NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING AGENDA

Tuesday, April 11, 2006
1:30 – 4:30 p.m. ET
The Grand Hyatt at Washington Center
1000 H Street NW
Washington, DC 20001

I.	**OPENING OF MEETING**	*Jenny Menna*, Designated Federal Officer, NIAC, Department of Homeland Security
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. *Kenneth Rapuano*, Deputy Homeland Security Advisor *Robert Stephan*, Assistant Secretary, Office of Infrastructure Protection, Department of Homeland Security (DHS)
IV.	**APPROVAL OF FEBRUARY MINUTES**	NIAC Vice Chairman *John T. Chambers*
V.	**FINAL REPORTS AND DELIBERATIONS**	NIAC Vice Chairman *John T. Chambers* Presiding
	A. WORKFORCE PREPARATION, EDUCATION AND RESEARCH	*Alfred R. Berkeley III*, Chairman and CEO, Pipeline Trading, LLC., NIAC Member *Dr. Linwood Rose*, President, James Madison University, NIAC Member
	B. DELIBERATION AND APPROVAL OF RECOMMENDATIONS OF FINAL REPORT	*NIAC Members*
VI.	**STATUS REPORTS ON CURRENT WORKING GROUP INITIATIVES**	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
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.
C. CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT CHALLENGES	*George Conrades*, Executive Chairman, Akamai Technologies, NIAC Member, *Margaret Grayson*, President, AEP Government Solutions Group, NIAC Member, and *Gregory A. Peters*, Former President and CEO, Internap Network Services Corporation, NIAC Member.
VII. NEW BUSINESS	NIAC Vice Chairman *John T. Chambers*, NIAC Members TBD
A. DELIBERATION AND VOTING ON NEW INITIATIVES	*NIAC Members*
VIII. ADJOURNMENT	NIAC Vice Chairman *John T. Chambers*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Vice Chairman Chambers, Mr. Berkeley, Ms. Grayson and Dr. Rose.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Chairman Nye, Mr. Davidson, Chief Denlinger, Mr. Gallegos, Ms. Marsh, Mr. Peters, Mr. Rohde, and Mr. Thompson.

MEMBERS ABSENT:
Mr. Barrett, Mr. Conrades, Lt. Gen. Edmonds, Mr. Hernandez, Commissioner Kelly, Mr. Noonan, and Mayor Santini-Padilla.

STAFF DESIGNEES PRESENT MONITORING PROCEEDINGS:
Mr. Frigeri (for Mr. Peters), Ms. Deb Miller (for Ms. Grayson), Mr. Muston (for Chairman Nye), and Mr. Watson (for Vice Chairman Chambers).

STAFF DESIGNEES MONITORING PROCEEDINGS VIA CONFERENCE CALL:
Mr. Baglien (for Mr. Rohde), Mr. Blanchette (for Ms. Marsh), Ms. Burns (for Chief Denlinger), Mr. Clyde (for Mr. Thompson), Mr. Holmes (for Mr. Davidson), Lt. Mauro (for Commissioner Kelly), and Mr. Rose (for Mr. Barrett).

OTHER DIGNITARIES PRESENT:
U.S. Government: Kenneth Rapuano, Deputy Homeland Security Advisor, 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 Deputy Homeland Security Advisor Kenneth Rapuano, Assistant Secretary for Infrastructure Protection Robert B. Stephan, NIAC Chairman Erle A. Nye, NIAC Vice Chairman John T. Chambers and all the members of the Council present or on the teleconference. She also welcomed the members' staffs and other Federal government representatives. Ms. Menna extended a welcome on behalf of DHS to the members of the press and public for attending. 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 fifteenth meeting of the NIAC and the second meeting of the year 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. *Kenneth Rapuano*, Deputy Homeland Security Advisor *Robert B. Stephan,* Assistant Secretary, Office of Infrastructure Protection, DHS

Chairman Nye thanked Ms. Menna and thanked all those attending. He told the group the NIAC continues to make great progress. Chairman Nye noted Secretary Chertoff's announcement forming the Critical Infrastructure Partnership Advisory Council (CIPAC). The NIAC's Sector Partnership Model recommendations provided the basis for the CIPAC, and the Council members should be proud of their work.

Due to his attendance via teleconference, Chairman Nye then asked Vice Chairman Chambers to conduct the remainder of the meeting.

Vice Chairman Chambers thanked the Chairman and expressed his appreciation to the members for all of the great work they have completed to date. He stated the NIAC's recommendations strongly impact policy implementation–the CIPAC is a perfect example.

Vice Chairman Chambers added the Council completed a study of one of the biggest challenges facing the United States: the preparation and education of the Nation's critical infrastructure workforce. He thanked Mr. Alfred R. Berkeley, III and Dr. Linwood H. Rose for their hard work and leadership throughout the project. In addition to the Workforce Report and Recommendations, three working groups would provide updates. Vice Chairman Chambers said he looked forward to hearing each of them.

Near the end of the meeting, the Council would discuss adding new initiative topics. Vice Chairman Chambers echoed Chairman Nye's commendation of Secretary Chertoff and the Department of Homeland Security (DHS) for implementing the NIAC's Sector Partnership Model. It facilitates private and public partnerships, leading to better coordination between the private sector and the government. He added that the Department asked the NIAC for a recommendation and then acted on it quickly. Vice Chairman Chambers asked Deputy Homeland Security Advisor Rapuano if he had any comments.

Mr. Rapuano thanked the Chairman, Vice Chairman and the members of the NIAC. He lauded the Council for their leadership, dedication and service and said the White House continues to appreciate the quality of the Council's reports and recommendations, such as the recent Sector Partnership Model Implementation and Risk Management Approaches to Protection. In early 2005, Secretary Chertoff asked the NIAC to assess the validity of the Sector Partnership Model proposed in the Interim National Infrastructure Protection Plan (I-NIPP). In response, the NIAC provided

timely advice and recommendations on the model's implementation and structure function. DHS incorporated the NIAC's Sector Partnership Model inputs along with the Secretary's request to execute Section 871 of the Homeland Security Act creating the CIPAC. The NIAC also assessed how private sector risk prioritization and management experience could guide critical infrastructure protection.

DHS is currently implementing the NIAC's recommendations to create and standardize cross-government risk management methodologies and mechanisms in the revised NIPP. Mr. Rapuano told the Council these examples display how NIAC recommendations have translated into significant benefits for the country. He said he looked forward to hearing the Workforce Preparation, Education and Research Working Group's Final Report and Recommendations. The President often stresses that national critical infrastructure protection requires a unique partnership between the government and the private sector. As shown in the aftermath of Hurricane Katrina and the London bombings, the private sector plays a pivotal part in effective preparation and response to natural disasters, as well as terrorist events. The government and private sector must continue to emphasize developing appropriate capability levels to address terrorist attacks and natural disasters. Part of the Homeland Security Council's *Hurricane Katrina Lessons Learned Report* resulted in the development of 125 specific recommendations to the President to better prepare the nation for catastrophic incidents. This preparation includes improving both public-private sector collaboration and the Federal government's utilization of private sector capabilities for both response and recovery efforts. He then stated the Federal government has not used all the private sector's unique capabilities and skills. The government realizes it must use these resources to protect the nation's critical infrastructure.

Mr. Rapuano added that the White House issued the National Strategy for Pandemic Influenza in November 2005. The combination of this effort and the impending release of the NIPP better prepares the nation and international community to fight a potentially devastating pandemic. DHS will release the NIPP and its sector-specific annexes, providing a better understanding of the risks, interdependencies, key nodes and systems of America's critical infrastructure. The NIAC must play an increasingly important role in lending key expertise to the study of these issues, both among sectors and between the physical and cyber elements of national infrastructure. Mr. Rapuano concluded his comments by thanking the Council on behalf of the President for their assistance and advice.

Vice Chairman Chambers thanked Mr. Rapuano for his comments and then asked Assistant Secretary Robert Stephan to provide the Council with any comments he may have.

Assistant Secretary Stephan thanked the Chairman and Vice Chairman for the invitation to speak at the meeting. He told the members of the Council many of the government's critical infrastructure accomplishments would have been impossible without the NIAC's hard work and leadership. The Assistant Secretary said the NIPP base plan is nearing completion, and the interagency policy coordination committee on critical infrastructure protection voted on and unanimously approved it. The Assistant Secretary said about half the comments received by the NIPP came from DHS' private sector partners, and the NIAC should take credit because they persuaded their colleagues to issue opinions on the NIPP Base Plan. Some key parts of the NIPP's final version are reflective of the NIAC's great energy and enthusiasm it poured into its earlier recommendations.

The Assistant Secretary stated the NIAC's recommendations for the Sector Partnership Model created something that did not previously exist in the public-private partnership. Like the NIPP Base Plan, the Federal government accepted the Sector Partnership Model as the roadmap DHS will follow. Assistant Secretary Stephan stated he spent time with each of the sector coordinating councils to discuss each sector's perspective. Additionally, Secretary Chertoff approved the CIPAC proposal, creating a framework for a sector partnership model with open collaboration between public and private sectors while allowing discussions that have very significant security implications. The Assistant Secretary then thanked the NIAC for their suggestion to develop such a model because it makes the collaboration between the private and public sectors easier.

