National Infrastructure Advisory Council

Meeting Agenda

Monday, February 13, 2006
1:30 – 4:30 p.m. ET
The National Press Club Ballroom
529 14th Street NW
Washington, DC 20045

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,* Chairman and CEO, Cisco Systems, Inc. *George W. Foresman,* Under Secretary, Preparedness Directorate, DHS *Neill Sciarrone*, Director, Infrastructure Protection Policy, Homeland Security Council
IV.	**National Infrastructure Protection Plan Status Update**	*Robert B. Stephan*, Assistant Secretary, Office of Infrastructure Protection, DHS
V.	**Approval of October Minutes**	NIAC Chairman *Erle A. Nye*
VI.	**Status Reports on Current Working Group Initiatives**	NIAC Chairman *Erle A. Nye* Presiding
	A. Intelligence Coordination	NIAC Vice Chairman *John T. Chambers*, Chairman and CEO, Cisco Systems, Inc. and *Gilbert Gallegos,* Chief of Police (ret.), Albuquerque, New Mexico Police Department, NIAC Member
	B. 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
	C. Chemical, Biological and	*Chief Rebecca F. Denlinger,* Fire Chief, Cobb

	RADIOLOGICAL EVENTS AND THE CRITICAL INFRASTRUCTURE WORKFORCE	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.
D.	**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 Chairman *Erle A. Nye*, NIAC Members TBD
A.	**STATUS REPORT ON IMPLEMENTATION OF RECOMMENDATIONS**	*Nancy J. Wong*, Designated Federal Officer, NIAC, DHS
VIII.	**ADJOURNMENT**	NIAC Chairman *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Chairman Nye, Mr. Berkeley, Lt. Gen. Edmonds, and Ms. Grayson.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Vice Chairman Chambers, Chief Denlinger, Chief Gallegos, Ms. Marsh, Mr. Noonan, Mr. Peters, Mr. Rohde, and Dr. Rose.

MEMBERS ABSENT:
Mr. Barrett, Mr. Conrades, Mr. Davidson, Mr. Hernandez, Commissioner Kelly, Mayor Santini-Padilla, and Mr. Thompson.

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

STAFF DESIGNEES MONITORING PROCEEDINGS VIA CONFERENCE CALL:
Mr. Allor (for Mr. Noonan), Mr. Blanchette (for Ms. Marsh), Mr. Clyde (for Mr. Thompson), Mr. Ellis (for Mr. Conrades), Mr. Holmes (for Mr. Davidson), Lt. Mauro (for Commissioner Kelly), Mr. Talbot (for Mr. Hernandez), and Mr. Watson (for Vice Chairman Chambers).

OTHER DIGNITARIES PRESENT:
U.S. Government: George W. Foresman, Under Secretary for Preparedness, Department of Homeland Security, Robert B. Stephan, Assistant Secretary, Office of Infrastructure Protection, DHS, Ms. Neill Sciarrone, Director, Infrastructure Protection Policy, Homeland Security Council, Mr. R. James Caverly, Director, Infrastructure Partnerships Division (IPD) of the Department of Homeland Security, Ms. Nancy J. Wong, Director, Infrastructure Programs Office and Designated Federal Officer (DFO) for the NIAC, and Ms. Jenny Menna, Designated Federal Officer (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 Infrastructure Partnership Division of the Department of Homeland Security (DHS). She welcomed Robert B. Stephan, Assistant Secretary for Infrastructure Protection, Ms. Neill Sciarrone, Director, Infrastructure Protection Policy, Homeland Security Council, 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. She extended a welcome on behalf of DHS to the members of the press and public for attending. Ms. Menna 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 to order the fourteenth meeting of the NIAC and the first meeting of the year 2006. Ms. Menna then proceeded to call roll.

II. ROLL CALL

III. OPENING REMARKS AND INTRODUCTIONS

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

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

George W. Foresman, Under Secretary for Preparedness, DHS

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

Chairman Nye thanked Ms. Menna and thanked those participating in the meeting. He told the group the NIAC continues to make some great progress. Chairman Nye acknowledged Assistant Secretary for Infrastructure Protection Robert Stephan. The Chairman also announced that the group expected Preparedness Under Secretary Foresman to arrive shortly.

Chairman Nye asked Assistant Secretary Stephan to give his presentation. Assistant Secretary Stephan thanked the Chairman and Vice Chairman and apologized for Deputy Secretary Jackson's absence, due to FEMA reorganization duties. The Assistant Secretary conveyed his excitement that DHS has accomplished a great deal with regard to critical infrastructure protection (CIP) in the first three years of its existence. He added that they still had a long way to go. Assistant Secretary Stephan informed the Council that he believed 2006 would be the year in which DHS sees the rewards of its matured partnerships.

Assistant Secretary Stephan described the National Infrastructure Protection Plan (NIPP) as an important product because it represents a baseline for how DHS will move forward with CIP. DHS needs a base plan so the government and the private sector can have something they agree on to tailor to specific risks and needs within each of the 17 sectors. The NIPP Program Management Office (PMO) put the NIPP through two major comment periods during the past few months, one in November and one in early December. During the comment periods, the document received close to eight thousand comments, including a few thousand from the federal register process. The NIPP PMO revised the document over the Christmas and New Year's holiday. Afterwards, they sent out a second draft in mid- January. The next comment period ended officially on Monday, February 6, 2006. Assistant Secretary Stephan told the Council that he and his team continued to work around the clock to make sure a good product lands in the hands of the Secretary for his approval by the end of February. That would allow the month of March for the NIPP to work its way through the White House Homeland Security Policy process, to get the signatures they needed to demonstrate the Federal cabinet level commitment this plan deserves.

DHS has been working very aggressively with its partners to figure out if they have the base plan correct. It is a challenge because the one thing the17 sectors share in common is they are very different. The sectors share the fact that they are very diverse, very different, with different risk landscapes, resources, authorities to enable protection, and no base plan can specifically meet all the requirements of every single partner in this model. The NIPP PMO has applied the Sector Partnership Model, which the NIAC previously recommended, to the NIPP. The NIAC Sector Partnership Model will act as the centerpiece for how the government and the private sector cooperate and work together, to enable the protection of the nation's critical infrastructures. The Sector Partnership Model has helped bring the process together to make sure a thoroughly vetted document developed with comments from both the public and private sectors gets put in place as the base plan. The Assistant Secretary and the NIPP PMO plan to complete the sector-specific plans that will become annexes to the base plan within six months following the issuance of the base plan. The individual sectors will then tailor the plan to their own needs, based upon general concepts agreed to in the base plan. The specifics of risk management, information sharing and progress measurement will be approached at the sector level. The comments by the NIAC in the Sector Partnership Model reference the need to achieve a balance between protecting sensitive critical information that could be intercepted and used to aid and abet our terrorist adversaries, with the need to also ensure the need to know and the right to know for the public. No corporation would like to share information relative to vulnerability with terrorist adversaries.

In terms of the risk analysis and risk management process, DHS expanded the vocabulary with an inclusive focus on assets, systems, networks and the connectivity and interdependencies between them. DHS is trying to blend the concepts of protection, personnel security, cyber dependencies and cyber resiliency and robustness into an overall protection framework umbrella. DHS also plans to look at expanding the risk methodology pieces, included in the initial draft so they can be tailored to the specific landscapes, assets, system and network mix seen across the 17 sectors.

Assistant Secretary Stephan expressed his pleasure in working for Under Secretary Foresman because the Preparedness Directorate in DHS will now make sure the grant programs are not seen as individual silos. DHS wants to connect the urban area security initiative grant monies as a baseline, with the transit grants, busing grants, port grants and specific infrastructure-targeted grants layered on top to provide additional layers of connected capability. At the top, the Buffer Zone Protection Plan Program will help DHS identify key vulnerabilities and requirements at Federal, state and local levels, along with prevention capabilities, forces and connectivity with private sector owners and operators. Through the national labs, DHS is developing an understanding of the dependencies and interdependencies, which will facilitate the allotment of federal money to the department's state and local government and private sector partners. This distribution of funding will create relationships that may otherwise lack sufficient robustness in the threat environment of the twenty-first century.

Assistant Secretary Stephan told the NIAC that he will continue looking to them for help in finalizing the NIPP, specifically requesting their assistance in developing the more challenging sector specific plans. The Assistant Secretary announced to the Council that DHS needs support in persuading the country to adopt this plan. Assistant Secretary Stephan praised the NIAC for its approach to its work with careful consideration and tact.

DHS is currently integrating the lessons learned from the hurricanes of 2005 into their preparedness plan. The NIPP has become a document that deals with all hazards, going beyond terrorism by ensuring the baseline of coordination systems, information sharing processes and approaches to include technical databases that will service the world of counter-terrorism protection, infrastructure restoration and recovery operations in the wake of a natural disaster or a major industrial accident. With the Katrina and Rita lessons learned, DHS continues to develop new standard operating procedures (SOP), and the Department will send the new SOP's to state and local governments via Homeland Security Advisors and to the private sector via the NIAC and other private sector entities. Chairman Nye offered DHS the Council's help with validating the lessons learned documents.

The Assistant Secretary then thanked all of those at the meeting who participated in the Cyber Storm exercise, a five day event that began as an initial threat, continued with an intelligence build up period and a lot of day-to-day background noise from which DHS had to flush out the malicious actors. The exercise focused on attacks on the aviation, telecommunication, and electricity industries. Assistant Secretary Stephan then thanked Chairman Nye and the Council and turned the floor back over to Chairman Nye.

Chairman Nye thanked Assistant Secretary Stephan for his kind words and told the meeting attendees that the Assistant Secretary's description of the NIPP was modest because it is an extremely impressive piece of work.

Chairman Nye then introduced George Foresman, the new Under Secretary for the Preparedness Directorate at DHS. The Chairman expressed the Council's willingness to work with the new Under Secretary in any way necessary. Chairman Nye told the Under Secretary the NIAC knew of his impressive history with CIP and the Council is extremely pleased to have him at the meeting. Chairman Nye deferred to Vice Chairman Chambers.

Vice Chairman Chambers congratulated the Under Secretary on his appointment and welcomed him to the meeting. The Under Secretary's stellar reputation as Vice Chairman of the Gilmore Commission and experience managing preparedness for Virginia gives the NIAC much confidence as he moves into his new role. The Vice Chairman told the Council the Secretary has restructured his organization into one viewing preparedness as an important responsibility. Vice Chairman Chambers approved of the Under Secretary's view of preparedness that includes physical and cyber, telecommunications, critical infrastructure and outreach. Vice Chairman Chambers stated Under Secretary Foresman should not hesitate to ask for any help from the Council. The Vice Chairman then asked Under Secretary Foresman to provide comments.

The Under Secretary thanked the Chairman and the Vice Chairman for reaching out so early in the process to ensure a solid partnership. He expressed his appreciation for his team at DHS, including Assistant Secretary Stephan, whose Infrastructure Protection Office has done great work and makes his job easier. Under Secretary Foresman told those at the meeting that he had three points he wished to offer the group. First, DHS and its partners have done a great job in protecting the Nation's critical infrastructure, but this public-private collaboration can do much more. There are policy and legal issues that need to worked through. There is momentum in these efforts already, but it will be tough. With the help of a tight partnership, DHS and its partners can make a great deal more progress.

Second, Under Secretary Foresman said DHS has not put a premium on the art of communication. The department spends a lot of time sending emails back and forth and asking people to comment on things, but that is not communication. Communication is the ability for everyone to have discussion, dialogue, and a sense of mutual understanding of what the other person is intending to convey in terms of information. Some of the biggest challenges Under Secretary Foresman faced in his first 45 days at DHS really came down to communication. Thus, the Under Secretary very much encourages an open and candid dialogue. He also pledged to make sure he and his team speak openly and directly with all of their private sector partners.

The third point made by the Under Secretary was to make sure everyone knows what it is DHS needs the NIAC to do. The Under Secretary told the meeting participants it would improve the process if everyone knew what type of work the NIAC should be doing versus another advisory group. The Under Secretary promised to create a process within DHS that will assist the NIAC in identifying topics to address, so the Council may continue to produce high impact work. Under Secretary Foresman thanked the Council for allowing him to participate in the meeting and then turned the floor over to Chairman Nye.

Chairman Nye again thanked Under Secretary Foresman and told him how much the Council appreciated his presence at the meeting. The Chairman agreed with Under Secretary Foresman in that the NIAC should only have so many undertakings, and the Council continues to have issues with prioritization of topics. Chairman Nye announced to the audience that he was extremely proud of the work Council continues to produce.

The Chairman then announced that the number of NIAC members has decreased in the last year, and he urged the White House to nominate more individuals for appointment to the NIAC. He believes that the NIAC has a great team in place, but it would be very helpful to have a few more members to provide insight from all the critical infrastructure sectors.

Chairman Nye then moved to the topic of the NIPP. He wanted to make sure that he said Assistant Secretary Stephan has made great improvements in the NIPP in front of the Under Secretary. The Chairman said that he has watched the process for two cycles and the NIPP has developed impressively. The Chairman said he was impressed that Assistant Secretary Stephan and his team brought together a tremendous amount of information in a coherent document in a relatively short period of time. Judging from the number of comments received by the NIPP PMO, many people are interested in the plan. Chairman Nye told Assistant Secretary Stephan he made inquiries about the document to some of the sectors and they are uniformly complimentary. Chairman Nye stated DHS must understand each sector has a unique knowledge of their respective industries, and they would like DHS to make sure that the department defer to the sector-specific plan as long as it is consistent with the framework the NIPP provides. Chairman Nye thanked Assistant Secretary Stephan and asked Under Secretary Foresman if he wished to comment.

Under Secretary Foresman thanked Chairman Nye and told the Council that as DHS develops the sector specific plans, the department will tailor them to meet the risk landscapes of the individual sectors. The tailoring of the risk landscapes can only be done with input from the individual sectors.

Chairman Nye asked if any NIAC members had comments regarding the Under Secretary's remarks or the discussion of the NIPP. Vice Chairman Chambers said he appreciated the Under Secretary's comments regarding open communication. He also admired the Under Secretary's candor about what DHS needs the NIAC to do. Vice Chairman Chambers told the Under Secretary that he should advise the NIAC where they can help, because it makes sense not to waste time or energy on work in areas where the NIAC does not add value.

