond to a biological event?
- What tools and technologies currently support your biological response capability?

Key Questions (cont.)

- What tools and technologies are currently insufficient and why do they not meet your requirements?
- Is there sufficient coordination between federal, state, local and private-sector entities?
- What can the federal government do to encourage or facilitate enhanced preparedness and response capabilities?
- What are key inter-dependencies in a biological event?
- What are the three or four critical vulnerabilities facing your organization today?

Critical Sectors Represented

- Critical sectors and leads include:
  - Fire/EMS
  - Food and Agriculture
  - Healthcare
  - Water
  - Finance
  - Communications
  - State and Local
  - Electricity
  - Information Technology
  - Commercial Facilities
  - Transportation

Findings

Findings that identified positive efforts or trends included:

- Finding #1: Awareness
  - Tremendous degree of awareness across all elements of the critical infrastructure, federal, state and local governments
- Finding #2: Organizational leadership
  - Multiple organizations dedicated leadership to biological event preparedness
  - Organization-wide preparedness activities being driven from highest levels
- Finding #3: Preparedness
  - Coordinated biological event response plans and exercises are becoming more commonplace.

Findings (cont.)

Findings that suggested preparedness and response risk included:

- Finding #1: Sustained Response
  - Sustained response (greater than 72 hours) efforts highly dependent upon uninterrupted provisioning of electric and water utilities and functioning logistics infrastructure
- Finding #2: Health and Welfare
  - Ability to deliver services correlates directly to health and welfare of responders and providers
  - Health and welfare of family members of particular concern
- Finding #3: Communications
  - Opportunities exist to improve communications capabilities and processes between responders and inter-dependent entities (i.e. law enforcement, transportation, emergency response, utilities, etc.)

Findings (cont.)

- Finding #4: Response Coordination
  - Federal, state, local and private sector response efforts require greater, and more detailed levels of coordination and planning
- Finding #5: Logistics
  - Logistical support for biological events remains a concern
  - Specific questions around vaccinations, resource delivery, and prioritization of services requires greater study and definition
  - Concerns exist around logistical surge capacity

ATTACHMENT D

Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States

National Infrastructure Advisory Council (NIAC)

Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States Working Group

Status Report
July 11, 2006

Martha H. Marsh
President and CEO
Stanford Hospital and Clinics

Chief Rebecca F. Denlinger
Fire Chief
Cobb County, GA Fire and Rescue

Bruce Rohde
Chairman and CEO Emeritus
ConAgra Foods, Inc.

NIAC Charge and Rationale

- Study and make recommendations on critical infrastructure prioritization for an influenza pandemic
- Rationale
  - A severe pandemic can significantly disrupt CI
  - Medical countermeasures (e.g., vaccine) can protect CI but supplies are limited
  - Defining priorities can lead to optimal use of limited resources and best preserve societal function in a pandemic

Charter

- Six specific pandemic questions
  - Identify and define “critical services” that must be maintained in a pandemic;
  - Establish criteria and principles for critical service prioritization;
  - Define critical services priority (with principles for variation, if needed);
  - Identify critical employee groups in each priority critical service;
  - Build a structure for communication and dissemination of resources; and
  - Identify principles for effective implementation by DHS and HHS

Study Group Contributors

Representatives From:

- Each Critical Infrastructure Sector
- National Security and Telecommunications Advisory Committee
- Department of Health and Human Services
- Department of Homeland Security
- State and local government

The Current Pandemic Context

- Pandemic threat
  - Three continents affected by H5N1 avian influenza
  - 228 human cases and 130 (57%) deaths (as of 6/20/06)
  - Mutation or recombination of genetic material between avian and human influenza could induce pandemic
- Potential pandemic impacts
  - ~2 million U.S. deaths if 1918-like severity
  - Societal and economic disruption – up to 40% workplace absenteeism assumed at pandemic peak

Current Pandemic Response Measures

- Vaccination
- Antiviral drug treatment and prophylaxis
- Community measures
  - Social distancing (e.g., close schools, telework, etc.)
  - Infection control & personal hygiene (e.g., masks, hand hygiene)
- Quality health care

NIAC Working Group Timeline

- June 27, 2006
  - Convened pandemic study group with revised charter
- October 10, 2006 NIAC Business Meeting
  - Present Findings and Recommendations
- January 16, 2007 NIAC Business Meeting
  - Finalize Report and Recommendations

Discussion

Questions?