Assistant Secretary Stephan discussed DHS' progress on NIAC's Risk Management Approaches to Protection implementation. The guidelines the members describe in the report now steer all the Department's risk management efforts. Their guidelines allow DHS to move their private sector partnership out to all infrastructure significantly affecting human life. They have used the nuclear energy and chemical sectors as pilots for the risk management approach. Their active collaboration is designed to develop and export risk methodologies, risk assessment tools and ensure they are commonly accepted by individual enterprises, associations and other private sector areas. For the first time, the risk management approach guided every infrastructure-related grant program that DHS has, and their actions in the infrastructure protection world are all risk-based. Because of the NIAC's recommendations, DHS made these progress-driving improvements.

He continued by saying DHS, in conjunction with its Federal, state and local partners and the White House, is working to prepare for the 2006 hurricane season. The Department is currently conducting tabletop exercises, planning events and operation pilots to work through the problems the Federal government experienced last year with Hurricanes Katrina and Rita. The Federal government must help the private sector restore critical infrastructures back to normal operation status and secure them in an uncertain security environment. The Assistant Secretary thanked the NIAC, saying the country was better prepared for these types of disasters due to the Federal government's relationship with the private sector. The NIAC members convinced many of their colleagues to meet with the government in an effort to further develop this relationship. Assistant Secretary Stephan told the Council he looked forward to hearing their upcoming recommendations and again thanked the NIAC for their work.

Vice Chairman Chambers thanked the Assistant Secretary for his kind words and said the Council appreciates their working relationship.

IV. APPROVAL OF FEBRUARY 13, 2006 MINUTES

NIAC Vice Chairman, *John T. Chambers* Presiding

Vice Chairman Chambers asked the Council if they were ready to move to the approval of the meeting minutes for the February 13, 2006 meeting.

The members concurred and Vice Chairman Chambers asked for a motion for approval. He received a motion and it was seconded. The NIAC unanimously approved the February 13, 2006 meeting minutes.

V.	**FINAL REPORTS AND DELIBERATIONS**	NIAC Vice Chairman *John T. Chambers* Presiding
	A. WORKFORCE PREPARATION, EDUCATION AND RESEARCH WORKING GROUP	*Alfred R. Berkeley III*, Chairman and CEO, Pipeline Trading, LLC., NIAC Member, *Dr. Linwood Rose*, President, James Madison University, NIAC Member

Vice Chairman Chambers opened the discussion on the Workforce Preparation, Education and Research Working Group's Final Report and Recommendations. The development of the nation's workforce is extremely important to critical infrastructure protection and in increasing the United States' global competitiveness. Vice Chairman Chambers said he examined the Working Group's Final Report and Recommendations and believed the document provided very helpful and meaningful recommendations. The Vice Chairman then turned the floor over to Working Group Co-Chair Mr. Alfred Berkeley.

Mr. Berkeley opened by saying the Working Group divided the work into four sections. He asked each Study Group member responsible for a section to present their findings. Mr. Berkeley said the presentation will address the Working Group's mission, approach, findings and recommendations. The question the Working Group began with was how to assure adequate intellectual capital development to maintain both cyber and physical critical infrastructure. They looked at the need to understand whether Cyber Corps, a cyber-oriented federal scholarship program, was really efficient and effective. They studied the issue of whether research and development priorities appropriately emphasized cyber security. The Working Group researched how to enhance cyber security certification programs' usefulness; the idea of certifying a certain level of expertise to more effectively utilize talent and provide a greater market for trained people could ensure a designated knowledge level. Finally, the Working Group attempted to understand the broader issue of math and science competency in the workforce, leading to an examination of K-12 math and science education.

The Working Group and Study Group held weekly meetings for eighteen months, hearing from subject matter experts on one of the four issues in the original question. The Group used a few meetings to discuss and digest information previously delivered by subject matter experts. The Working Group used this expertise to develop a thorough set of final recommendations. They also used relevant research and theoretical academic papers, along with studies done by other commissions and government-sponsored groups that looked into the same issues. Mr. Berkeley turned the floor to Dr. Rose to discuss the topic of cyber security research and development.

Dr. Rose told the Council the Working Group developed five recommendations for the cyber security research and development section. In regards to cyber security research and development,

the Working Group first addressed the need to establish consensus on cyber security research-related national priorities. Various federal agencies attempted to articulate research priorities, but efforts appear fragmented and disjointed. No one organization has established national research and development priorities, and the Working Group believes this is necessary to consistently communicate the most critical needs and signal where research should be directed so enterprises might more effectively and efficiently respond to those needs. Dr. Rose stated the Working Group found it difficult to determine the amount of financial resources needed for cyber security research. Without one source of funding-initiative-related information, and partly because the subject itself is ill-defined, it is difficult to accurately allocate expenditure data.

Funds directly go either to agencies, or the National Science Foundation (NSF) research projects allocate them. Estimates of cyber research expenditures vary considerably, ranging anywhere from sixty to one hundred fifty million dollars. Questions have emerged about cyber-based research around a balance between classified and unclassified, fundamental and applied research and between short-term and long-term. Current research efforts reflect post-9/11expectations, and the balance of research activity is skewed to shorter-term agency-driven research. For example, only twenty percent of National Security Agency (NSA) expenditures are devoted to long-term fundamental research, and only six percent extends to academic research. Approximately one third of advanced research and development activity goes to academic research.

Interviews and reviewed reports generally support additional funding, and during fiscal year 2004 and 2005, DHS earmarked $18 million toward cyber security efforts. Budget proposals included $73 million to enhance DHS programs and its National Cyber Security Division (NCSD) for FY06, while $94 million was provided for National Science Foundation cyber security research, education and training investments. If the Federal government can establish national research priorities, as the Working Group recommends, the government could complete a needed funding gap analysis to gain a clear research allocation picture. Affordability, demand, the legal implications of intellectual property protection and the classified nature of research products all affect this timeline. Dr. Rose stated the Working Group determined more effort must be devoted to better understanding how to advance time-to-market dynamics. The study concluded the released research solicitations seem to see a sufficient number of responding proposals. Dr. Rose expressed the Working Group's belief that if cyber research priorities are clear, if those needs are adequately resourced and if the funding is continuous rather than sporadic, the research community will respond and the available talent pool will grow.

Although not initially identified as a point of concern, a requirement exists for the creation of a national coordinating entity or validation of a current body like the cyber security and information assurance interagency working group. There is not a Presidential or Congressional coordinating body for that role. Homeland Security Presidential Directive-7 (HSPD-7) gives DHS responsibility for critical infrastructure cyber security under overlapping leadership with other bodies on cyber security issues. Leadership turnover has also complicated the coordination issue.

The Working Group recommends developing a national research agenda prioritizing cyber security research efforts to include the following areas:

1. Reduced vulnerability to cyber attack through additional research, software assurance security protocols and security metrics; reduced damage and recovery time from attacks through additional research, monitoring, intrusion detection, attack response and recovery, cyber forensics and reduced vulnerability through the promotion of cyber security awareness and training.
2. Increase the critical infrastructure and cyber security related research funding base. Adequate and predictable funding of a national cyber security research plan will attract a research talent pool and enhance national security.
3. Conduct additional studies to find solutions for increasing cyber security research products' time to market.
4. Ensure an adequate talent pool by increasing and stabilizing funding for fundamental research in unclassified cyber security.
5. Designate a coordinating body to oversee cyber security research efforts.

Mr. Berkeley then asked Study Group member Mr. Rick Holmes to shift to the topic of the Cyber Corps or Scholarship for Service (SFS) program's efficacy. This is an effective tool for the Federal government to educate cyber security professionals, but some adjustments could maximize the program's effectiveness.

The program's creators set out to establish an information assurance workforce capable of focusing on critical infrastructure protection. NSF annually budgeted Cyber Corps at $14 million in 2005 and $10 million in 2006. More than 600 students received scholarships in exchange for serving in an internship program and working for two years at a Federal agency upon graduation. The program covers students' scholarships, room and board, all additional fees and includes an $8,000 stipend for undergraduates and $12,000 stipend for graduate students. The Study Group developed recommendations for the program to improve the use of graduates, grow the number of graduates available for the workforce and ultimately result in improvements in the nation's critical infrastructure program. The challenges the Study Group found begin after graduation when students try to find internships within the Federal program. From student feedback, the Study Group discovered it is difficult to gain Federal employment. Lead agencies did not know the program existed and/or did not possess defined job descriptions matching the Cyber Corps program graduates. They also found the lack of billets dedicated to this program prevents agencies from offering jobs to these students. Additionally, more than half the program's students went to the NSA. While the NSA is important for information assurance needs, their role does not directly benefit critical infrastructure protection. In the next largest category, fifteen percent of the students went to work for the Department of Defense (DoD), another non-critical–infrastructure-protection unit. That leaves one third of the students graduating and working for Federal government agencies, responsible for protecting fifteen percent of the nation's critical infrastructure.

Mr. Holmes moved on to the DoD Scholarship for Service (SFS) program. Of the sixty-six NSA-designated Centers of Academic Excellence in Information Assurance Education (COAEs), twenty-six universities graduated students participating in the SFS program. The Cyber Corps program is similar to the SFS, but DoD administers its program differently.

There is also wide variability in costs among COAE universities participating in the scholarship programs. It could be up to four times more expensive to go to a private institution for a similar

degree than a state school. Because grants to schools are the same, regardless of the school's tuition rates, the Study Group believes it is possible to place more students in the program if they went to state schools. Finally, the difficulty in obtaining clearances concerns the Study Group; a clearance would require six to eighteen months once the work begins.