Vice Chairman Chambers then addressed Assistant Secretary Stephan's comments, applauding the Assistant Secretary for the monumental effort by the Assistant Secretary and his staff, as well as Assistant Secretary Stephan's openness and receptiveness to ideas from the private sector. Vice Chairman Chambers told the meeting participants that the NIPP will be effective and useful if it accomplishes three tasks. First, it must acknowledge the private sector's actions will always occur first and the federal actions and coordination will be welcome augmentation. Second, the NIPP must focus on risk management and priorities based on threats, abilities and consequences. Finally, the NIPP and the NIPP PMO must be ready for additional discussions on the relationships between individual targets of highest risk and what, if anything, this means about the relative risk to various sectors. Vice Chambers then deferred to Chairman Nye.

IV. APPROVAL OF OCTOBER 11, 2005 MINUTES — NIAC Chairman, *Erle A. Nye*

Chairman Nye asked the Council if they were ready to move to the approval of the meeting minutes for the October 11, 2005 meeting minutes. The NIAC concurred, and Chairman Nye began by providing a comment regarding the relationship between the NSTAC and the NIAC. On page 30 of the minutes there is a discussion about the relationship between NSTAC and NIAC. Chairman Nye commented the Council talked about the fact that there needs to be an understanding of how NIAC relates to NSTAC in its longstanding work around telecommunications. Chairman Nye told the Secretariat the Council wished for the minutes to reflect that the NIAC defers to its charter on the delineation between NSTAC and NIAC. This is because the NIAC charter has been approved throughout the government. Chairman Nye asked for the minutes to read that the NIAC only defers to the NSTAC with respect to national security and emergency preparedness around communications. He also asked that the minutes reflect what the Council says on the NIAC-NSTAC relationship to be consistent with the NIAC charter. Chairman Nye motioned to approve the minutes that would be amended by the NIAC Secretariat at some point in the future. The motion was seconded and the minutes were approved.

V. STATUS REPORTS ON CURRENT WORKING GROUP INITIATIVES — NIAC Chairman *Erle A. Nye* Presiding

Chairman Nye told Under Secretary Foresman the NIAC has produced seven reports that have been submitted to the White House. The White House has given the NIAC comments back on their reports, stating they have been meaningful. The Chairman speculated the NIAC is the most active Council on a current basis. He believes the reason for this is that the role the government assigned the NIAC forces them into action because understanding how to protect the Nation's critical infrastructure is crucial to having a secure United States.

In addition to the seven reports the President has received, the NIAC has sent one report, the Sector Partnership Model, to the Secretary. The Chairman thanked those who worked hard to get the Sector Partnership Model out, in particular, Mr. Martin McGuinn and Ms. Marilyn Ware, both of whom recently resigned from the NIAC. Ms. Ware had the honor of being nominated by the President to become ambassador to Finland, and Mr. McGuinn has resigned because he retired from his post as Chairman and CEO of Mellon Financial Corporation. Chairman Nye followed those comments by thanking Ms. Susan Vismor and Mr. Bruce Larson, the points of contact for Mr. McGuinn and Ms. Ware, respectively.

The Chairman told the meeting participants that the Council has nearly completed the Risk Management Report, and it will go to the President in the very near future.

A. INTELLIGENCE COORDINATION WORKING GROUP

NIAC Vice Chairman *John T. Chambers,* Chairman& CEO, Cisco Systems, Inc. and *Chief Gilbert Gallegos*, Chief of Police (ret.), Albuquerque, New Mexico Police Department, NIAC Member

After receiving no comments concerning the Sector Partnership Model and the Risk Management Report, Chairman Nye moved to the current Working Group initiatives, starting with the Intelligence Coordination Working Group. The Chairman described the intelligence coordination initiative as a thoughtful effort and asked Vice Chairman Chambers to report on the status of the Working Group.

Vice Chairman Chambers thanked Chairman Nye. The Working Group's efforts on the topic are coming to a conclusion. This quarter launched the case study sub-group, which is using recent events to illustrate findings and conclusions. The Working Group believes this will make the recommendations even more crisp and to the point. The Vice Chairman told the group that Mr. Al Berkeley is adding CEO-level perspective through interviews. With the Intelligence Coordination Report, the Working Group wishes to provide CEO-level perspectives as well as operational level perspectives. Vice Chairman Chambers asked Mr. Ken Watson to lead the Intelligence Coordination Working Group status presentation.

Mr. Watson thanked the Vice Chairman. He began by saying the Study Group is confident that work will be complete and the report and the final recommendations will be provided to the NIAC in time for the next meeting in April. The Working Group has been digging deep into issues that answer two basic questions. First, in what ways can the intelligence community help the private sector and by the private sector the Working Group means the owners and operators of the critical infrastructures? Second, in what way does the private sector help the intelligence community to refine their collection, analysis and dissemination? Law enforcement plays a key role especially as information from foreign and domestic sources is fused.

The Study Group adopted a very effective approach that started with the previously mentioned macro questions and divided the concerns into individual micro issues. The Study Group members then studied these micro issues in depth. Afterwards, the Study Group members came back together to develop issue papers, which were further developed into the macro findings, conclusions and recommendations. DHS has been very helpful in outlining existing information mechanisms as the Study Group looks at the ways the intelligence community and the private sector have shared information or have been unable to because of certain barriers. All the participants in these meetings, both from the intelligence community and the critical infrastructure sectors, expressed worked with enthusiasm and looked forward to building relationships that will help solve these key problems going forward.

The Study Group is currently drafting a report as they conduct a small case study effort to add specific examples to illustrate the findings. The four cases the Study Group is using are:

- the August 2003 blackout,
- the July 2004 financial services terrorist alert when the threat level was raised to orange,
- the July 2005 London bombings that happened on two separate dates, and
- the September 2005 public transit alert in New York and New Jersey

Each case contains specific differences and will provide unique perspectives. The blackout and the bombings involve information sharing and investigations after an event. The other two involve information shared after analyzing intelligence and leading up to decisions made in the financial services, public transit, and other affected sectors. All four cases involve lessons learned regarding who the key decision makers were, whether they were included in information distribution and whether the information originators knew who needed what information when.

The purpose of the case studies is not to point fingers but to see if the Study Group can improve the processes that are in existence or that do not exist yet. Mr. Watson thanked Ms. Robin Roberts from Cisco Systems and Mr. Bob Beecher and Ms. Gail Kaufman, both with DHS, for their hard work in supporting this effort. The ongoing CEO strategic vision survey will add an important perspective that only a group like the NIAC can provide. At the operational level, decisions are made to prepare for or react to incidents. At the CEO level, the decisions are about managing risks, core values, prioritizing investments and allocating resources for the benefit of customers and interest of the industry. Information sharing is vital to both levels, but an understanding of the decision making process is important so the right information is provided to both levels. Mr. Watson then turned the floor over to Vice Chairman Chambers.

Vice Chairman Chambers added that although CEOs need to be involved in the operational issues, the key takeaway here is the primary focus is on customers, risk management, long-term effects and strategies for success. The Vice Chairman then asked for Mr. Alfred Berkeley to provide comments.

Mr. Berkeley told the NIAC the Working Group is trying to take what they learned from their research and apply it to discussions with 20 to 25 CEOs from the perspective that the corporation has an adversary that will not go away.

Sample questions to the CEOs include:

- How has the reality that this adversary is not going away changed your approach to your investments, your ability to be resilient, and/or your planning?

- From your point of view as a CEO, what would it take to have a more effective relationship with the government, particularly the intelligence community?

Mr. Berkeley believes it is not a complicated mission and he told the Council that he plans to do this during March. He also asked the NIAC CEOs for their participation and help in getting other CEOs from their sector to participate.

Chairman Nye asked Mr. Berkeley if it would be possible for Mr. Berkeley to let the NIAC members know if he wanted to talk to someone from their sector. Mr. Berkeley agreed.

Chairman Nye turned the microphone back to Mr. Watson. Mr. Watson stated the Working Group would wrap up the case studies and CEO questionnaires by incorporating them into the report by the end of March. Coordination between the government and the private sector does have its challenges, but the Study Group has developed some clear requirements for information sharing, dependent on multiple inputs. The Working Group also understands the need to protect sources, classification and expertise, making the information sharing process complex. Sometimes, the government industry analysts do not have the industry expertise to know whether a piece of information is important, and sometimes the private sector does not know how to input that information, or their requirements into the intelligence process. Now, how a sector decides to provide that expertise will depend on the sector and other constraints. Since the sectors are different they will respond to this differently, and the Group will outline these differences as options in the report.

Mr. Watson expressed the existence of four key requirements for the Intelligence Coordination Working Group. First, there is a need to fuse information from intelligence, law enforcement and other sources at the national level. There needs to be a capability to fuse information from multiple sources that look at different perspectives. Secondly, intelligence analysts need access to industry-specific expertise, and this can only come from relationships of trust. Third, the private sector needs to know how to provide inputs into intelligence requirements. Finally, sensitive information not covered by government classification must be protected but also must be shared with decision makers who need to know. So the identification of decisions makers and the protection and sharing of information has become critical.

Mr. Watson explained to the meeting attendees the Study Group discovered they need to provide clear definitions. The term intelligence means something different to the intelligence community than it does to the business community. The Study Group found other terms that have multiple meanings for different participants. The more the group looks at the information sharing needs, the more they understand the lack of a need for sharing classified information with private sectors owners and operators for most phases of protecting critical infrastructures.

The New York Police Department's (NYPD) approach underscores this fact with their Area Police/Private Security Liaison (APPL) and other programs. The NYPD has given the Study Group several presentations about their programs, showing the ways to protect classified sources and methods and also to get timely information to decision makers at the unclassified level. Lastly, the Study Group does not anticipate the need for new federal funding. Substantial investments have already been made so tweaking of existing charters or modification of existing information sharing mechanisms may have to be done, but planned appropriations should be sufficient. Mr. Watson asked Chief Gallegos, Co-Chairman of the Working Group to add his comments regarding the law enforcement perspective.

Chief Gallegos began by stating that the Working Group wants to make it understood in the intelligence coordination process that law enforcement is the center point and more needs to be done to bring them into the process. He thanked the NYPD and the Los Angeles Police Department (LAPD) for their help in the development of the Intelligence Coordination report. He stressed the report will show law enforcement must have an active part in the intelligence coordination process. The Nation needs law enforcement to participate in intelligence coordination because the combination of domestic intelligence and foreign intelligence helps the agencies combat terrorism. The Working Group must add law enforcement depth into the report as they move forward. He suggested the Working Group initiate a follow-up project for a task force to identify all the law enforcement needs to play. Chief Gallegos reiterated the complexity of the issue of the relationship between law enforcement and the intelligence community and the need to bring the two sides together. He then turned the floor over to Vice Chairman Chambers.

The Vice Chairman thanked Chief Gallegos. He then asked the Council for constructive feedback on the report.

Chairman Nye asked Vice Chairman Chambers if the NIAC would have the final report before the April meeting, and the Vice Chairman confirmed this.

Under Secretary Foresman told Vice Chairman Chambers that DHS has had some phenomenal advancement just over the course of the last ninety days across the entire Federal government with information sharing and intelligence efforts. Under Secretary Foresman asked Assistant Secretary Stephan to make sure Assistant Secretary for Information Analysis Charlie Allen and his team give the NIAC an update on the most current environment with the information and intelligence sharing efforts that DHS has because two important things may result. One, it may help the NIAC adjust their perspective of intelligence coordination because there has even been a lot of change since the London bombings. It may also help because the NIAC could ask Assistant Secretary Allen to make some changes quickly regarding intelligence coordination.

Vice Chairman Chambers thanked Under Secretary Foresman for the idea and asked Mr. Watson to initiate the process by calling Assistant Secretary Allen.

Chairman Nye told the Vice Chairman he and his group may want to take the questionnaires to the trade associations because many CEO will listen to the trade associations if they recommend something for the industry. The Chairman then thanked Vice Chairman, Mr. Berkeley, Chief Gallegos, and Mr. Watson for their intelligence coordination update.

B. 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

Chairman Nye asked the Council and other meeting attendees to shift their focus to the Workforce Preparation, Education and Research Working Group. He invited Dr. Linwood Rose and Mr. Berkeley to present their status update on the topic.

Mr. Berkeley told the meeting participants the group has completed almost 75 percent of the final report, and they continue to work on the K-12 section of the report. The Working Group undertook the workforce preparation issue because the country cannot have a secure cyber infrastructure unless there is an educated workforce.

Since the NIAC last met in October, the Study Group reviewed a National Academies of Sciences report titled *Rising Above the Gathering Storm, Energizing and Employing America for a Brighter Future*. The work in this report complements what the NIAC Workforce Working Group is doing, and the Working Group will endorse the recommendations of that report. The Department of Education and Congress are in the process of preparing legislation that would significantly increase the number of math and science teachers and math and science students in school systems. Also, the program manager for the Department of Defense's Scholarship for Service program spoke to the Working Group on the program's progress. The Working Group heard from the Executive Director of the Baltimore Curriculum Project (BCP) regarding the Direct Instruction (DI) approach to teaching, a back to basics model that works effectively. Mr. Berkeley stated he and his team have started working these presentations into their final report. Mr. Berkeley asked Dr. Rose if he wished to add anything. Dr. Rose reiterated the report would be in its completed state prior to the April meeting. They only need to finish the K-12 Section and insert the Cyber Corps recommendation.

Chairman Nye expressed his appreciation for the update but told the presenters that the research material for this group is time sensitive so it is good that they are releasing the report soon.

Vice Chairman Chambers thanked Mr. Berkeley and Dr. Rose for their solid work on this Working Group. He feels that this report will really makes a difference upon its release.