In the DoD program, agencies reserve billets for students coming from their own programs, enhancing the chances of students getting jobs they trained for. The security clearance process begins when the student enters the program, so that the graduates are cleared by the time they began work. Mr. Holmes also said that the final report recommends scholarship funding be either a flat or matching gift model. This idea suggests a costing model that sets an average cost across all institutions but only pays the actual cost up to that average cost. The more expensive schools then must make accommodations, or the students would have only partial scholarships in those cases. Some institutions could also have matching gift scholarships where the school would match the funds the government provided for each student for this program so more students could participate in the program. The Group developed its final recommendation in this section in an effort to make the security clearance process for these students similar to the DoD process. The security process would begin when the student entered the program, so upon graduation and the first day of employment, they would be cleared.

Mr. Berkeley then invited Study Group member Mr. Ken Watson to turn the Council's attention to certifications. The key question is whether current information assurance or security certification programs certifying individuals fills the need for critical infrastructure assurance? The Institute for Defense Analyses (IDA) had asked a similar question in its recent study. IDA reviewed more than one hundred and fifty private security certification programs and mapped them against the jobs DoD needed—there were two areas of recommendations. They identified the programs that matched knowledge, skills and abilities (KSAs) to DoD's needs and recommended there be joint certification with those privately administered programs recognized by the government. IDA also created six standardized position description fields, three in technical fields and three in managerial skills. All description fields have an entry level, a middle grade and then a senior level person. IDA recommended DoD standardize those six different position descriptions and then map them to the qualifying certification programs that provide appropriate KSAs.

Since the completion of the IDA study for DoD, DHS has taken on the task of adopting its recommendations to apply them across the Federal government, and is currently working with the Office of Personnel Management (OPM) to achieve that goal. The Study Group also sees a challenge in the governance structure of a certification program. If it is a private program, how can they get government influence to accredit these different private sector certification programs to apply for federal jobs? Mr. Watson told the Council the Group found the third challenge in a number of small testing issues. Some of the existing tests are subject to cheating, and they do not accurately measure the KSAs. There are new tools that are available to improve the entire testing process

Mr. Watson presented the recommendations for the certification section. The first recommendation is to follow through on the IDA recommendations and develop and maintain standardized information assurance position descriptions across the Federal government, including required and recommended KSAs for each of the three grade levels for technical and managerial fields.

Secondly, the government should designate a privately administered, public-private information assurance training certification body. Several exist in the private sector and the government can choose one. The Group does not recommend the government create a new one, but they should choose from the several that exist and designate that certification body with the administration of the certification programs for information assurance. Third, the Federal government needs to review the testing procedures and reform them to provide outcome-based, modular, computer-based testing and metrics. These new tools would provide for tracking mastery and allow for modular flexibility. A student can look at the modules they want to test. If they can demonstrate mastery at the beginning of the module, they will not need to take that part of the test and may skip to the next one, which makes testing much quicker. It also reduces the ability to cheat, because students have to demonstrate the knowledge to be able to select the right answer. The students would not have the option of looking at another person's answer on a piece of paper. Mr. Watson concluded his presentation on the certification recommendations.

Mr. Berkeley discussed the Kindergarten through 12th grade (K-12) Education section. The Working Group examined the international competitiveness of America's K-12 education and developed a recommendation. A globally competitive workforce is the foundation of long-term protection for the nation's critical infrastructure and economy. Global competition now sets minimum performance standards for American workers and the education establishment that trains them. The United States must implement internationally competitive standards. The Working Group examined how and what American children learn. Schools should teach facts, concepts and skills to make the workforce competitive. The scientific method prevalent in medicine, engineering and other disciplines should be applied to education. Converting schools over to this will create challenges. The Federal government has very little influence over education. By law, it may not dictate curricula or teaching methods. On the other hand, it can provide research, comparisons and analysis. Mr. Berkeley stated the Working Group wants to arm educational decision makers and parents with information on what works and what does not in educating children. The Group examined dozens of potential recommendations and talked to numerous experts, but came down to one recommendation: make American standards internationally competitive. To improve the nation's workforce, the United States must compare its programs with those of other successful nations. The Working Group believes tests should measure students' knowledge levels and determine if those levels are globally competitive.

Mr. Berkeley also explained the Group found a tremendous lack of curricula coherence, especially regarding its logical consistency. In the District of Columbia, for example, standards for kindergarten students require them to type, read and write before undertaking a particular math curriculum. This is totally backwards. This lack of coherence leads to unintended social consequences, particularly for those moving from district to district. Relocated students might not have the opportunity to excel because the sequence of math and science courses at one school may differ from another school. The Group looked at the issues of pedagogy, the methods teachers are taught in schools of education. They discovered a tremendous conflict in beliefs regarding "the right way" to teach a student. In both math and reading, should children learn more by rote and repetition or by self-discovery and exploration?

Mr. Berkeley told the Council the Working Group discovered one main recommendation with a number of sub recommendations for that section. They recommended the Federal government do

everything it can to assist the states in implementing internationally competitive education standards, nationally competitive curricula and internationally competitive teaching methods (pedagogies). To assist in this implementation, the Group wants to use the Federal government's ability to research and perform comparisons and analysis to bring out thorough comparisons and research the stark contrast between U.S. curricula and international curricula. The Working Group recommends the research determine the most effective international standards, curricula and teaching methods. This research should determine the strengths and weaknesses of those competitive curricula and compare each state's curricula to effective international curricula.

Mr. Berkeley stated that the Group's research found that many children could not enter collegiate math and science, because they do not possess the prerequisite information. The remediation process becomes too difficult so they opt out because they did not get the right sequence of logic, facts and concepts in elementary and high school. The Working Group feels American educators should test children against international standards. Educators should develop internationally competitive, low-risk self-tests children can take by themselves. This would allow them to get on the web and test themselves to determine their own knowledge level. They could get practice taking tests and understand their weaknesses.

Mr. Berkeley acknowledged a major conflict in this country between two different schools of thought on education, self-discovery versus the basic skills approach. In the self-discovery method, children find the meaning of words and mathematic and scientific rules through discovery. This process only works well for privileged children. The basic skills approach believes teaching America's children basic skills enables them to understand words, scientific facts and mathematical theory, knowledge benefiting society in the long run. The Working Group believes the Federal government should research which of these techniques works best in each region of the country. The government spent $600 million on this issue in the 1970s and discovered the best process for reading. They must find the optimal process for math and science.

The Group would like the government's research to examine textbooks. The textbook manufacturers meet the standards required of them by those who purchase them. Few subject matter experts review these textbooks to check their accuracy. One example was an American eighth-grade science textbook that had the equator running through Florida. If a geographer reviewed this book, this mistake would not have made it to publication. This Group also believes the Federal government should determine a curriculum's and teaching methods' global competitiveness.

The Working Group also found a tremendous amount of teacher education in teaching methods and teaching curricula has not proven to be effective or internationally competitive. Mr. Berkeley stated the Group sought research to determine whether states actually use research-based, No Child Left Behind-compliant curricula. The Working Group remains skeptical about the claims that some states use research-based curricula and pedagogy. A national education website should publish the results of this research to make the information broadly available not only to people in the educational decision-making process, but to parents and students. The Working Group also wants accountability mechanisms available to the Federal government. These mechanisms include federal funding incentives implemented to encourage individual school districts and teacher preparation programs to implement and achieve internationally competitive standards, curricula and teaching methods. Mr. Berkeley then asked for questions regarding the presentation.

Chairman Nye told the Council he was pleased with the work and that it was very well done.

Working Group member Ms. Margaret Grayson thanked Mr. Berkeley and Dr. Rose for their hard work and leadership.

Vice Chairman Chambers asked the Council for questions and comments.

Ms. Martha Marsh stated she is very happy with the work the Working Group provided to the Council.

Vice Chairman Chambers thanked Ms. Marsh for her input. These recommendations move the country toward an international competitiveness they need. Vice Chairman Chambers thanked the Working Group for a great product.

Chief Gilbert Gallegos motioned for the approval of the report and its recommendations. Ms. Grayson seconded the motion, and they voted unanimously to send the recommendations to the White House.

Assistant Secretary Stephan asked the Working Group for help as DHS finalizes the NIPP.

VI	**STATUS REPORTS ON CURRENT WORKING GROUP INITIATIVES**	NIAC Vice Chairman, *John T. Chambers* Presiding
	A INTELLIGENCE COORDINATION WORKING GROUP	NIAC Vice Chairman, *John T. Chambers*, President and CEO, Cisco Systems, Inc., and *Chief Gilbert Gallegos*, Chief of Police (ret.), Albuquerque, New Mexico Police Department, NIAC Member

Vice Chairman Chambers transitioned the conversation to the current Working Group initiatives and started with the Intelligence Coordination Working Group. He said this Working Group is currently in the finalization process, and it will present its report at the July meeting. Vice Chairman Chambers asked Chief Gallegos if he had anything to add.

Chief Gallegos thanked Vice Chairman Chambers. After many months of work by the Working Group and its Study Group, he believes the recommendations will cause the private sector and governmental agencies to assess their operational and strategic planning on how to handle intelligence information. Through the systematic exchange of intelligence information, government and the private sector will be prepared to handle this more effectively and avert critical incidents detrimental to homeland security.