C. Chemical, Biological and Radiological Events and the Critical Workforce Working Group

Chief Rebecca F. Denlinger, Fire Chief, Cobb County, Georgia Fire and Emergency Services, NIAC Member, *Martha H. Marsh*, Chairman and CEO, Stanford Hospital and Clinics, NIAC Member, and *Bruce Rohde*, Chairman and CEO Emeritus, ConAgra Foods, Inc

Chairman Nye introduced the next initiative, Chemical, Biological and Radiological Events and the Critical Infrastructure Workforce. The Council asked Chief Rebecca Denlinger, Ms. Martha Marsh and Mr. Bruce Rohde to chair this Working Group, and they have obliged. Chairman Nye asked Chief Denlinger for some introductory comments.

She stated the Working Group has already defined the scope of their undertaking and identified an approach. Chief Denlinger asserted the timeline appears short for the completion of the project, but because this issue deals with matters of urgency, it appears necessary to hasten the process. Chairman Nye agreed, and told her that while it may be necessary to work quickly on this project, the Working Group needs to work carefully and thoroughly.

Mr. Rohde told Chairman Nye the NIPP has the concept of awareness as one of its pillars, and he felt the Working Group should take time to include this concept into its recommendations.

Following Mr. Rohde's comment, Ms. Marsh asked Mr. Scott Blanchette to begin the Chemical, Biological and Radiological (CBR) Events presentation. As a new Working Group, the CBR Working Group planned to deliver three topics at the meeting. They wish to review the objective and scope, outline an approach for tackling the question, and validate the next steps that follow. The Group outlined its objective to provide recommendations for keeping those who maintain and work in areas of the critical infrastructure (CI) safe, healthy, ensure they have the tools, training and equipment to recover in the event of a chemical, biological or radiological emergency. Mr. Blanchette said the Working Group will identify critical infrastructure operating personnel and the CBR requirements. Secondarily, they want to identify how those needs are currently being handled, specifically public health and emergency response organization. Thirdly, they want to identify gaps and solutions that will strengthen the capabilities of CI operating personnel in case of a CBR event.

The approach will differ from previous Working Groups in terms of organization and answering the question. The CBR Working Group plans to form a core Working Group that remains constant throughout the process, comprised of the NIAC members. Secondarily, they will form a core Study Group, which will be consistent throughout the process as well. Core Study Group participants will include NIAC POCs, the NIAC Secretariat, and various sector specialists from DHS and other government agencies who will support the Group throughout the life of the project. Supporting this should be a topic-specific group with specific expertise in at least one of the three events. The unique nature of the chemical, biological and radiological questions suggests that the Working Group needs subject matter experts who understand the problem statement with a high degree of detail and specifically, how these threats may impact the critical infrastructure worker. Supporting these core Working Groups and Study Groups will be three distinct chemical, biological and radiological Study Groups that will work in series throughout the life of the project.

The proposed timeline for this Working Group will likewise differ from past Working Groups. The CBR Working Group will work toward three deliverable milestones addressing each of the topics as separate deliverables with a final deliverable that will address all of the topics and their interdependencies. The Group proposed to put together a Biological Study Group with the intention of providing an initial deliverable at the July 2006 NIAC meeting. Following that meeting, they will put together a Chemical Study Group with the intention of putting together a deliverable in the December 2006 meeting and put together a Radiological Study Group, with a deliverable due date of July 2007. Also during that July 2007 meeting, the CBR Working Group will want to put together one document that identifies trends, interdependencies or links between these three topics.

This approach allows the Group to offer valuable threat-specific recommendations earlier than the final July 2007 date, while also delivering a comprehensive set of recommendations that address the entire question along a timeline that allows the study of the unique nature of each threat. Mr. Blanchette then asked the Council for feedback on the outline he and the CBR Study Group have put forward. Next, he said the Working Group wants to gain a consensus on the deliverables and then gain an endorsement on the approach, specifically around the Study Group addressing biological events first, chemical events second, and radiological events third. Finally, he asked if they could solicit NIAC members for Points of Contact or Subject Matter Experts with knowledge in chemical, biological or radiological threat, vulnerabilities or more specifically response capabilities across the critical infrastructure.

Chief Denlinger then asked the NIAC for any response to the approach the Group had formulated.

Assistant Secretary Stephan stated DHS appreciates this Working Group's timeliness and order of activities because the Federal government has a biological issue it currently has to address, avian flu. DHS has done a lot of groundwork with their private sector counterparts over the last several months, beginning with the President's strategy announcement last October. Mr. Jim Caverly, the Director of the Infrastructure Partnership Division, and his shop have been working aggressively across various sectors to help get a handle on how exactly pandemic influenza might affect the critical infrastructure sectors and what kinds of things the government and the private sector can do in advance to kind of stay ahead of developments in the avian flu. The Assistant Secretary stated DHS would love to feed all of their previous efforts up to this point into this Working Group, and in return, DHS would ask for any insight developed by the Working Group.

Chief Denlinger expressed her interest in the collaboration between the Working Group and DHS, because this would help the Working Group with its report and help DHS with its protection against the avian flu.

Ms. Marsh told the group that the Chief of Infectious Diseases from Stanford, who has a breadth of knowledge in biological events, has offered to provide advice to the Working Group.

Assistant Secretary Stephan told the meeting participants that after the DHS Second Stage Review, he took over the former elements of FEMA that were responsible for chemical and radiological stockpile emergency preparedness.

Chairman Nye added that the nuclear industry has many experts that could add input, and Mr. Bill Muston could provide the Working Group with their names. Obviously, this has to take place in order so Mr. Muston will provide the names when the group gets to the radiological events section.

D. 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 Services Corporation, NIAC Member.

Chairman Nye asked the Council to move to the topic of the convergence of physical and cyber technologies and related security management challenges, chaired by Mr. George Conrades, Ms. Margaret Grayson, and Mr. Greg Peters.

Ms. Grayson thanked the Chairman and the rest of the Council. She said that the President, through the Council, 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 and technologies converge and network management for both consolidates, this Working Group finds it appropriate to consider whether industry and the government adequately address vulnerabilities. The Working Group also wants to consider what actions might be appropriate to address this important issue. The topic covers Supervisory Control And Data Acquisition systems (SCADA) and Process Control Systems (PCS) for production facilities and infrastructure services, an area where the impact or consequences of vulnerabilities can be extremely significant, like water systems and power grids. The Working Group has begun by considering key questions that must be explored. They have focused on providing well-considered and actionable recommendations-recommendations that can be clearly measured and monitored during the implementation phase. Ms. Grayson then asked Mr. David Frigeri, from Internap, to provide the Convergence presentation.

Mr. Frigeri thanked Ms. Grayson and began the presentation. He stated that his purpose at the meeting was to present the group's actions, initial findings and next steps. The purpose of the Group is ultimately to investigate opportunities for improvement in better protecting national critical infrastructure from cyber threats. The Study Group developed five framework questions as the foundation of the mission. They have also identified and invited infrastructure sectors that include electric, other energy, water and chemical. Mr. Frigeri and the NIAC Secretariat have invested a lot of time in educating the Study Group with briefings from Cisco, DHS and Idaho National Labs. The Group needed to develop an understanding of what SCADA and PCS are and how they can be compared and contrasted with business operations systems. From that perspective they share a couple of commonalities, one commonality being that the world is more interconnected with the Internet, Virtual Private Networks, dial-up modems. SCADA, PCS and normal business operations systems share similar underlying technologies in the TCP/IP and Ethernet protocols and in operating systems.

How the SCADA, PCS and normal business operations systems differ also interests the Study Group. One way they differ most significantly is in the consequences of their exploitation. If a business operations system is exploited, the company can expect something along the lines of lost revenue, decreased employee productivity, and maybe some loss of goodwill with their customers. SCADA and PCS exploitation can lead to physical damage, broad economic impacts and potential loss of life.

The Study Group also plans to look into the great deal of work that has been done from a physical and a cyber security perspective for business operations systems. There are many organizations, programs and processes in place for collecting and disseminating data in a way that is both safe for industry and useful for government. The Study Group plans to do the same with SCADA and PCS. SCADA and PCS have not adequately been included with all the other security and cyber security work that already exist. The Study Group's five framework questions will help them understand the broad topic and break it down into interrelated sections with answerable questions.

The first topic the Study Group has developed is "Security as an Enabler." Historically, the main goals of critical infrastructure managers have been reliability, availability and safety. A goal of the Study Group is to directly connect how owners/operators protect critical infrastructure from cyber threats, how that can lead to improved availability and reliability and safety. The Study Group has already found a number of examples available for review. As an example of how we can better educate the marketplace, the Study Group will try to answer the question: if your systems are attacked, could you potentially lose visibility or control over your infrastructure, critical infrastructure?

"Market Drivers" is another topic the Study Group believes will help create recommendations. Vendors need a market to which they can sell, and customers must have a clear need in order to justify the purchase of hardware and software that will protect against cyber threats.

With the "Executive Leadership Awareness" topic, the Study Group's objective is to share information with executives by having an outreach program to executives in the private sector, educating them in terms of what they can do to ensure that they not only protect against the threats to their brand or customer relationships, but also the economic and human tolls that could happen. Mr. Frigeri stated that the Study Group would like to provide executives with answers, like intrusion rates of all reported systems and whether or not an intrusion would cost a company more than a million dollars. We want to provide data to chief executives so they can start to quantify and put some definition around what that would mean for their own businesses.

The topic of "Federal Government Leadership Priorities" gave the Study Group the initial observation that there is an opportunity to illuminate some redundant efforts. There is also an opportunity to improve information sharing and an opportunity to improve public-private partnerships.

"Improving Information Sharing" is the final topic. Agencies and the private sectors have done a great deal of work to measure physical and cyber security faults and attacks. The Study Group wants to pull in data on attacks specific to SCADA and PCS that may not be being tracked today, so there are programs and infrastructure in place for future efforts. Mr. Frigeri said the Study Group has taken as their responsibility to articulate a way organizations can provide this information safely, allowing both owners/operators and the government to utilize the information.

Mr. Frigeri stated that the group is crafting an overview draft report they plan on completing by March 16th to present to the Study Group. The Study Group will continue to receive briefings from both private and public sector.

Ms. Grayson thanked Mr. Frigeri and asked if Mr. Greg Peters, another chairperson for the Working Group, has anything else to add.

Mr. Peters thanked Ms. Grayson and Mr. Frigeri for their presentation and hard work on the Study Group. He commented that they held a conference call every week to discuss a different facet of the topic, which has allowed the Study Group to gain a great depth of knowledge on the subject. Mr. Peters also highlighted three of the topics discussed by Mr. Frigeri. First, the Study Group has seen a significant amount of work, but there is a great deal that they have not seen. Second, the Study Group has focused on the fact that there are various ages of infrastructure. Some of it is still working after 25 years, and those companies with the older equipment do not see the Return on Investment (ROI) to upgrade to systems that would be a more resilient infrastructure for IT and control systems. This is a big issue because if they cannot identify the ROI, rarely are they going to take action to upgrade their infrastructure. The final question highlighted by Mr. Peters was the question of standards and what the standards should be for security in this area, across disparate industries and entities. Mr. Peters said this is a very difficult question, but the Study Group has made significant progress and their work on it will grow in importance as the Study Group's mission closes.

Chairman Nye reached out for the Council to provide more comments for the Working Group. He then asked if there is a place for best practices like industry and regulatory standards to have a role. Mr. Peters stated that there does not appear to be a role for regulation. He continued by saying that the Working Group wants to make sure the operational and executive leadership understand the problems of the cyber threats to SCADA and PCS before they look into anything regarding regulation.

Ms. Grayson brought up the fact that the Study Group noted that often as legacy systems are modernized, this increases the possibility of exposing vulnerabilities, a possibility the Study Group will have to take into consideration when developing recommendations.

Chairman Nye asked Ms. Grayson if the Working Group has a sense of when the recommendations would be completed, and Ms. Grayson answered that it is too early in the process because they are still gathering information.

Mr. Berkeley added that the Study Group may want to engage the insurance industry, because they study business continuity and can put numbers on the situations that the Study Group has discussed. Ms. Grayson thanked Mr. Berkeley and told the Council that the Study Group will look into individuals in the insurance industry who could help them create recommendations.

VI. NEW BUSINESS — NIAC Chairman *Erle A. Nye* Presiding

A. STATUS REPORT ON IMPLEMENTATION OF RECOMMENDATIONS

Chairman Nye shifted the focus of the conversation to the status of the implementation of the NIAC's previous recommendations. He asked Ms. Nancy Wong, a DFO of the NIAC, to present a report on the status of implementation of the hard work of the Council.

Ms. Wong thanked the Chairman. She stated the NIAC has asked for a report on a regular basis regarding the status of the recommendations of this Council. On the morning of the meeting, DHS sent a pre-decisional document to all the members with a format and a layout for reporting on the status of those reports. DHS will provide the Council feedback twice a year on the status recommendations directed towards the agency itself. DHS will consistently track the implementation of the recommendations within each of its Directorate, and the White House will lead the status tracking for inter-agency implementation of the recommendations. DHS will collect the feedback the White House collects and place it in the recommendation tracking document, along with the feedback from the DHS Directorates. The report will consist of a status in terms of acceptance of the recommendation plus actions being taken and who it is assigned to in terms of agency. Ms. Wong asked the Council members for feedback on the format of the recommendation tracking report.

Chairman Nye thanked Ms. Wong for her presentation because the Council appreciates seeing the actions within agencies that their recommendations provide.

Vice Chairman Chambers agreed with the Chairman, saying the Council likes to see this feedback because it shows the Council the value of their work. The Vice Chairman asked the Council to review the format to make sure it contained all it needed.

VII ADJOURNMENT — NIAC Chairman, *Erle A. Nye*

Chairman Nye told the Council the meeting was about to be adjourned. The next meeting will be a teleconference scheduled for April 11, 2006 at the Grand Hyatt at Washington Center. This is located at 1000 H Street, NW Washington, DC, for those who can attend in person. The third meeting of the year is tentatively scheduled for July 11, 2006, and the President may wish to see the Council during this part of the summer. The Chairman asked the Council to put both meetings on their calendars and attempt to attend the July meeting in person. Chairman Nye also said the Council should hear a few reports at the April meeting, and he is looking forward to them. The Chairman then thanked everyone at the Press Club and on the phone for their participation in the meeting. He cited their busy schedules and the fact that they are still able to provide input to this important effort. Chairman Nye asked Assistant Secretary Stephan if he has any closing comments.

The Assistant Secretary thanked the NIAC for all they are doing, stating DHS truly appreciates the partnership because it allows the private sector and the government to work together to secure the country's critical infrastructure. The NIPP will further define the work within the 17 sectors.

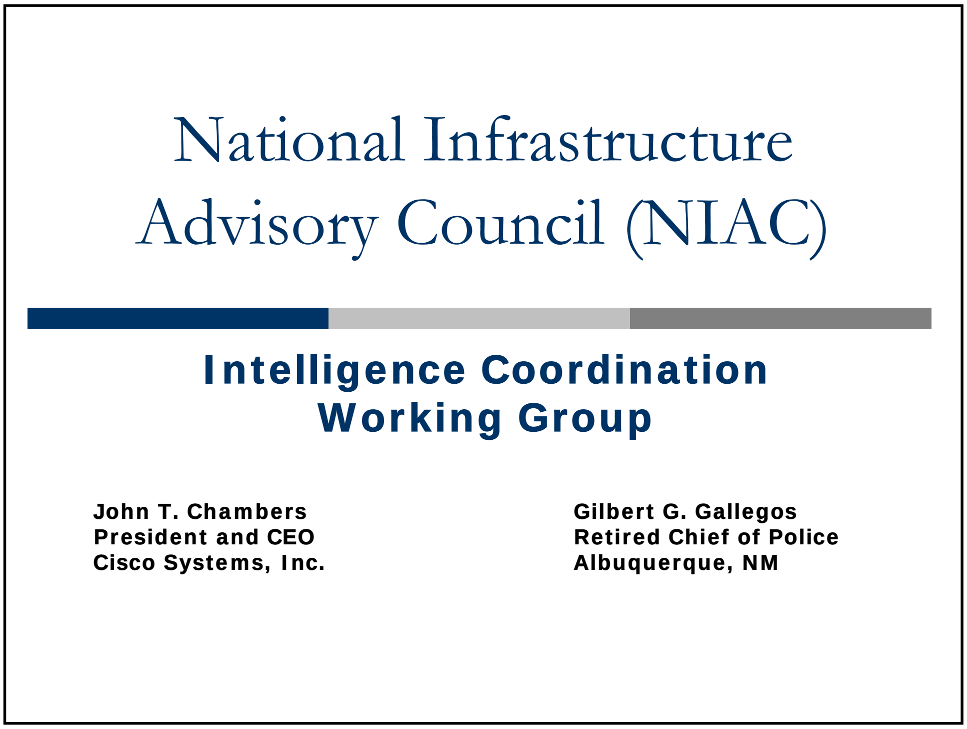
At this point, Chairman Nye again thanked the Council, and adjourned the meeting.

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: _4/11/06____
Erle A. Nye, Chairman

ATTACHMENT A

Intelligence Coordination

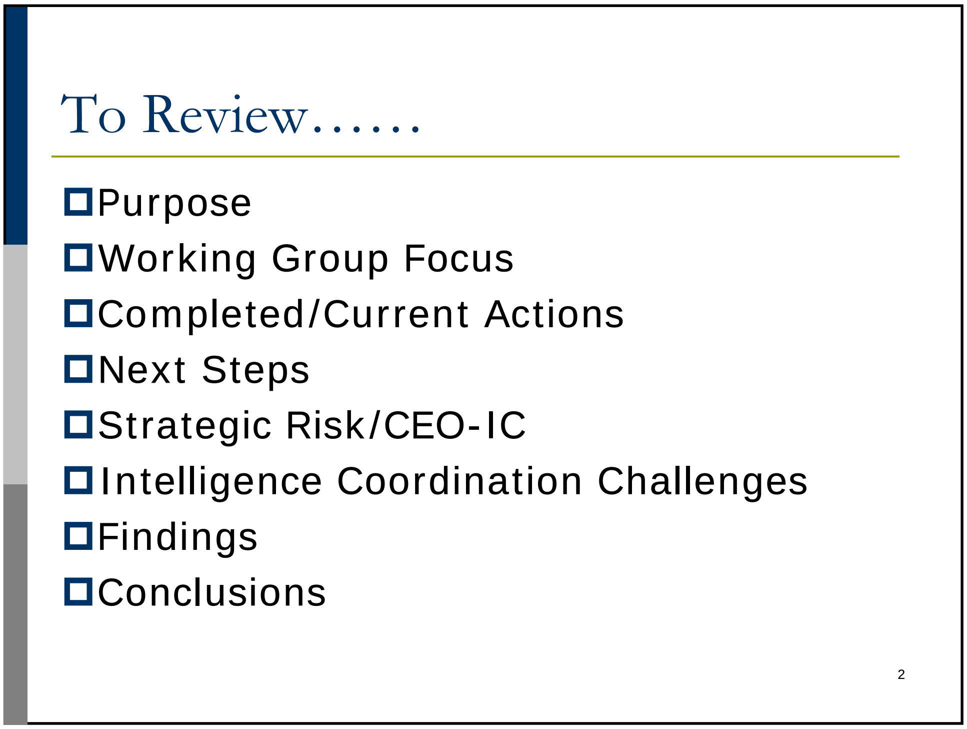


National Infrastructure Advisory Council (NIAC)

Intelligence Coordination Working Group

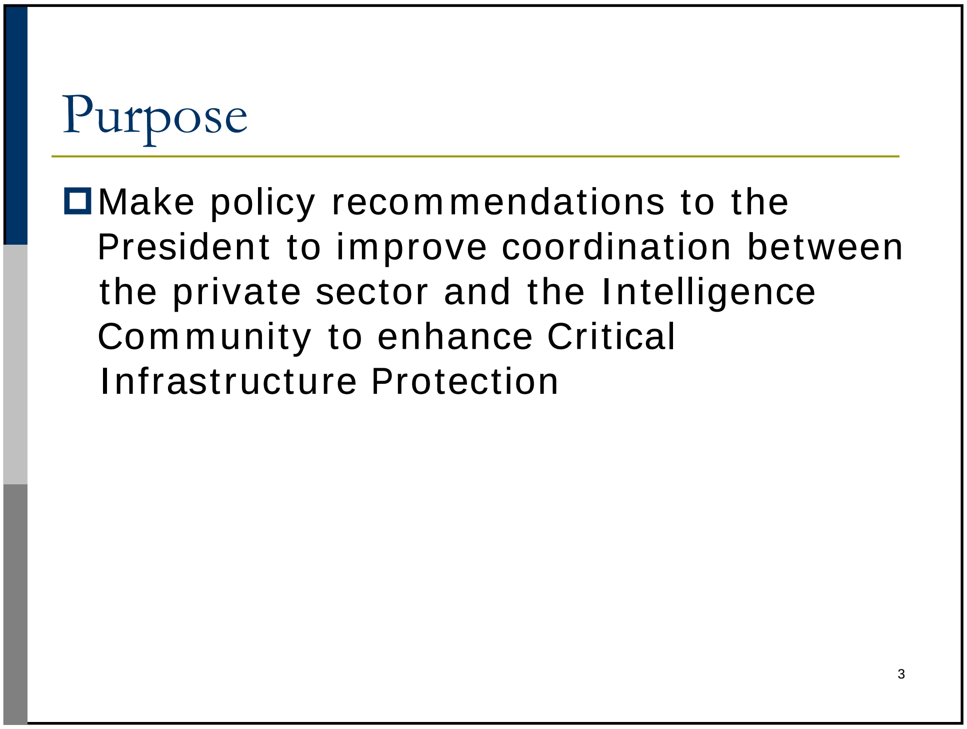
John T. Chambers
President and CEO
Cisco Systems, Inc.

Gilbert G. Gallegos
Retired Chief of Police
Albuquerque, NM



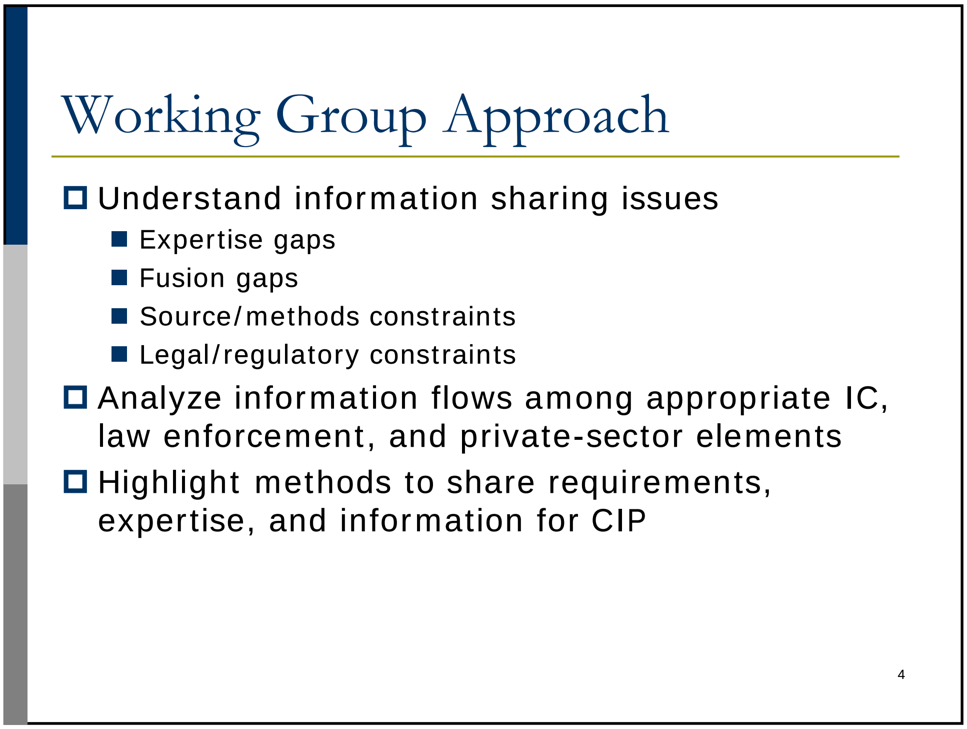
To Review……

- □Purpose
- □Working Group Focus
- □Completed/Current Actions
- □Next Steps
- □Strategic Risk/CEO-IC
- □Intelligence Coordination Challenges
- □Findings
- □Conclusions



Purpose

- □ Make policy recommendations to the President to improve coordination between the private sector and the Intelligence Community to enhance Critical Infrastructure Protection



Working Group Approach

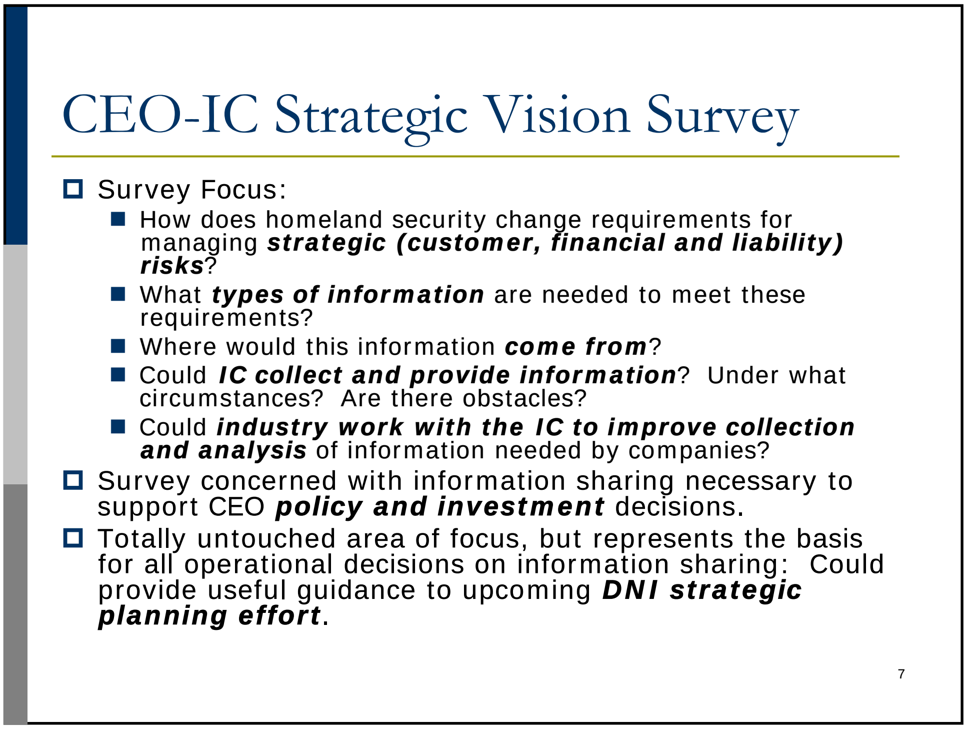
- □ Understand information sharing issues
  - ■ Expertise gaps
  - ■ Fusion gaps
  - ■ Source/methods constraints
  - ■ Legal/regulatory constraints
- □ Analyze information flows among appropriate IC, law enforcement, and private-sector elements
- □ Highlight methods to share requirements, expertise, and information for CIP

Completed/Ongoing Actions

- □ Completed 12+ month dialog among critical private-sector representatives and the IC
- □ Educated Working Group members on IC, DHS information flows, and support to the private sector
- □ Analyzed how intelligence is integrated to support CIP
- □ Conducted information sharing and expertise gap analysis
- □ Examined law enforcement information reporting mechanisms
- □ Conducting information flow case studies on four recent events
- □ Concluding CEO-IC Strategic Vision survey
- □ Writing initial draft of NIAC report