Vice Chairman Chambers thanked Chief Gallegos and asked Mr. Watson to provide the details of the Intelligence Coordination Working Group's status update.

Mr. Watson thanked the Vice Chairman and told the meeting participants the purpose of the report really has not changed. In July 2004, the Working Group received the task of addressing challenges in information sharing and intelligence requirements definition and developing recommendations for federal policy changes. This breaks down to two simple questions the Working Group focused on for the entire study:

1. How can the intelligence community help the private sector?
2. How can the private sector help the intelligence community?

This process started with the big picture, breaking down each issue into its parts and then reassembling everything to develop findings, conclusions and recommendations. Mr. Watson stated the Study Group noted, like all other NIAC Study Groups before, the differences among the sectors. These differences will affect how each sector implements the recommendations. In the discussions about the inclusion of sector subject matter expertise and intelligence analysis, some sectors are very willing and do not have legal or other issues with stationing private sector representatives in government organizations to help provide analysis. Other sectors will not respond in that way. They may provide on-call people on the telephone or by email to answer questions from the intelligence community, but the Study Groups found sectors will respond to this particular issue differently. Despite the sectors' differences, national-level actions, in terms of overall architecture, will improve the security of all infrastructures and simultaneously allow for implementation differences. Mr. Watson discussed the importance of thinking of these recommendations in the context of critical infrastructure security steps as presented in the NIPP.

As someone thinks about information sharing between the private sector and the intelligence community, it is in the terms of deterrence, protection, preparedness, response and recovery. It is also important to remember there are decision makers at two distinct levels. Both need information from the intelligence community. Understanding how they will use the information will help identify what kind of information is needed. At the operational level, decision makers need information to respond to an incident or prepare for something in real time or near real time. At the CEO level, decisions are made to prioritize resources and make long-term investment decisions. CEOs have an awareness of a company or organization's daily activities, but there are two separate sets of decision makers dealing with problems either daily or on a long-term investment basis. The Working Group developed four findings, consistent throughout the study and reinforced by the CEO interviews.

Their first finding dealt with the fact that intelligence analysts and companies approach problems differently. The intelligence community and corporations use different languages, different vocabularies and different skill sets, so even the term "intelligence" means something different to an intelligence analyst than it does to a businessperson. Because of this, the Working Group decided to develop a glossary to accompany the report, so everyone reading the report could understand its language. There are also differences in understanding priorities. Mr. Watson used the example of the railroad derailer to make this point. Some intelligence analysts at one point thought the theft of a derailer is a big issue for the railroad industry, but when analysts discussed this with the railroad industry, they already had mechanisms in place to deal with the problem, relieving any issue. Thus, intelligence analysts do need access to private sector subject matter expertise.

In the Working Group's second finding, multiple government agencies and multiple levels of government each ask infrastructure owners and operators for the same information. Sometimes these requests originate from a single requirement. DHS may need to compile information, so it will ask the private sector and also ask the states. The states will ask the private sector for the same information, due to their requirements to provide that to the Federal government. Some critical infrastructure owners believe that once they provide information to the government, they never see anything happen to that information or find out its usefulness. Some infrastructure owners and operators do not know how to validate news reports of threats, because they do not know how to get information from the government to determine the accuracy of the information from the press. Even with the latest government reforms, the creation of the Director of National Intelligence (DNI) and National Counter Terrorism Center (NCTC), they have no single point of entry for the critical infrastructures to access either requirements or information from the intelligence community.

Third, the various markings and handling requirements prevent timely federal information sharing. Mr. Watson used the example of "For Official Use Only" (FOUO) to make his point. Different agencies define that differently. Some say the FOUO marking means prohibiting the delivery of documents with FOUO markings to foreign nationals, and others do not see the marking as a restriction, allowing foreign nationals to receive the documents. The Working Group will recommend the creation of a specific definition of FOUO along with other prohibitive document markings. Mr. Watson stated that an implication of not allowing foreign nationals to see certain documents is not allowing the key decision makers in some critical infrastructure companies. They need to find a way to get them the information if that is the case. Originator control has created another roadblock in the area of document marking. Sometimes DHS, or other departments need to get information to a particular infrastructure owner-operator, but they are prohibited because they have to go get permission from the originator of the information. This process has its merits, but it delays individuals from receiving sensitive information. Sometimes, this results in the individual receiving information too late to take appropriate action. The government should share certain information with the decision makers but still keep it from the general public because of some of the sensitivity of the information. This idea has developed into a problem because the government does not have a particular marking for that category.

In their fourth finding, the Intelligence Coordination Working Group discovered that the government's alerts and warnings do not often reach the right people at the right time. The system is much more inconsistent than it should be. The intelligence agencies need to work with local law enforcement or the new Critical Infrastructure Partnership Advisory Committee (CIPAC), which has a great awareness of each sector's decision makers. Mr. Watson emphasized this concept with the example of the raising of the threat level for five financial services targets in New York, New Jersey and Washington, D.C. Some members of the private sector believed other sectors needed notification because they shared a wall with some of those target areas or they had infrastructure running beneath the street at that same location. If an explosion occurred at one of those sites it would affect more than the named targets.

Mr. Watson told the meeting participants that the Study Group conducted case studies looking at four recent incidents to back up some of the findings and add specific data, and the Working Group will add the case studies to an appendix in the report. They looked at the August 2003 blackout, the

July 2004 financial services threat alert, the July 2005 London bombings and the October 2005 public transit threat alert. The Group found interesting similarities and differences in the four case studies. Two of these were post-event analyses, two were preventive warnings, three were related to actual or possible hostile acts and one was a non-hostile event, the blackout. The case studies covered the spectrum of risk and looked at pre- and post-event analysis. They all involved information sharing between intelligence and critical infrastructures. Mr. Berkeley led the effort to interview a number of critical infrastructure company CEOs to gain their perspective for the report. Mr. Watson asked Mr. Berkeley to describe his work on the CEO perspective interviews.

Mr. Berkeley told the meeting participants the Working Group asked him to do the CEO interviews to add the CEO point of view to the NIAC's Intelligence Coordination Report. He stated that the report had a great deal of work done on it to this point, but it did not have enough CEO input. The Group decided to have him engage CEOs and ask them questions such as:

- How have they changed their investment strategies?
- How have they changed hiring policies?
- How have they changed information sharing with the government?
- How do they interact with their board on these issues?
- Do they feel they had information that they could share but had never been asked?
- Did they have questions that they had asked that had never been answered?

Mr. Berkeley said he received interesting responses that the Working Group will include in the final report and recommendations of the Intelligence Coordination Working Group. Mr. Berkeley found that some CEOs have good working relationships with people in government, normally regulators. He found at least one major CEO in the food industry had been asked so many times by many different people for the same information and saw no results. This CEO decided he did not want to answer anymore until someone higher up in the Federal government asked him for the information. Mr. Berkeley said the Working Group wants to develop a mechanism for CEO interaction with the intelligence community based on trusted relationships. CEOs of companies need to know the principals in the intelligence community in some structured way that does not take too much time and begins to build some personal relationships. Mr. Berkeley found that throughout all of the interviews two main points came up every time:

1. The intelligence community and the critical infrastructure CEO must develop a personal, trusting relationship. The CEOs ask that they want to get to know the people with whom they would share this information. The dynamic of this relationship would make the CEO more comfortable and more willing to discuss issues.
2. These CEOs want to go directly to the person who has the right answer. They want to know, if they have a question, who to call that can get them an answer and not get them a runaround.

These CEOs will identify people in their company who can get very fast answers for the government as long as there is a real need for that. Mr. Berkeley also observed the CEOs' willingness to take intelligence community analysts on board and train them. He stated the Working Group found the whole classification model creates distraction and may be irrelevant. People want to interact with government without having to get many people cleared. They want to get to the

heart of the matter and typically do not care about sources. The CEOs just want to know what they need to do to protect their business and be resilient. Mr. Berkeley closed, stating some people may not feel the CEO surveys are necessary to the report, but after speaking with the CEOs, he feels they add an important dimension.

Vice Chairman Chambers thanked Mr. Berkeley for his update. The Vice Chairman concurred with Mr. Berkeley saying the CEOs will want their companies to participate and give the government information as long as they see that the information will be used constructively. He also stated the Working Group saw no need for additional federal funding to implement this group's recommendations. The Vice Chairman asked for comments.

Chief Gallegos described the importance of the implementation process. The Group will need the support of the NIAC because everyone has an interest in improving critical infrastructure's ability to deal with terrorist attacks and other incidents. He emphasized that the NIAC should follow up on the progress of the implementation because of its importance.

Vice Chairman Chambers asked if anyone had any questions or comments.

Assistant Secretary Stephan stated DHS has developed some new capabilities since the Intelligence Coordination Working Group began its study. Since the beginning of the Working Group, DHS has created their Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), which will address quite a few of the pieces of the puzzle that the Intelligence Coordination Working Group brought together in the briefing. The Assistant Secretary reminded the Council that the members of his office will ask the Working Group if DHS is effectively working to correct problems discussed in the Working Group's recommendations. The National Infrastructure Coordinating Center is working in concert with each of the sectors right now in preparation for hurricane season 2006. Assistant Secretary Stephan thanked the Working Group for their efforts on this very timely research project.

Vice Chairman Chambers told the Assistant Secretary the Working Groups developed an expertise on certain subject because of their extensive research. The Vice Chairman thought if the members of the Working Groups sit down with members of government agencies and other councils' working groups, then they could cut through a lot of the issues they have experienced.

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 A. Marsh*, Chairman and CEO, Stanford Hospitals and Clinics, NIAC Member, and *Bruce Rohde*, Chairman and CEO Emeritus ConAgra Foods, Inc.

Vice Chairman Chambers moved the conversation to the Chemical, Biological and Radiological (CBR) Events and the Critical Infrastructure Workforce Working Group.

Chief Rebecca Denlinger thanked the CBR Study Group for all the great work they have done. The Group has reached out to different sectors to see what they do to protect against these events. She asked Study Group member Mr. Scott Blanchette to give the Group's status update.

Mr. Blanchette said the Group is concentrating its efforts on preparedness, training, awareness, response, tools, technologies and response coordination. The Group expanded the scope to focus on post-incident continuity and recovery capabilities, which tends to be an area in terms of business continuity and recovery that many organizations have dedicated a tremendous amount of effort and assets. The CBR Study Group is not focusing its efforts on specific threats or threat factors. Mr. Blanchette said DHS, DoD, the Center for Disease Control, the Department of Health and Human Services, and a number of other federal organizations alongside their state and local counterparts are better prepared to address the threat and threat factor problem statement. The Study Group's efforts focus on response and recovery capabilities. The Working Group focuses on high-risk critical infrastructures as well as key interdependencies supporting those high-risk infrastructures. Finally, it will look at public-private sector linkages—connections that have become very evident in Study Group discussions.

The Study Group is looking at both strategic and tactical problem statements. From a sector-wide perspective, the Study Group is looking at strategic awareness across entire sectors. Many of their conversations return to tactical problems. Mr. Blanchette described a common set of eight key questions to collect data points the Study Group thinks will create an end state of some very articulate findings and recommendations.

1. What is the nature of CEO awareness, preparedness and response programs? Who leads this function? Are they enterprise-focused in nature or is this a person who has a very limited role within the organization? We have asked a number of CEOs and other leaders of corporations, "Are there industry leaders we should be talking to around biological event preparedness and response?" And finally, what lessons have they learned from that?
2. How are risk management decisions made? What assumptions go into that and what models are they using? What are the financial considerations that are going into this exercise? And are they seeing trends?
3. Is a sufficient communication infrastructure in place? How and through what channels are owners/operators informed? What role do the sector coordinating councils, ISACs or a number of other organizational representative bodies play in this type of event? Are some bottlenecks identifiable and could they help expediently distribute valuable information?
4. Are the tools and technologies for biological surveillance communications, event coordination, response and recovery sufficient? Do they meet the current requirements? If not, why?
5. How is coordination managed across strategic and tactical levels? What communications structure is in place to help facilitate that coordination?
6. What role will the Federal government play in a biological event? What role does the private sector envision the Federal government playing in a biological event?
7. How are interdependencies managed? Are they mapped out or well understood today? Through what channels are those interdependencies being managed? How are interdependencies or interdependent communications being managed?

8. What are the three or four most critical vulnerabilities facing an organization? What course of action have you outlined for that? Who owns it? Who is responsible within your organization for working that problem statement on a daily basis and what is that timeline? Is this something very strategic in nature that may take twelve to twenty-four months to realize the benefit of this activity, or is this something with a much shorter timeline?

Mr. Blanchette told the meeting participants by the time the Group begins formulating their findings, the list of questions will likely expand. He said the Study Group enjoys active participation from Fire and Emergency Medical Services providers, members of the Food and Agriculture, Healthcare, Water, Finance and Communications sectors, as well as state and local government contributors. He thanked Chief Denlinger for bringing so many experienced state and local government officials with plans, programs and communications infrastructure in place. Having this understanding from the state and local level is invaluable to the CBR Study Group. The Group engaged the electricity and information technology sectors, along with the recent additions of the commercial facilities and the transportation sectors.

Mr. Blanchette stated the Group recently sought more interaction with the National Guard to understand their role in a biological event. It has become increasingly apparent states will play an integral role in any large-scale biological event. The Study Group recently found many state National Guard resources have gone to Iraq and Afghanistan.

The Study Group found some organizations like Wal-Mart, FedEx and Home Depot who have sound biological preparedness and response programs; the Group will seek their contributions. Additionally, the Business Executives for National Security (BENS) conducted biological preparedness and response exercises recently in a major metropolitan area. The Study Group is working with them to not only understand the extent of that exercise, but also to understand lessons learned from the experience.

While the Study Group had not completed its data collection phase, they have sufficient data to create sound findings and thoughts on potential recommendations. The Group aims to have a complete set of findings and recommendations by June 1 to present to the Working Group and other NIAC members.

Mr. Blanchette asked if there were any questions or comments.

Ms. Marsh thanked Mr. Blanchette and said the Study Group found certain critical infrastructure groups need a different line of recommendations than those developed for the public.

Vice Chairman Chambers thanked Ms. Marsh, Mr. Bruce Rohde and Chief Denlinger for their leadership. He asked if there is sufficient communications infrastructure to respond to a biological event.

Mr. Blanchette said at an organizational level, the Study Group has just started a more tactical assessment of how organizations have prepared. Sector leads responsible for interfacing with key, sector-specific organizations better understand some of those challenges. The Study Group has not yet studied the remote telecommuter scenario, but there will be key findings from sector leads.

C CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT CHALLENGES WORKING GROUP

George Conrades, Executive Chairman Akamai Technologies, NIAC Member, *Margaret Grayson*, President, AEP Government Solutions Group, NIAC Member, and *Gregory A. Peters*, Former President and CEO, Internap Network Solutions Corp., NIAC Member.

Vice Chairman Chambers moved the conversation to the Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group. He called on Ms. Margaret Grayson to give the presentation.

Ms. Grayson thanked the Chairman and the Vice Chairman. The President, through the Council, has asked the Convergence Working Group to consider the questions surrounding the convergence of cyber security and the control of physical systems. As physical and cyber security converge, related technologies and network management of both consolidate. This Working Group continues to consider what actions might be taken by industry and the government to address these important areas and protect the nation's critical infrastructure. The scope for the Study Group includes supervisory control and data acquisition systems (SCADA) and also process controls systems (PCS).

The Working Group began by considering five key questions to frame the development of policy recommendations.

1. How can the country position cyber security as a contributor and as an enabler to ensure availability and safety goals in the management of SCADA and PCS?
2. What are the market drivers to gain industry attention and commitment to research and product development?
3. How might this Working Group best generate executive leadership awareness?
4. What are the appropriate federal government leadership roles and priorities?
5. What are the obstacles and what recommendations are needed for improving information sharing about PCS and SCADA systems, their threats, vulnerabilities, and risks, and what are the solutions?

Ms. Grayson stated that she and her fellow co-chairs, Mr. Greg Peters and Mr. George Conrades appreciate the active participation they have seen thus far in the Group. It has allowed the Group to make impressive progress. Ms. Grayson continued by saying the Group has completed all objectives they had identified as next steps at the previous meeting, and they have created a path to move forward. The Group still has a great deal of work to do and will continue to focus on actionable recommendations. Ms. Grayson asked Study Group member, Mr. David Frigeri of Internap, to present the details of the Study Group's actions.

Mr. Frigeri thanked Ms. Grayson and thanked the Council for allowing him to present. He introduced his presentation saying he would discuss the summary of the Study Group's

commitments from the last meeting, the timeline of the Group, actions thus far by the Group, as well as key observations they have made and next steps. The mission of the Convergence Working Group tasks them to investigate important questions and make recommendations regarding protection of SCADA and PCS from cyber threats.

Mr. Frigeri said the group continues to garner key input from industry and government, and the participants have been very gracious with their time and their knowledge, especially from the vendor communities. Siemens and Cisco have both provided the Study Group with presentations. British Columbia Institute of Technology gave a briefing on their incident database which offered a different perspective. Recently, Mr. Doug Maughan, from DHS Science and Technology, provided the Study Group with some great inside views and knowledge of how the government coordinates such things as research and development. The Study Group has submitted a draft report to the Working Group Chair's point of contact. Mr. Frigeri thanked the NIAC Secretariat's Mike Schelble for his hard work on this. Mr. Frigeri stated the Working Group now has the raw material of the final report in front of them, and now the team needs to refine and understand this raw data.

Mr. Frigeri referenced the Study Group's timeline. The Council chartered the Convergence Working Group in October 2005, and the Study Group has had about twenty meetings. The Study Group has had two vendor briefings, three government department briefings and four institution briefings.

Mr. Frigeri moved to the Group's actions to date. They received a secret-level briefing for a better understanding of the existing threat. They have also identified key elements in the next steps for developing policy-level recommendations for the five framework questions. They are currently investigating and evaluating how the market can act as a catalyst to spur further investment in the owner/operator community. This provides the vendor community, including hardware, software, and system integrators, a defined marketplace to help justify their research and development into specific technologies and products that can further protect critical infrastructure from cyber threat.

Mr. Frigeri moved to the Group's key observations to date. The Group acknowledges the diversity of the sectors in terms of response to the emerging threat against SCADA and PCS. The Study Group concentrated on the motivating factor of consequence. Mr. Frigeri commented about the Study Group's need to do a better job with providing definition and quantifying the consequences and how that risk is actually being managed. He thanked Co-Chairman Peters for facilitating an initial conversation with the University of Georgia on this topic. The Group also needs to conduct CEO discussions, which they plan to do well before the final report.