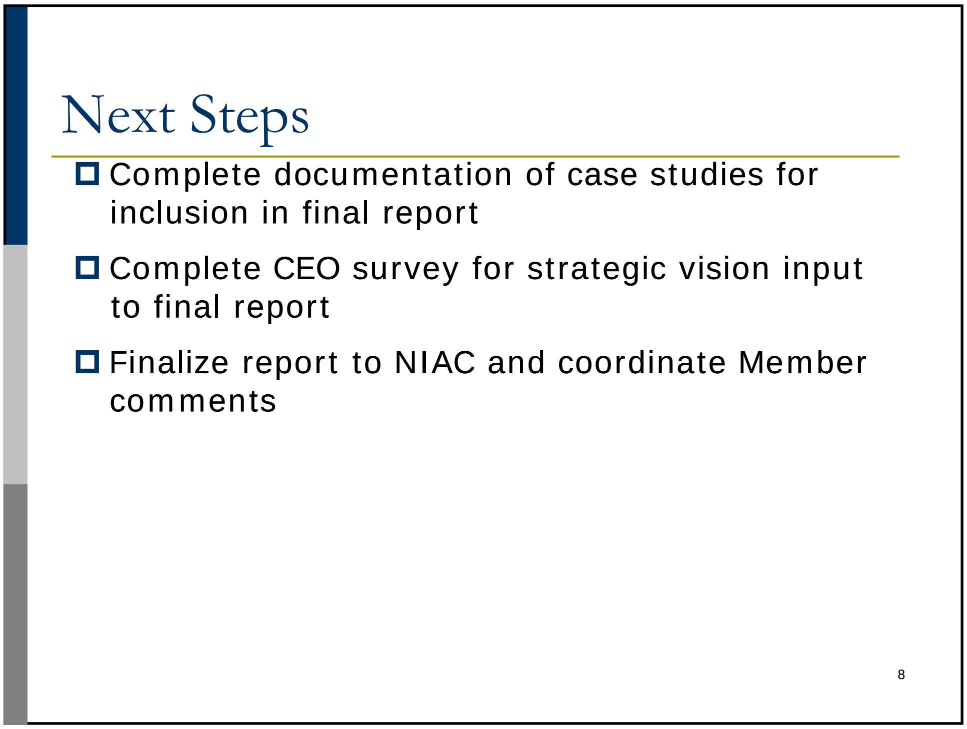
Strategic Risk Management

- □ Changing culture: Need to incorporate security into normal business risk decision-making framework and structure
- □ Based on what is known, what is affordable, and what consequences must absolutely be avoided to maintain viability of institution
- □ Business risk management affects business risk calculation and acceptance, financial investments, operational processes, and contingency planning



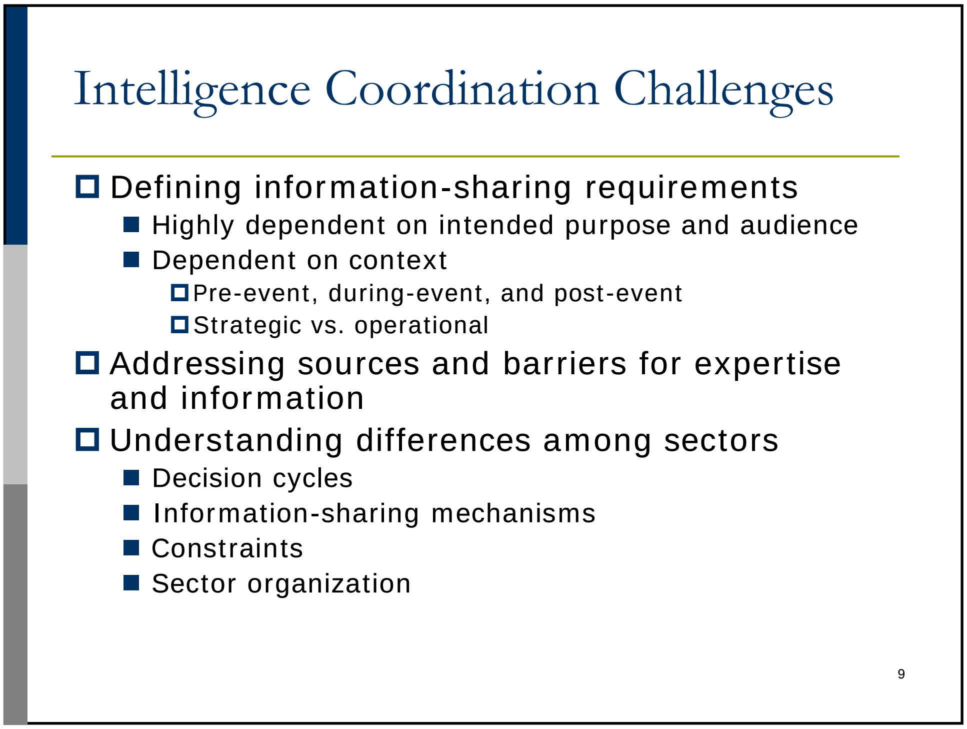
CEO-IC Strategic Vision Survey

- Survey Focus:
  - How does homeland security change requirements for managing ***strategic (customer, financial and liability) risks***?
  - What ***types of information*** are needed to meet these requirements?
  - Where would this information ***come from***?
  - Could ***IC collect and provide information***? Under what circumstances? Are there obstacles?
  - Could ***industry work with the IC to improve collection and analysis*** of information needed by companies?
- Survey concerned with information sharing necessary to support CEO ***policy and investment*** decisions.
- Totally untouched area of focus, but represents the basis for all operational decisions on information sharing: Could provide useful guidance to upcoming ***DNI strategic planning effort***.



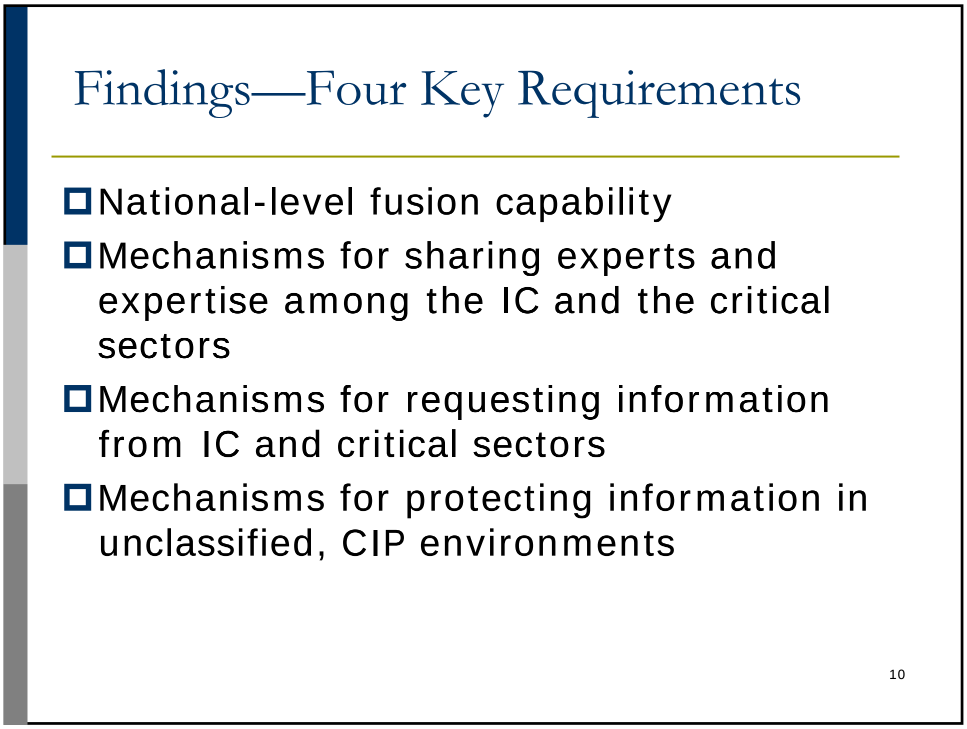
Next Steps

- Complete documentation of case studies for inclusion in final report
- Complete CEO survey for strategic vision input to final report
- Finalize report to NIAC and coordinate Member comments



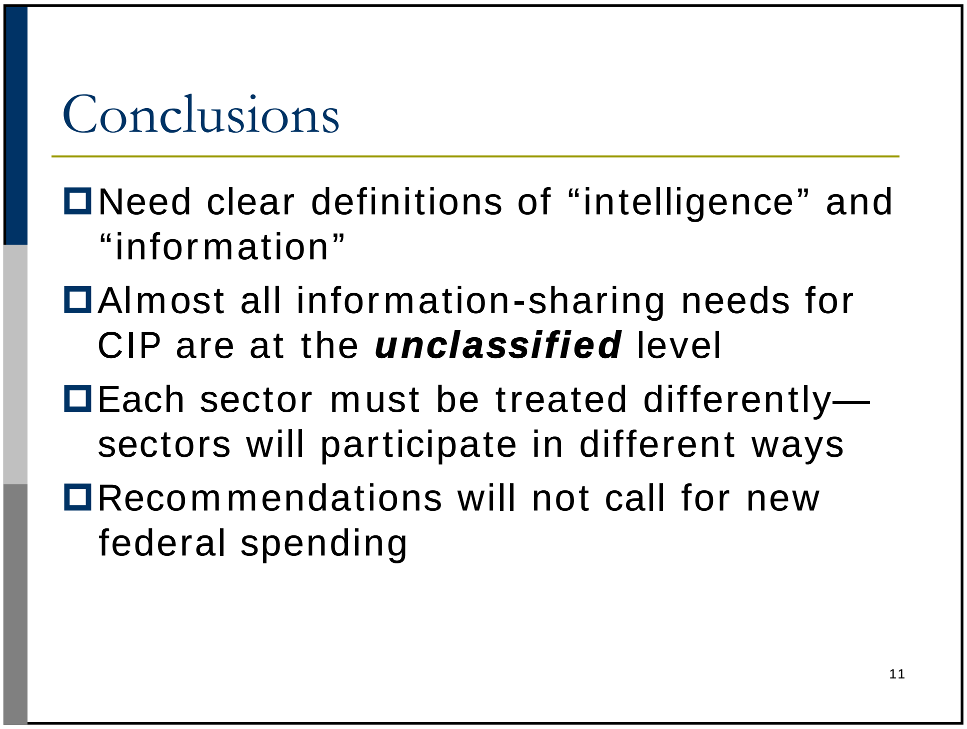
Intelligence Coordination Challenges

- Defining information-sharing requirements
  - Highly dependent on intended purpose and audience
  - Dependent on context
    - Pre-event, during-event, and post-event
    - Strategic vs. operational
- Addressing sources and barriers for expertise and information
- Understanding differences among sectors
  - Decision cycles
  - Information-sharing mechanisms
  - Constraints
  - Sector organization



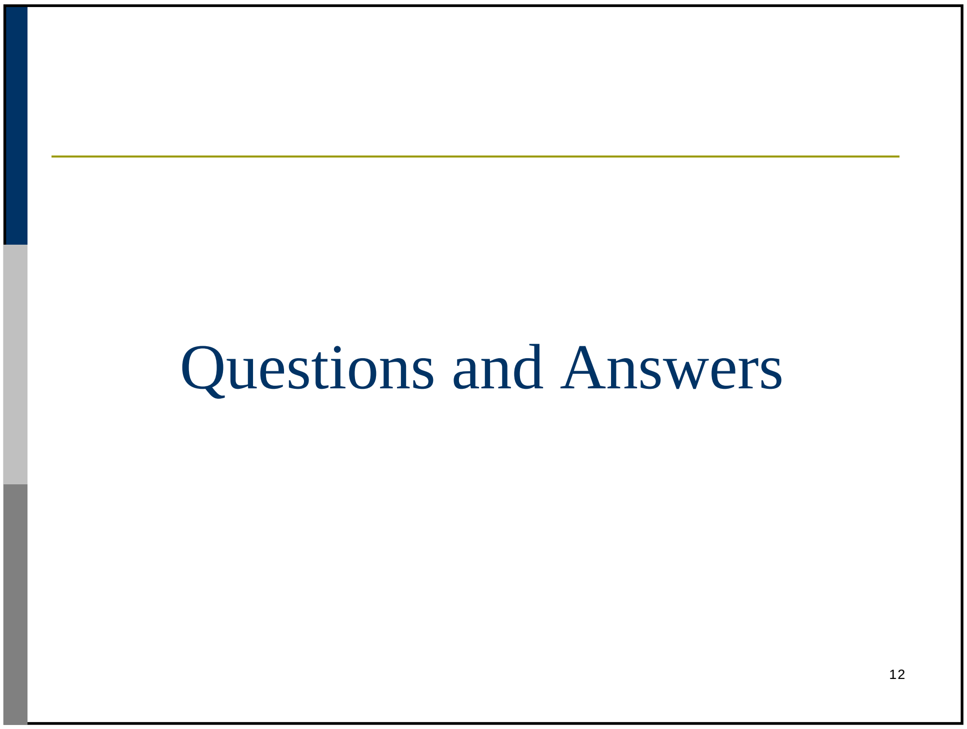
Findings—Four Key Requirements

- National-level fusion capability
- Mechanisms for sharing experts and expertise among the IC and the critical sectors
- Mechanisms for requesting information from IC and critical sectors
- Mechanisms for protecting information in unclassified, CIP environments



Conclusions

- □ Need clear definitions of “intelligence” and “information”
- □ Almost all information-sharing needs for CIP are at the ***unclassified*** level
- □ Each sector must be treated differently—sectors will participate in different ways
- □ Recommendations will not call for new federal spending



Questions and Answers

ATTACHMENT B

Workforce Preparation, Education and Research

National Infrastructure Advisory Council (NIAC)