Ms. Grayson thanked Mr. Frigeri for his presentation. The Group will be collecting data at the Process Control Systems Forum (PCSF) in a briefing in June to better understand what their work and what information the Study Group can use from research completed by PCSF. Ms. Grayson asked the Council for questions.

Mr. Peters thanked the Study Group for their continuous hard work. Mr. Peters approached the Dean of the University of Georgia's Department of Risk Management and Insurance to determine if they look at SCADA and PCS when they assess companies for various quality aspects. The Dean told Mr. Peters they had not yet studied SCADA and PCS as part of the program. He agreed to

bring it up at the next board of overseers meeting to see if it should be part of the program. Mr. Peters used this as an exampled of the Group's struggle with a lack of corporate awareness of the potential problem of SCADA and PCS attacks. Mr. Peters stated most corporate leaders do not have motivation to secure their own critical infrastructure, let alone the nation's critical infrastructure. He concluded by saying the Convergence Working Group and their team has done an incredible job, and he believes the final recommendations of the Working Group will help protect the nation's SCADA and PCS.

Vice Chairman Chambers told the Convergence Co-Chairs their Group appears to be moving quickly toward their goals. He thanked Ms. Grayson, Mr. Peters and Mr. Conrades for their leadership of this Group. The Vice Chairman believes the Working Group understands the right policy issues to make the best recommendations for the President. He then asked if anyone had any questions or comments for the Convergence Group before they moved forward.

Assistant Secretary Stephan told the Council DHS greatly appreciated their help in developing the NIPP, and they will look to the NIAC for assistance when they begin creating the Sector Specific Plans. He also asked the Council to feel free to give DHS any tips or strategies to help the Department move toward hurricane season 2006.

VII **NEW BUSINESS** — NIAC Vice Chairman, *John T. Chambers*, NIAC Members, *TBD*

A. DELIBERATION AND VOTING ON NEW INITIATIVES — NIAC Members

The Vice Chairman moved to the topic of voting on new initiatives. At the October meeting, the Council developed a list of possible new initiatives. Vice Chairman Chambers asked Mr. Watson and Bill Muston to review the possible initiatives and the possible prioritization of the list.

Mr. Muston thanked the Vice Chairman. He told the meeting participants he and Mr. Watson had conducted a running dialogue on potential new work topics, and at the October meeting they had a list comprised of inputs from a number of Council members. From this list, the Council initiated two new topics, creating the Convergence Working Group and the CBR Working Group.

Since some groups are nearing completion of their studies, Mr. Watson and Mr. Muston believed it to be the right time to present new topics for consideration for future work. Mr. Muston announced to the Council he would review the previously prioritized list from the October meeting and engage the Council in discussion of those topics. After the discussion, Vice Chairman Chambers would provide a decision on which direction to go with the new topics.

Mr. Muston then listed the potential topics:

- Interdependencies
- Technologies for critical infrastructure
- Self governance
- Role of risk transfer

- Software assurance

Mr. Muston noted at the last new initiative vote, the Council decided to combine the initiative on the use of networked information systems and the database correlation initiative, calling it technologies for critical infrastructure. The interdependencies initiative and the technologies for critical infrastructure initiative received the most votes, while the other three ideas received no votes.

The interdependencies topic raised the discussion of whether risks associated with interdependencies among critical infrastructures could be reduced through new analytical approaches, consideration of supply and value chains, critical infrastructure input to state, local, regional and federal planning modeling and exercises, and the quantification of interdependencies. Critical infrastructures are dependent upon each other, dependent upon their supply and value chains and dependent on local, state and Federal government agencies. Entire governments have dependencies on critical infrastructures. Individual businesses may possess awareness of their supply and value chains, but may lack awareness of critical upstream cross-sector dependencies or productivity or business benefits through secured integration. Contingency planners may not know geographical concentrations and co-location of critical infrastructure key resources, amplifying cascading risks if disrupted. Mr. Muston said owners and operators may concentrate critical infrastructures geographically, and supported this fact with how the hurricanes affected the supply of gasoline due to the geographic concentration of refineries. Such instances may include a concentration of a single type of infrastructure within one area, including their supply chains, or a nexus of multiple types of infrastructure coming together in a single area, such as a bridge or water crossing that might have highway, rail, communications, power and pipelines. Local, state and regional planning and exercises might better identify interdependencies, co-locations, and geographic concentrations of key resources and measures to reduce risk, mitigate damages and speed recovery. Can the state and local levels of government develop good public/private partnership models? Input by critical infrastructure to the design of various analytical modeling studies and into the planning of exercises may provide scenarios with more meaning to critical infrastructures than those designed primarily by government agencies. The development of meaningful quantification of interdependencies might aid the prioritization of resources.

Mr. Watson stated the two questions in the combined technology topic:

1. Can emerging technology capabilities be reasonably utilized for critical infrastructure protection, and do such capabilities pose any policy issues such as privacy concerns?
2. Can commercial technologies be used to help government agencies correlate various, disparate databases for more effective terrorist tracking and crime prevention?

Mr. Watson continued by describing the basis of the questions in more detail. The first question discusses how the capabilities of remote monitoring and sensing continue to expand while their costs decrease. Such capabilities include video, intrusion and contact sensors, and gaseous sensors. The costs to make information from such monitors and sensors available through networked information systems to owners and operators of critical infrastructure and to law enforcement and government also continue to decrease. As a result, substantial monitoring, prevention and deterrence capabilities may near broad availability.

- How could they provide value to owners and operators and to law enforcement and to government?
- Are there values to owners and operators beyond critical infrastructure protection that would provide or support the business case for the purchase and use of such systems?
- Does the use of such systems raise other issues such as privacy and does the technology itself offer any help with such policy issues?

The other question, regarding database correlation for terrorist tracking and crime prevention, has a similar policy issue. Critical infrastructure enterprise companies with global reach routinely take advantage of networking technology and databases to optimize productivity. This often involves allowing different levels of access, complying with various national jurisdictional rules and protecting customer and employee private information. Correlation of disparate business database has become a routine function of supply chain management and customer relationship management. Intelligence agencies and law enforcement agencies must work together to prevent terrorist attacks and crimes against critical infrastructures. Currently, tracking potential miscreants through various law enforcement agencies, state driver's license departments, Customs, Immigration, telephone records and intelligence agency watch lists is not correlated. Putting together enough data to track a single malicious actor through these uncoordinated databases, can take weeks, possibly too long to prevent the next terrorist attack. Correlation of these databases is not a technical issue but one involving policy. Privacy concerns are paramount, but data protection and oversight are also important. How can policy changes remove barriers to needed database correlation without compromising civil liberties? What are the proper roles of federal agencies, federal, state and local law enforcement agencies, the intelligence community and the private sector in this effort?

Mr. Watson and Mr. Muston recommended the Council deliberate two topics, the interdependency topic and the technologies for critical infrastructure protection topic. The NIAC should choose one of the topics and pursue it once the Council finds it can add to its workload.

Vice Chairman Chambers thanked Mr. Watson and Mr. Muston. He wanted to make it known the Council makes it its goal to never lose track of their role to add value and focus on what the President and DHS Secretary want them to do. He then stated the NIAC has a considerable workload, and they may lack available resources at this time. He continued by saying the Council needs to continue to create quality recommendations. Vice Chairman Chambers asked to hear recommendations and opinions regarding these topics.

NIAC Member John W. Thompson brought up an additional topic the NIAC may want to research. He believes the issue of common criteria and how the government uses and applies it across the board and how it might help the country build better software products that are more secure and, candidly, meet a more pressing global standard for assurance. There appear to be multiple agencies in government working on the problem, but Mr. Thompson did not believe they have as much coordination as necessary or have enough industry involvement in that process. He told the Council the topic could add value to the NIAC and it would serve the interest of both technology industry as well as the government in general. He volunteered to chair the effort if Council chooses to research the topic.

Vice Chairman Chambers agreed about the topic's importance and asked the Council to begin considering that topic for future initiatives.

Assistant Secretary Stephan interjected, stating DHS would like to see efforts on all of the topics presented for voting. The Assistant Secretary suggested the group should also look at the issue of the insider threat. He told the group this issue has become more pressing to the critical infrastructure community in the past year.

Vice Chairman Chambers asked the Council if they had any additional thoughts on the subject. Prior to the next meeting, Mr. Watson and Mr. Muston should coordinate with the White House to assess the two topics. Vice Chairman Chambers asked the Council if any members would like to chair either of the topics.

Mr. Berkeley told Vice Chairman Chambers he wishes to finish his current initiative for the NIAC before becoming the chair of another Working Group.

Mr. Thompson expressed his willingness to chair the technologies for critical infrastructure protection. Ms. Marsh told the Vice Chairman she would help Mr. Thompson on this project. Vice Chairman Chambers recognized the workload of the Council and its staff and asked Ms. Menna in the Council could have the final vote for the new initiative at the July meeting where more members will attend in person. Ms. Menna told the Vice Chairman the vote could take place in July.

VIII **ADJOURNMENT** — NIAC Vice Chairman, *John T. Chambers*

Vice Chairman Chambers thanked DHS for their continued support. He thanked the NIAC members, members of the public and the press for attending the meeting. The NIAC's next quarterly business meeting is July 11 2006 at the National Press Club, when the Council has scheduled a meeting with the President. Vice Chairman Chambers 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: 7/11/06
Erle A. Nye, Chairman

ATTACHMENT A

Workforce Preparation, Education and Research

National Infrastructure Advisory Council (NIAC)

Workforce Preparation, Education and Research Working Group

Status Report
April 11, 2006

Alfred R. Berkeley, III
Chairman and CEO
Pipeline Trading, LLC.

Dr. Linwood H. Rose
President
James Madison University

Agenda

- Question
- Approach
- Findings
- Recommendations

NIAC Question

- "**How do we ensure adequate development of intellectual capital to protect critical American information infrastructure and infrastructure concepts?"**
- Examined four areas to increase intellectual capital:
  1. Efficacy of the National Science Foundation's Scholarship for Service Program (Cyber Corps)
  2. Research and development priorities to improve cyber security
  3. Enhance the usefulness and availability of cyber security certification programs
  4. Improve math and science competency of K-12 learners

Approach (cont.)

- Why these areas?
  - Efficacy of Scholarship for Service (Cyber Corps) program
    - Government funded
    - Has a more immediate impact on workforce
  - Enhance cyber security research and development funding
    - R & D invigorates economy and infuses new knowledge into workforce
    - Drives innovation
  - Enhance the usefulness and availability of cyber security certification programs
    - Certification allows current workforce to gain new knowledge quickly
    - Strong method to update skills and learn new skills
  - Improve math and science competency of K-12 learners
    - Underlying key to a competent workforce, global competitiveness, innovation and protection of Nation's cyber security and critical infrastructure

Approach (cont.)

- Reviewed relevant research and available
- Interviewed subject matter experts from academia, government, the business world and the private sector

Findings

- Area #1: Efficacy of Scholarship for Service (Cyber Corps) program
  - The goal is to provide government with a qualified IA workforce
    - Managed by National Science Foundation (NSF)
    - In 2005, budget $14.2 million; 2006 budget request is $10 million
    - Over 600 students have received scholarships since Spring 2005
    - Recipients required to intern at and find permanent jobs at government agencies

Findings: Cyber Corps

- Challenges:
  - Locating an internship and job at a Federal agency
  - Lack of Cyber Corps awareness among agencies
  - Half of graduates end up at the National Security Agency, protecting information but not necessarily critical infrastructure
  - Financial considerations
  - Security clearances

Recommendations: Cyber Corps

1. Set up “draft” system (DoD has SFS program set up this way)
2. Provide hiring flexibility
3. Expand employment options
4. Restructure scholarship funding to be either Flat or Matching
5. Ease challenge of obtaining security clearances

Findings: Research & Development

- Area #2: Enhance cyber security research and development funding
  - The Study Group's research and interviews brought out seven key findings:
    - Research Agenda
    - Current Funding Status
    - Balanced Funding Portfolio
    - Adequacy of Funding
    - Time to Market
    - Talent Pool
    - Coordinating Body

Recommendations: Research and Development

1. Develop national research agenda to prioritize cyber security research efforts
2. Increase funding base for critical infrastructure protection and cyber security related research
3. Conduct additional studies to find solutions for decreasing cyber security research products' "time to market"
4. Ensure an adequate talent pool, increase and stabilize funding for fundamental research in unclassified cyber security
5. Designate coordinating body to oversee cyber security research efforts

Findings: Certification

- Area #3: Enhance the usefulness and availability of cyber security certification programs
  - Institute for Defense Analyses (IDA)
    - IDA conducted a study mapping Commercial IA Certifications to Pentagon IA Workforce Levels and Functions.
    - DHS has a goal to establish nationally recognized, privately administered certifications

Findings: Certification

- Challenges:
  - Making cross-government position attributes standard
  - Governance structure of a national information assurance (IA) certification program
  - Current testing methods may not adequately measure increases in Knowledge, Skills and Abilities (KSAs)

Recommendations: Certification

1. Develop and maintain standardized IA position descriptions, including required and recommended KSAs for each level of each Federal department and agency position
2. Designate a privately administered, public-private IA training certification body
3. Review and reform IA testing procedures, providing outcome-based, modular computer-based testing and metrics whenever possible

Findings: K-12

- Area #4: Improve math and science competency of K-12 learners
  - A globally competitive workforce is essential to any long-term protection of America's critical infrastructure and economy
  - Schools should teach facts, concepts and skills to make its workforce competitive in a global economy
  - The scientific method must be more rigorously applied to education

Findings: K-12

- Challenges
  - The Federal government cannot legally mandate curricula or teaching methods
    - Education is a mix of local, state and Federal decision making
- The Federal government can:
  - Provide existing research, comparisons, and analysis
  - Sponsor additional research in areas where rigorous, peer-reviewed, substantiated research is lacking
- The goal is to arm education decision-makers and parents, with information on what works and what doesn't to educate our children

Findings: K-12

- Standards: What Students Should Know at Each Grade Level
  - America's educational standards--local, state or Federal--must align with the realities of global competition
- Testing
  - Tests should measure whether a student knows what they are expected to know
- Curricula: What We Teach
  - State educational standards should be competitive with high performing international standards and their curricula should reflect those standards
  - Lacking curricula coherence
    - Teach a mile wide and an inch deep
    - Sequence is important
  - Leads to unintended social consequences

Findings: K-12

- Issues of Pedagogy: How Teachers Teach
  - Reading wars and Math wars
  - Teaching Aids: Textbooks
  - The Role of Automation in Teaching

Recommendations: K-12

1. The Federal government should do everything in its power to assist states in implementing internationally competitive standards, curricula and teaching methods.

Recommendations: K-12 (cont.)

2. To assist in this implementation, the Federal government should sponsor independent, third party peer reviewed research to:
   - Determine "high achieving" international competitors, be those competitors domestic or foreign
   - Determine the most effective international standards, curricula and teaching methods
   - Determine the strengths and weaknesses of the most internationally competitive curricula and teaching methods
   - Compare each state's educational standards to the standards, curricula and teaching methods of the high achieving international competitors

Recommendations: K-12 (cont.)

- Compare the most widely used U.S. curricula for each subject against the curricula of high achieving nations in those same subjects
- Compare each state's curricula sequencing and coherence against the curricula sequencing and coherence of the highest performing states and international competitors
- Test U.S. students against the most competitive international standards using the National Assessment of Educational Progress
- Develop low-risk self-tests covering internationally competitive K-12 curricula
- Compare the effectiveness of "self-discovery" and "basic skills" approaches to teaching

Recommendations: K-12 (cont.)

- Determine whether approved textbooks have been independently peer-reviewed by subject matter experts in the disciplines involved in the books
- Determine whether the curricula and teaching methods taught in teacher certification programs are substantiated as globally competitive by independent, third-party, peer-reviewed research
- Determine whether each state's curricula used in compliance with No Child Left Behind have a basis for effectiveness substantiated by research
- Publish the results of all research relevant to the topics listed above on the Internet to make them widely available to educators and parents

Recommendations: K-12 (cont.)

- All research initiated as a result of these recommendations, including research on Project Follow Through and the Trends in International Mathematics and Science Study (TIMSS) should be published and made publicly available via the Internet
- Accountability mechanisms, including Federal funding incentives, should be implemented to encourage States, school districts and teacher preparation programs to achieve internationally competitive standards, curricula and teaching methods

Discussion

- Questions?

ATTACHMENT B
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
- Actions Taken
- Guiding Principle
- Context
- Findings
- Case Studies
- CEO Survey
- Conclusions

Purpose

- Improve coordination between critical infrastructure sectors and the Intelligence Community to protect critical infrastructures

Actions Taken

- Formed Study Group
- Held four workshops and bi-weekly calls
- Defined and studied key issues
- Used recent events as case studies
- Interviewed CEOs and IC seniors for executive perspective

Guiding Principle

- Critical infrastructure sectors differ greatly in terms of
  - Needs
  - Complexity
  - Regulatory environments
  - National boundaries
  - Organization
- "One size fits all" solutions will not suffice
- Recommendations aim to improve national capability, but allow for sector differences
  - Architecture approach
  - Process-based trust relationships
  - Information protection

Context

- Findings and recommendations must be applied to:
  - Deterrence
  - Protection
  - Preparedness
  - Crisis Management and Response
  - Recovery (Restoration and Reconstitution)
- Implementation will depend on level of focus
  - Strategic planning and decision-making
  - Operational or tactical decision-making

Findings

- Differences in experience, vocabulary, culture, and specialized skills inhibit information exchange and analysis
- Current information sharing mechanisms complex, poorly understood, not customer focused
- Government caveats and classifications impede timely and appropriate information sharing
- Current alert and warning process does not reach appropriate decision makers

Case Studies

- Purpose: Illustrate issues and findings
- Four recent significant incidents involving critical infrastructures and the intelligence community
  - Focused on information sharing
  - Covered all hazards to critical infrastructures
  - Two cases represent pre-event warnings to critical infrastructures
  - Two cases represent post-event analysis
  - Three cases related to terrorist acts or intentions; the other was a non-hostile event
    - August 2003 Blackout
    - July 2004 Financial Services Threat Alert
    - July 2005 London Bombings
    - October 2005 New York Public Transit Threat Alert