Workforce Preparation, Education and Research Working Group

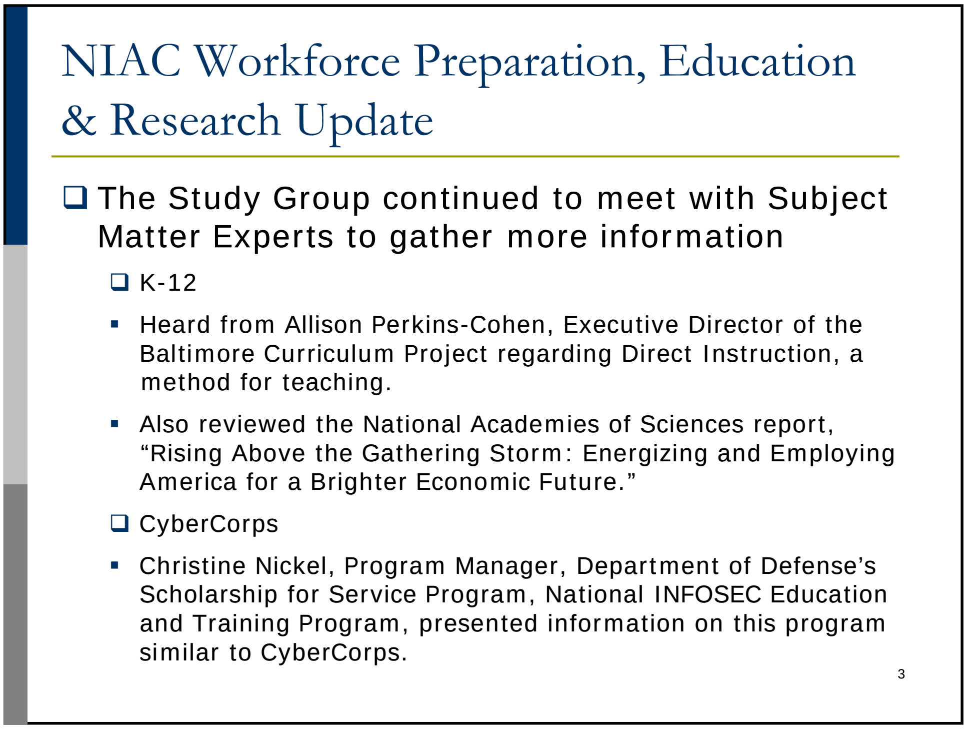
Status Report
February 13, 2006

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

Dr. Linwood H. Rose
President
James Madison University

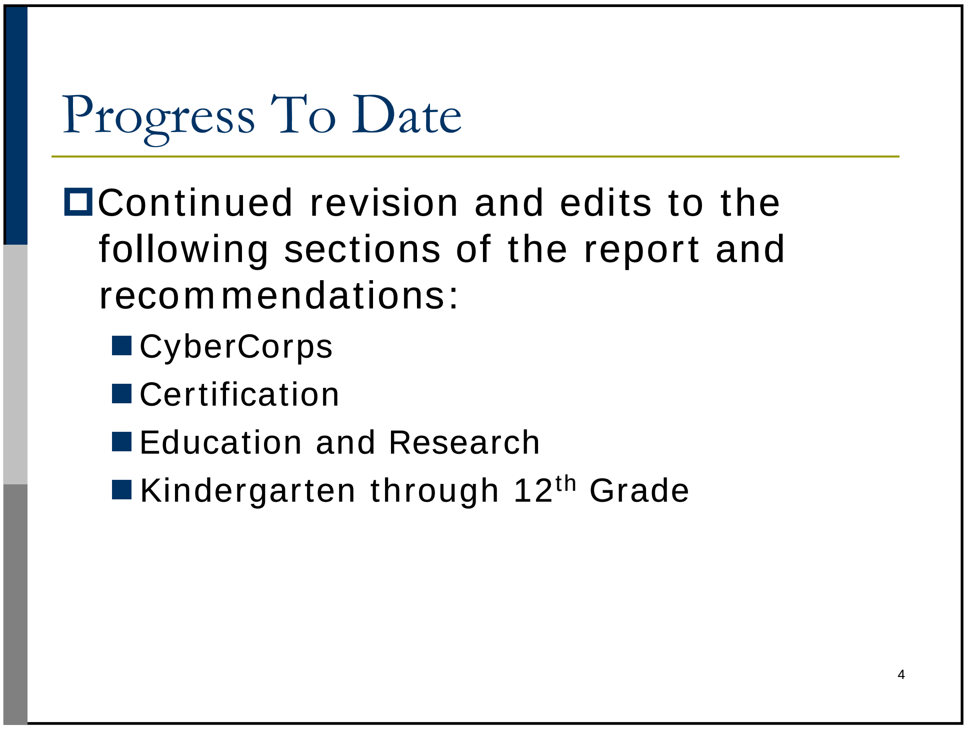
Mission

❑ Determine what can be done to ensure the current and future workforce is able to meet the nation’s needs to secure cyber-based critical infrastructures.



NIAC Workforce Preparation, Education & Research Update

- ❑ The Study Group continued to meet with Subject Matter Experts to gather more information
  - ❑ K-12
    - Heard from Allison Perkins-Cohen, Executive Director of the Baltimore Curriculum Project regarding Direct Instruction, a method for teaching.
    - Also reviewed the National Academies of Sciences report, “Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future.”
  - ❑ CyberCorps
    - Christine Nickel, Program Manager, Department of Defense’s Scholarship for Service Program, National INFOSEC Education and Training Program, presented information on this program similar to CyberCorps.



Progress To Date

- ❑ Continued revision and edits to the following sections of the report and recommendations:
  - CyberCorps
  - Certification
  - Education and Research
  - Kindergarten through 12th Grade

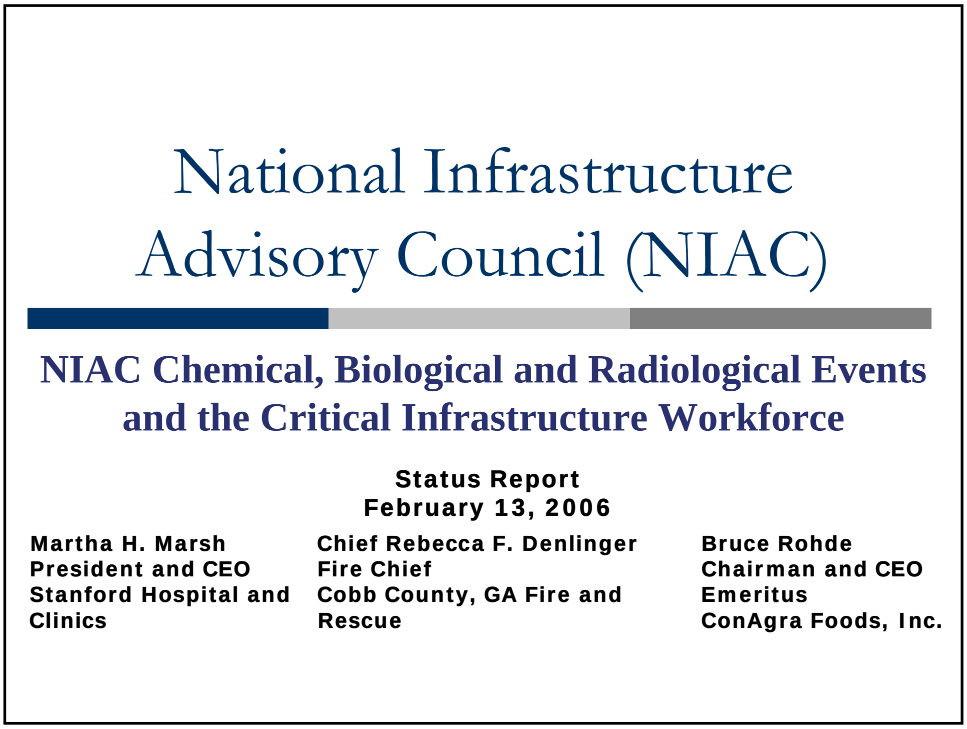
Next Steps

- ❑ Wordsmith and format entire report.
- ❑ Send to Designated Federal Officer for review.
- ❑ Send to NIAC to review 30 days prior to Spring meeting.
- ❑ Have final report and recommendations ready for April NIAC meeting.

Questions?

ATTACHMENT C

Chemical, Biological and Radiological Events and the Critical Infrastructure Workforce



National Infrastructure Advisory Council (NIAC)

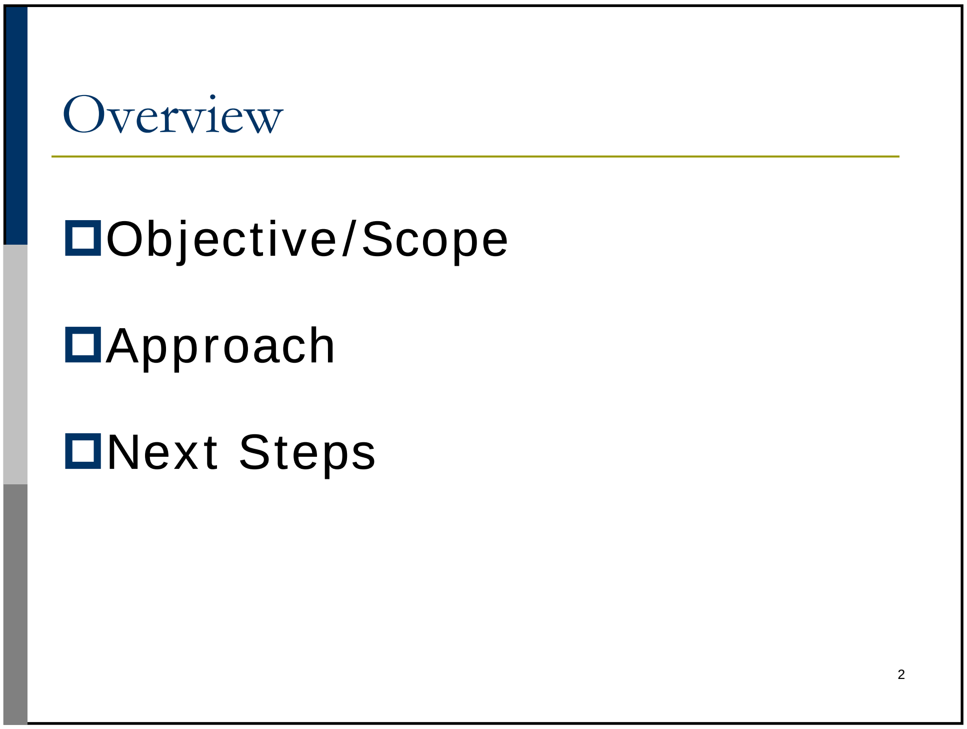
NIAC Chemical, Biological and Radiological Events and the Critical Infrastructure Workforce

Status Report
February 13, 2006

Martha H. Marsh
President and CEO
Stanford Hospital and Clinics

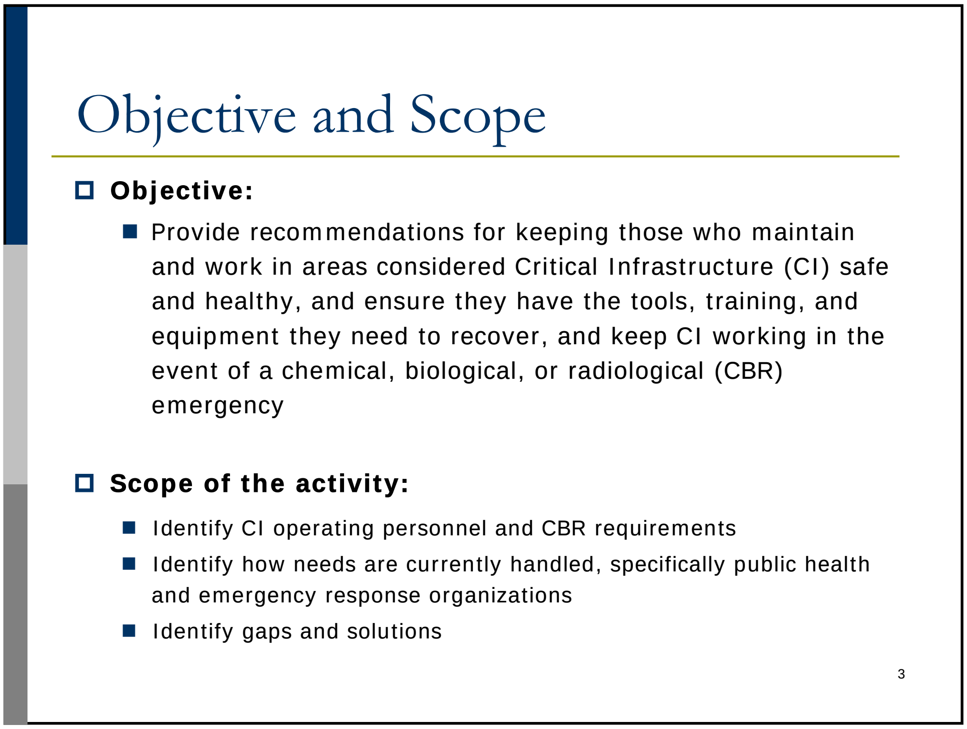
Chief Rebecca F. Denlinger
Fire Chief
Cobb County, GA Fire and Rescue

Bruce Rohde
Chairman and CEO Emeritus
ConAgra Foods, Inc.