CEO Survey

- Survey questions related to changes since 9/11/2001:
  - Investment strategies
  - Training priorities
  - Information requirements (from government)
  - Information sharing (with government)
  - Top-level concerns
  - Board involvement
- Survey concerned with information sharing necessary to support CEO policy and investment decisions
- Could provide useful guidance to upcoming DNI strategic planning effort

Common CEO Themes

- Implications of 9/11 considered and incorporated without strategic input from government
- Claims of inadequate security not supported by shared intel or criteria but worst-case speculation
- Inability to provide meaningful information for policy and investment decisions due to:
  - Absence of agreement on end-state
  - No joint processes for planning and implementation
  - Lack of understanding of sector business operations
- More emphasis placed on response than additional protection w/o credible threat information

Preliminary Recommendations

- Establish trusted CEO-IC relationships
- Create process for CEO-IC strategic planning and information sharing
- Develop sector business expertise in IC to better identify and satisfy information needs; establish liaisons with relevant corporate officers
- Focus on information requirements not classification

Conclusions

- All involved in Critical Infrastructure Protection doing the best they can with information they have
- Better information sharing will improve timely actions and coordination
- Recommendations simple, but not easy

Questions and Answers

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

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
- Study Group Timelines
- 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

- Common set of data points to collect across critical sectors; contributes to trending/consistency
- Question #1
  - Do CEOs and their organizations have employee awareness, preparedness and response training programs?
    - What is the nature of the training program?
    - Who leads this function?
    - Is this an enterprise issue?
    - Are there industry leaders that excel at biological preparedness?
    - What lessons learned are derived from your experiences or the experiences of those industry leaders?

Key Questions (cont.)

- Question #2
  - Is there a market incentive to invest in biological preparedness and response programs?
- Question #3
  - Is there sufficient communication infrastructure in place to respond to a biological event?
    - How are owner/operators informed? Via what channels?
    - How quickly is information distributed?
    - What are the bottlenecks to information distribution?
    - What role do SCCs or ISACs play in biological events?

Key Questions (cont.)

- Question #4
  - What tools and technologies currently support your biological response capability?
  - What tools and technologies are currently insufficient and why do they not meet your requirements?
- Question #5
  - Is there sufficient coordination between federal, state, local and private-sector entities?
    - What inter-dependent plans are currently in place?
    - How is coordination managed between entities at multiple public and private sector levels?
    - How is communication managed?
    - Are there examples of successful exercises across entities?

Key Questions (cont.)

- Question #6
  - What can the federal government do to encourage or facilitate enhanced preparedness and response capabilities?
- Question #7
  - What are key inter-dependencies in a biological event?
    - How are those inter-dependencies managed? Via what channels? Are they federal, state, local, private or multiple combinations of all four?
    - How are inter-dependent communications managed?

Key Questions (cont.)

- Question #8
  - What are the three or four critical vulnerabilities facing your organization today?
    - What are the proposed best courses of action to remedy those vulnerabilities?
    - Who owns responsibility for managing these responsibilities and what role should each responsible party play?
    - What is the timeline to address identified vulnerabilities?

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

Critical Sectors and Leads (cont.)

- A number of other less-linear contributors:
  - Federal
    - HHS/CDC
    - DHS
    - DoD
  - Companies or representative organizations with biological preparedness/response capabilities
    - Wal-Mart
    - Federal Express
    - Home Depot
    - Business Executives for National Security (BENS)
  - Academia

Study Group Timeline

- April 15, 2006
  - Data collection and interviews complete
- May 15, 2006
  - First draft of initial findings and recommendations
- June 1, 2006
  - Complete draft findings and recommendations and distribute to NIAC membership
- July NIAC Meeting
  - Present final findings and recommendations

Discussion

- Questions?

ATTACHMENT D
Convergence of Physical and Cyber Technologies and Related Security Management Challenges

National Infrastructure Advisory Council (NIAC)

Convergence Working Group

Status Report
April 11, 2006

George H. Conrades
Executive Chairman
Akamai Technologies

Greg Peters
Former Chairman and CEO
Internap Network Services

Margaret Grayson
President, AEP Govt.
Solutions Group

Overview

- Purpose
- Status of *Next Steps* from Last Meeting
- Timeline
- Actions
- Key Observations to Date
- Next Steps

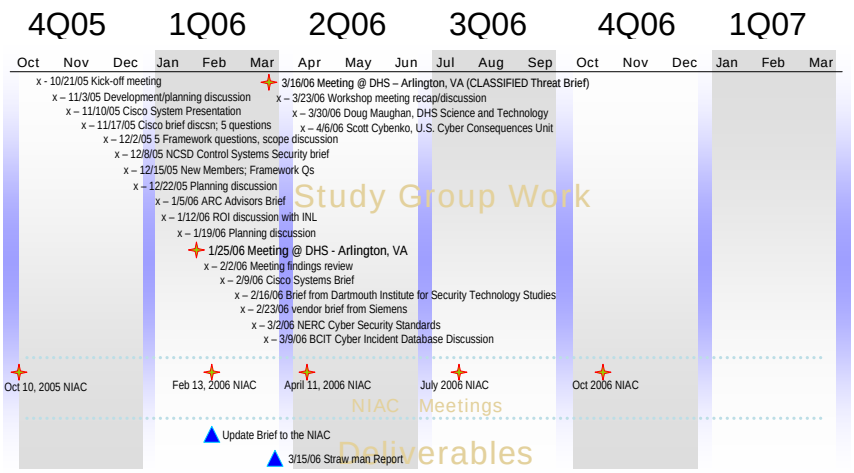
Purpose

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

Status of *Next Steps* from Last Meeting

- ✓ Continue group development with key input from Industry and Government
  - Classified Threat Brief
  - Andrew Wright and Venkat Pothamsetty, Cisco Systems CAIG
  - Professors Cybenko and Smith, Dartmouth Cyber Security Program
  - Paul Skare, Siemens
  - Tom Flowers, NERC
  - Professors Eric Byres and David Leversage, BCIT
  - Doug Maughan, DHS Science and Technology
- ✓ Draft report submitted to Working Group Chair point of contact for review.
  - Includes full synopsis of all findings on the five framework questions
  - Established interrelationships between five framework questions

Time Line



Actions

- Held second workshop meeting
- Received secret-level threat brief to help develop understanding of existing threat to SCADA and Process Control Systems
- Identified key elements, interrelationships and next steps for developing policy-level recommendations for the five framework questions.
- Developed four draft recommendations
- Continuing to work with subject matter experts on key elements

Key Observations to Date

- There is significant diversity both within and across sectors in terms of response to this emerging threat.
- The motivating factor for businesses that have addressed SCADA/PCS security is *consequence.*
  - threats from cyber security were directly correlated to failures in reliability, availability and safety
- Opportunities exist for the federal government to lead in information sharing, research and development coordination, creating market stimuli, and facilitating executive leadership access to important information.

Key Observations to Date *(continued)*

- Standards and application of existing standards are inconsistent across sectors
- Access to threat and consequence information is critical to motivating executive leadership to act on the emerging cyber threat.
- Threat and consequence information are missing elements in the return on investment equation for cyber security case that must be made to executives.
- There is no universally accessible mechanism for sharing threat and incident information, and barriers exist for companies to do so.

Next Steps

- Address consequences element with Scott Borg, U.S. Cyber Consequences Unit and Insurance industry
- Conduct CEO outreach
- Further develop potential recommendations
- Consult University of Georgia Department of Risk Management

Discussion

- Questions?

ATTACHMENT E
New Topics

National Infrastructure Advisory Council (NIAC)

Possible New Initiatives

Ken Watson
Cisco Systems, Inc.

Bill Muston
TXU

Overview

- Previous prioritized list
- Remaining topics
- Discussion
- Voting and Decision

October 2005 Priorities

1. Physical/Cyber Convergence
2. Biological/Chemical/Radiological Events and Critical Infrastructure Workers
3. Interdependencies: Analysis, Planning, Exercises, & Practice
4. Use of Networked Information Systems for Critical Infrastructure Protection
5. Database Correlation for Terrorist Tracking and Crime Prevention
6. Self Governance for Critical Infrastructures
7. Role of Risk Transfer Mechanisms
8. Software Assurance for Critical Infrastructure Owner/Operators

Remaining Initiatives and Previous Votes

1. Interdependencies: Analysis, Planning, Exercises, & Practice (6 votes)
2. Use of Networked Information Systems for Critical Infrastructure Protection (5 votes)
   Database Correlation for Terrorist Tracking and Crime Prevention
3. Self Governance for Critical Infrastructures (0 votes)
4. Role of Risk Transfer Mechanisms (0 votes)
5. Software Assurance for Critical Infrastructure Owner/Operators (0 votes)

Interdependencies: Analysis, Planning, Exercises, & Practice

- Question: Can risks associated with interdependencies among critical infrastructures be reduced through (1) new analytical approaches, (2) consideration of supply and value chains, (3) critical infrastructure input to local, state, regional, and federal planning, modeling and exercises, (4) quantification of interdependencies?

Technologies to Enhance Critical Infrastructure Protection

- Combined questions:
  - Can emerging technology capabilities be reasonably utilized for critical infrastructure protection, and do such capabilities pose any policy issues such as privacy concerns?
  - Can commercial technologies be used to help government agencies correlate various, disparate databases for more efficient terrorist tracking and crime prevention?

Voting and Decision

Discussion