Overview

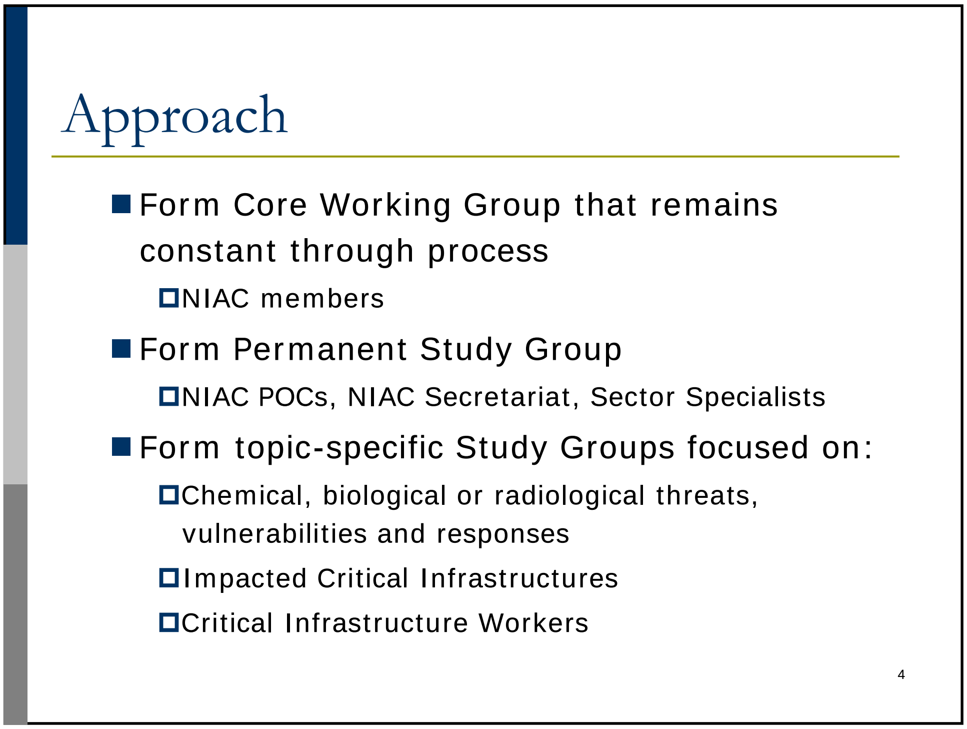
- □Objective/Scope
- □Approach
- □Next Steps



Objective and Scope

- □ **Objective:**
  - Provide recommendations for keeping those who maintain and work in areas considered Critical Infrastructure (CI) safe and healthy, and ensure they have the tools, training, and equipment they need to recover, and keep CI working in the event of a chemical, biological, or radiological (CBR) emergency

- □ **Scope of the activity:**
  - Identify CI operating personnel and CBR requirements
  - Identify how needs are currently handled, specifically public health and emergency response organizations
  - Identify gaps and solutions



Approach

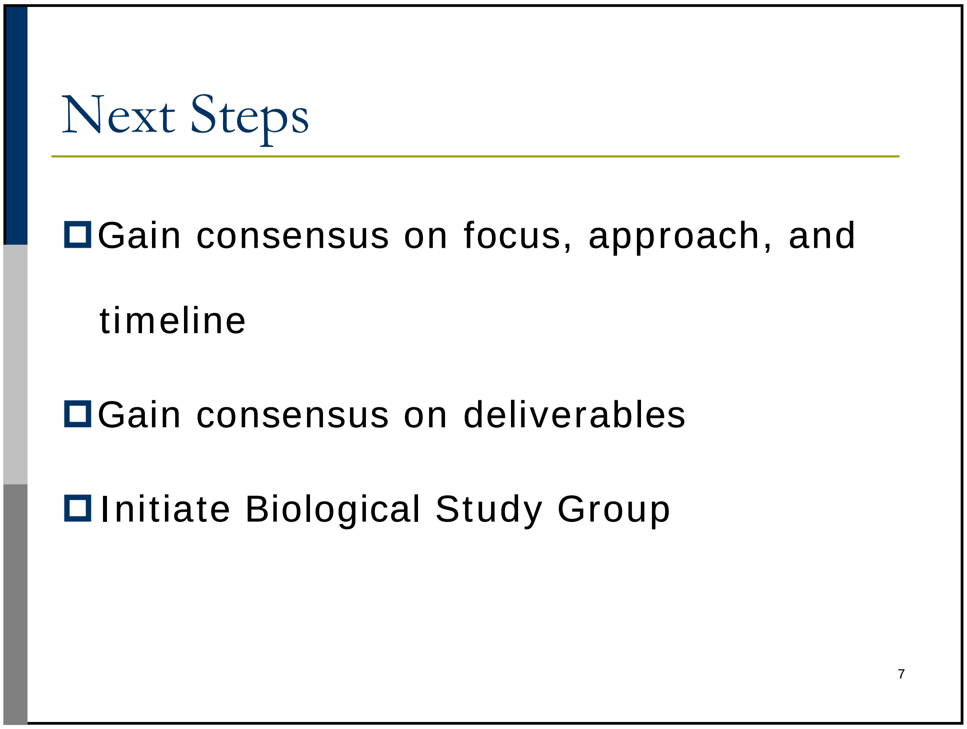
- Form Core Working Group that remains constant through process
  - □ NIAC members
- Form Permanent Study Group
  - □ NIAC POCs, NIAC Secretariat, Sector Specialists
- Form topic-specific Study Groups focused on:
  - □ Chemical, biological or radiological threats, vulnerabilities and responses
  - □ Impacted Critical Infrastructures
  - □ Critical Infrastructure Workers

Approach (cont.)

- Topic-specific Study Groups to meet for six months, consecutively
- Proposed Timeline:
  - Biological Study Group to form first – Jan. 2006
    - Collect data, analyze gaps - April 2006
    - Report on deliverables, provide initial draft report for review and comment - July 2006
  - Chemical Study Group – July 2006
    - Collect data, analyze gaps - Oct. 2006
    - Report on deliverables, provide initial draft report for review and comment – Dec. 2006

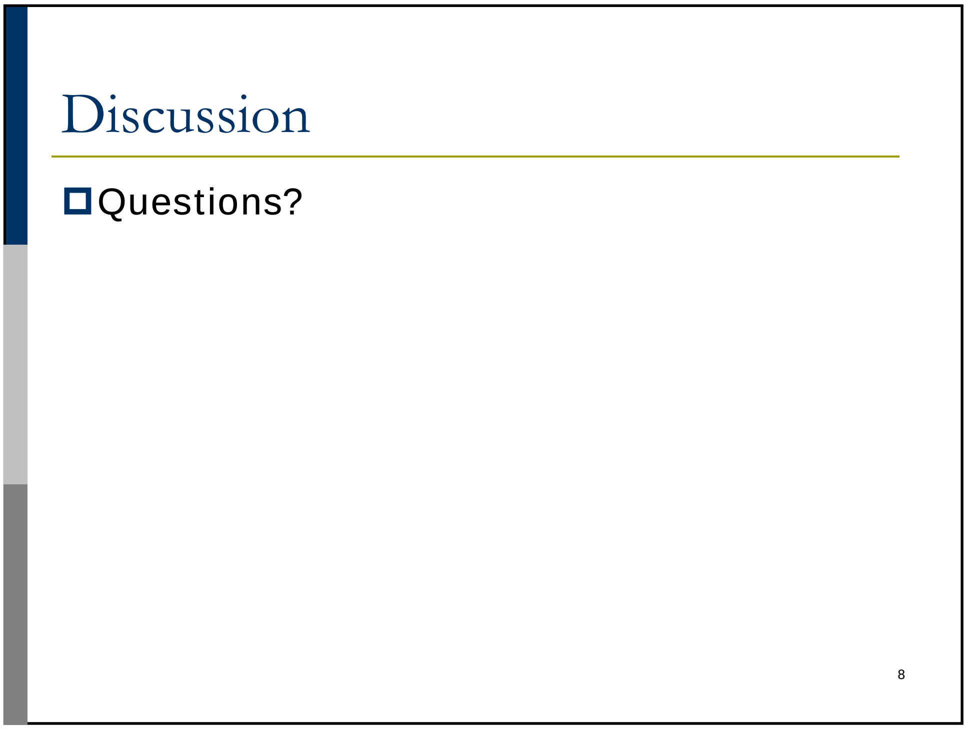
Approach (cont.)

- Radiological Study Group – Jan. 2007
  - Collect data, analyze gaps – April 2007
  - Report on deliverables, provide initial draft for review and comment – July 2007
- Final Report and Recommendations – July 2007



Next Steps

- □ Gain consensus on focus, approach, and timeline
- □ Gain consensus on deliverables
- □ Initiate Biological Study Group

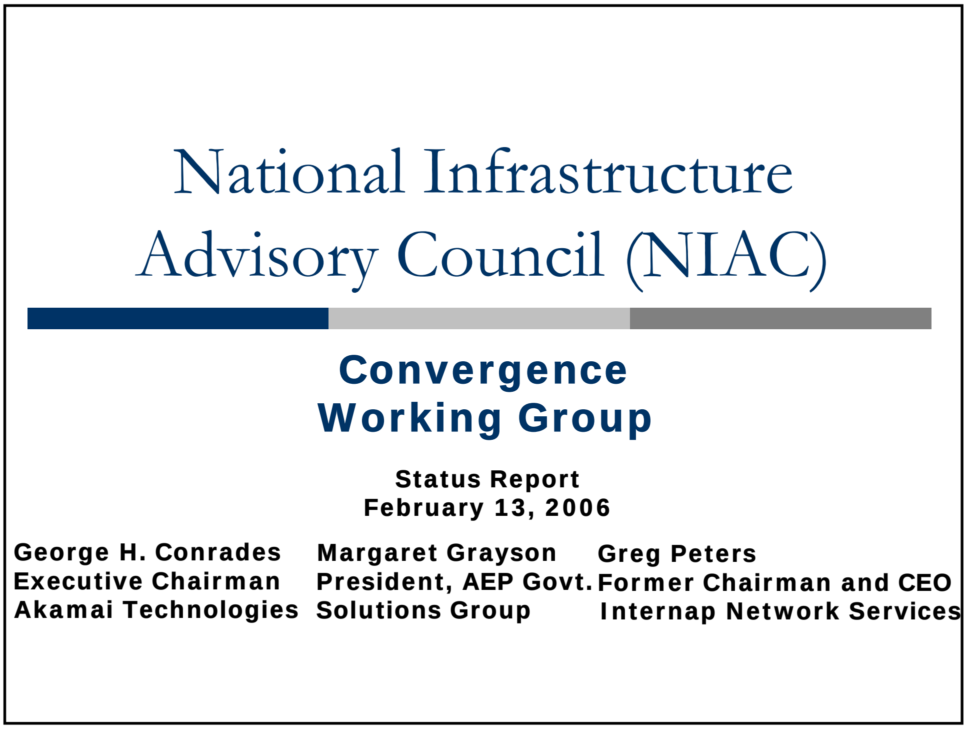


Discussion

- □ Questions?

ATTACHMENT D

Convergence of Physical and Cyber Technologies and Related Security Management Challenges



National Infrastructure Advisory Council (NIAC)

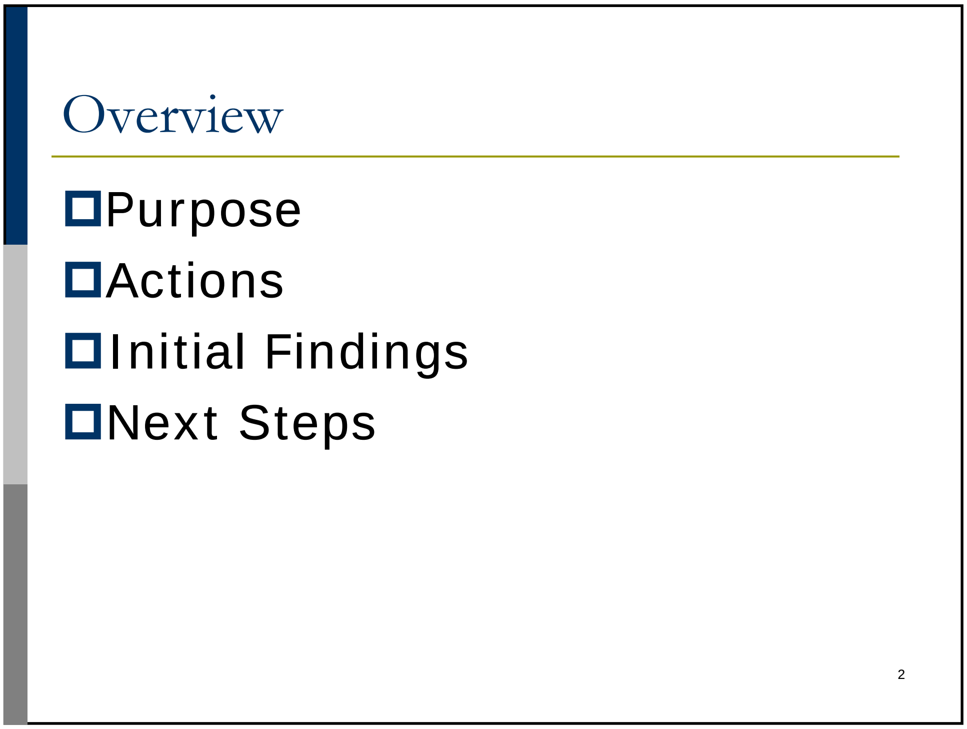
Convergence Working Group

Status Report
February 13, 2006

George H. Conrades
Executive Chairman
Akamai Technologies

Margaret Grayson
President, AEP Govt.
Solutions Group

Greg Peters
Former Chairman and CEO
Internap Network Services



Overview

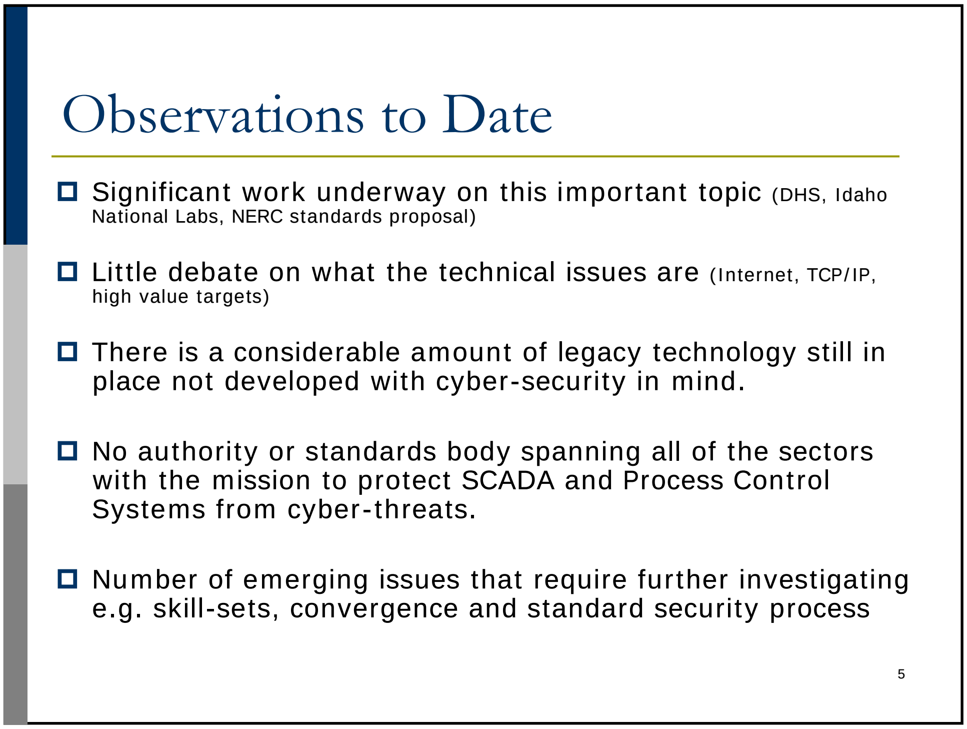
- □Purpose
- □Actions
- □Initial Findings
- □Next Steps

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.

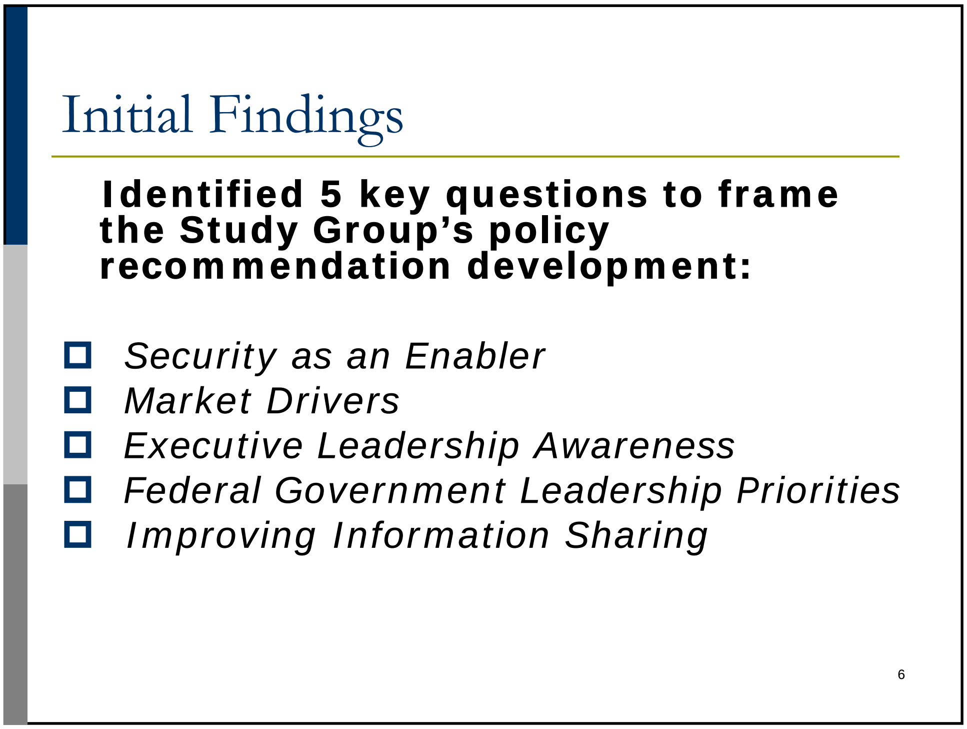
Actions

- Held weekly conference call discussions
- Developed Five Framework Questions to scope development of policy-level recommendations
- Identified and invited 5 key infrastructure sectors to participate in the study group
- Educating the study group with briefs from those already involved in developing Process Control and SCADA systems security solutions
- Held 1st workshop meeting to discuss further group development and future Study Group work



Observations to Date

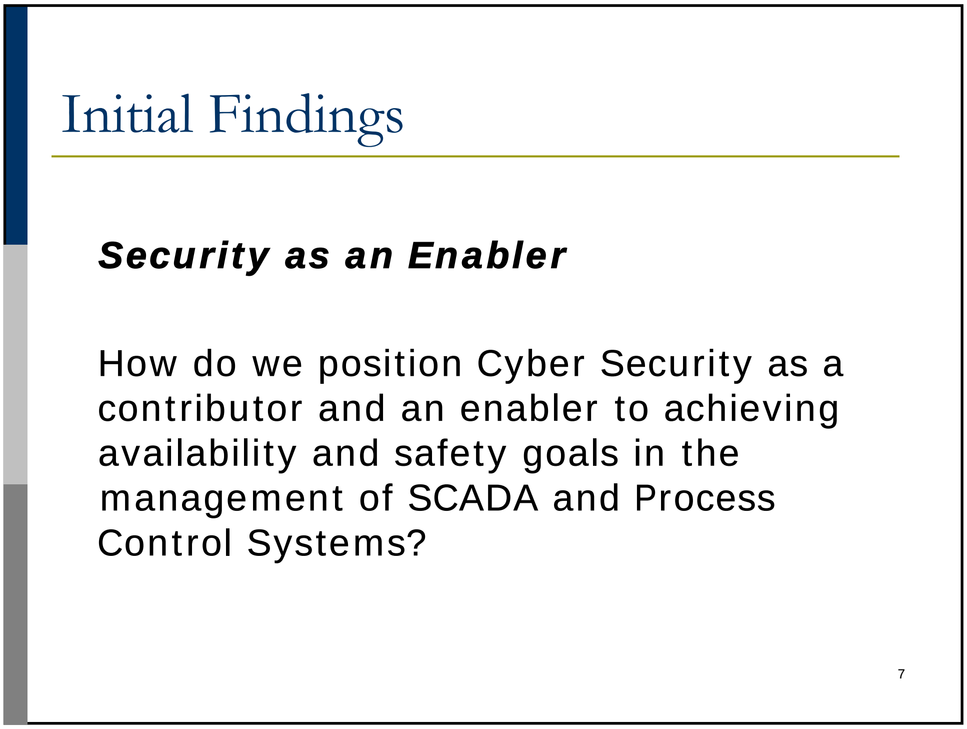
- Significant work underway on this important topic (DHS, Idaho National Labs, NERC standards proposal)
- Little debate on what the technical issues are (Internet, TCP/IP, high value targets)
- There is a considerable amount of legacy technology still in place not developed with cyber-security in mind.
- No authority or standards body spanning all of the sectors with the mission to protect SCADA and Process Control Systems from cyber-threats.
- Number of emerging issues that require further investigating e.g. skill-sets, convergence and standard security process



Initial Findings

Identified 5 key questions to frame the Study Group’s policy recommendation development:

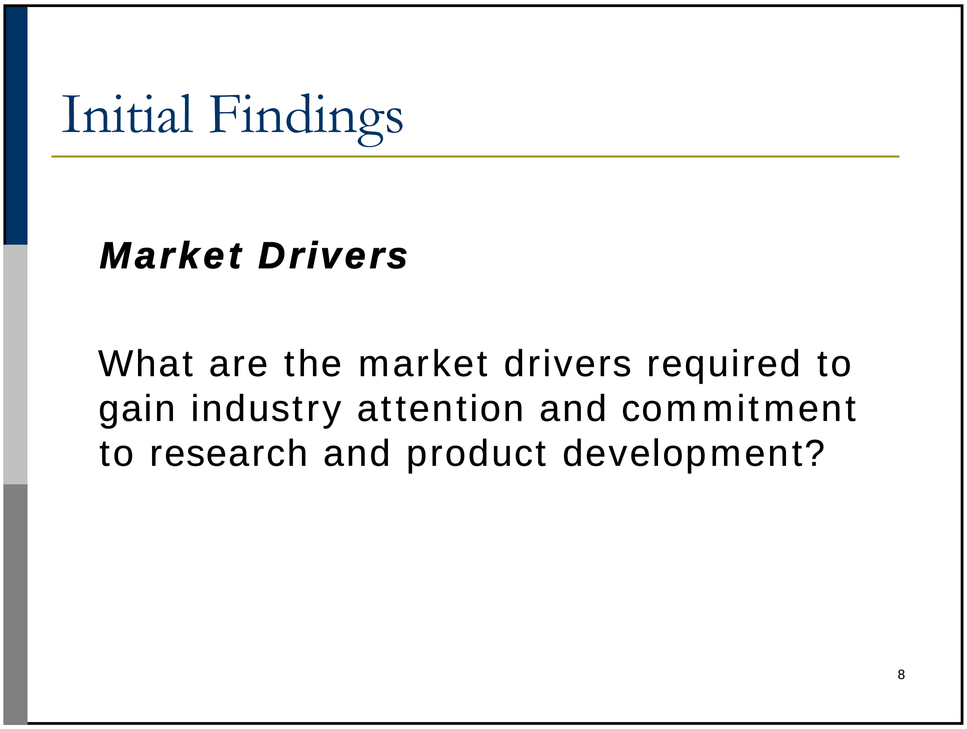
- *Security as an Enabler*
- *Market Drivers*
- *Executive Leadership Awareness*
- *Federal Government Leadership Priorities*
- *Improving Information Sharing*



Initial Findings

Security as an Enabler

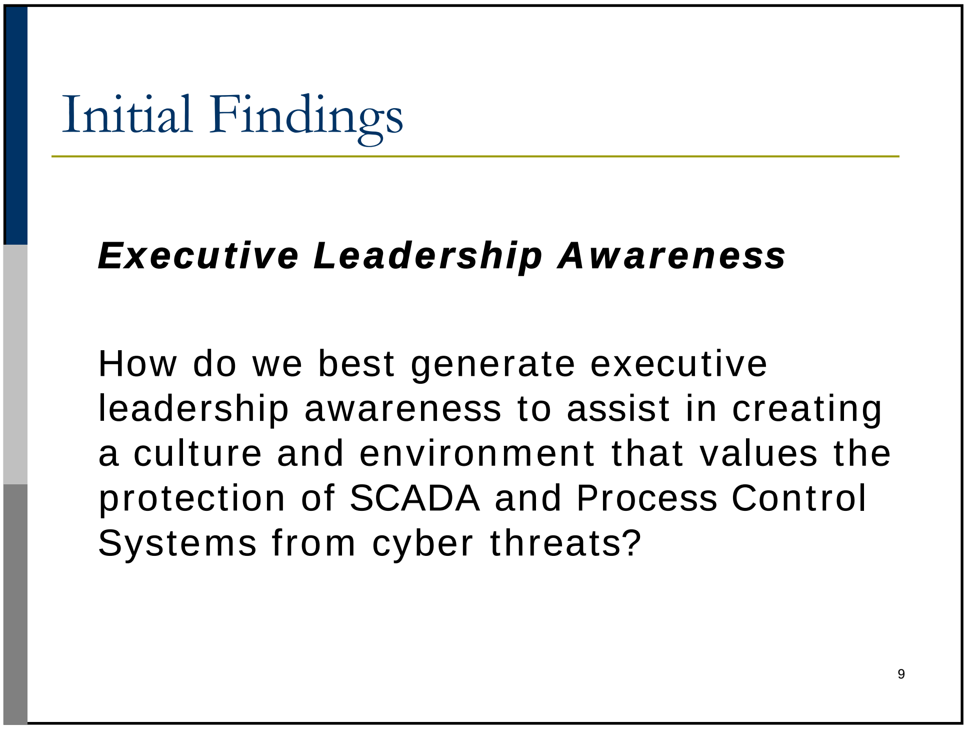
How do we position Cyber Security as a contributor and an enabler to achieving availability and safety goals in the management of SCADA and Process Control Systems?



Initial Findings

Market Drivers

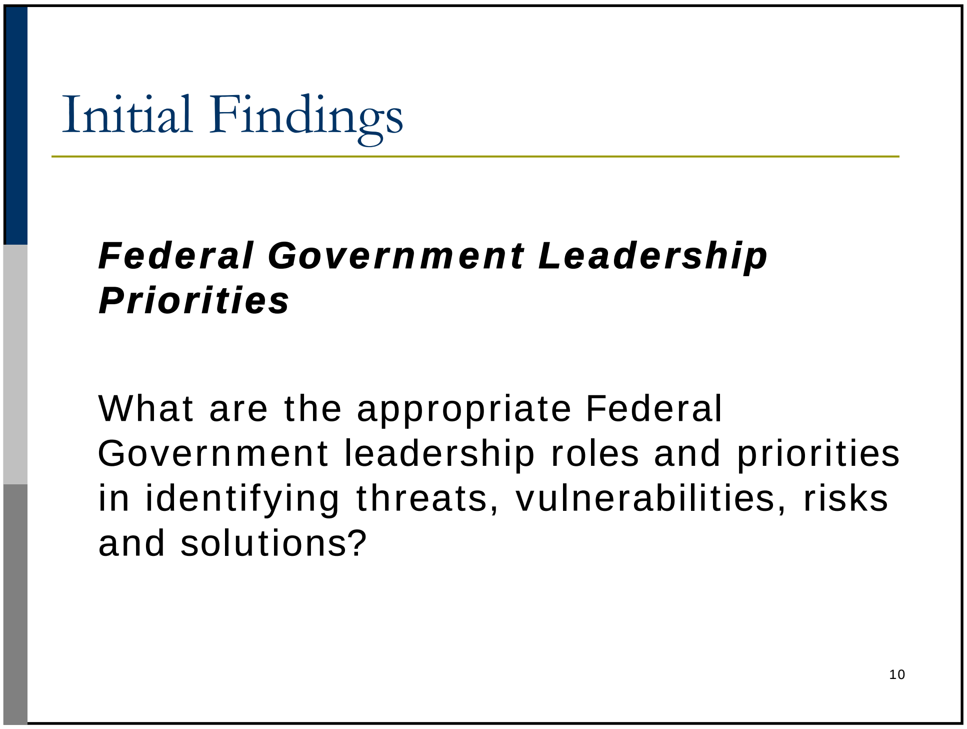
What are the market drivers required to gain industry attention and commitment to research and product development?



Initial Findings

Executive Leadership Awareness

How do we best generate executive leadership awareness to assist in creating a culture and environment that values the protection of SCADA and Process Control Systems from cyber threats?



Initial Findings

Federal Government Leadership Priorities

What are the appropriate Federal Government leadership roles and priorities in identifying threats, vulnerabilities, risks and solutions?

Initial Findings

Improving Information Sharing

What are the obstacles and recommendations for improving information sharing about Process Control Systems and SCADA threats, vulnerabilities, risks and solutions?

Next Steps

- □ Continue group development with key input from Industry and Government
- □ Begin development of straw man report
- □ Write and review final report

Discussion

- □ Questions?