NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING AGENDA

Tuesday, July 12, 2005
9:30 a.m. – 12:30 p.m. ET
National Press Club
Washington, DC

I.	**OPENING OF MEETING**	*Nancy J. Wong,* U.S. Department of Homeland Security (DHS) / Designated Federal Officer, NIAC
II.	**ROLL CALL OF MEMBERS**	*Nancy J. Wong*
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. *Michael Chertoff,* Secretary, Department of Homeland Security *Frances Fragos Townsend,* Assistant to the President for Homeland Security/Counter Terrorism (APHS/CT) *Robert B. Stephan,* Acting Under Secretary Information Analysis and Infrastructure Protection (IAIP) Assistant Secretary, Office of Infrastructure Protection, DHS *Cheryl Peace,* Director, Cyberspace Security, Homeland Security Council
IV.	**PRESENTATION OF NEW MEMBERS CHIEF DENLINGER, MR. ROHDE, MR. PETERS**	*Frances Fragos Townsend,* Assistant to the President for Homeland Security/Counter Terrorism (APHS/CT)
V.	**APPROVAL OF APRIL 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 & CEO, Cisco Systems, Inc.
B.	**RISK MANAGEMENT APPROACHES TO PROTECTION**	*Martha Marsh*, President & CEO, Stanford Hospital and Clinics, NIAC Member; *Thomas E. Noonan*, Chairman, President & CEO, Internet Security Systems, Inc., NIAC Member;
C.	**EDUCATION AND WORKFORCE PREPARATION**	*Alfred R. Berkeley III*, Chairman, Pipeline Trading, LLC., NIAC Member *Dr. Linwood Rose*, President, James Madison University, NIAC Member
D.	**SECTOR PARTNERSHIP MODEL IMPLEMENTATION**	*Martin G. McGuinn*, Chairman & CEO, Mellon Financial Corporation, NIAC Member *Marilyn Ware*, Chairman Emerita, American Water, NIAC Member
VII.	**NEW BUSINESS**	NIAC Chairman *Erle A. Nye*, *NIAC Members*
A.	**NATIONAL INFRASTRUCTURE PROTECTION PLAN (NIPP)**	*Robert B. Stephan*, Acting Under Secretary Information Analysis and Infrastructure Protection (IAIP) Assistant Secretary, Office of Infrastructure Protection, DHS
VIII.	**ADJOURNMENT**	NIAC Chairman *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Chairman Nye, Vice Chairman Chambers, Mr. Berkeley, Chief Denlinger, Lt. Gen. Edmonds, Ms. Grayson, Ms. Marsh, Mr. Noonan, Mr. Peters, Mr. Rohde, Dr. Rose, Mr. Thompson, and Ms. Ware.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Mr. Conrades, Mr. Hernandez, and Mr. McGuinn.

MEMBERS ABSENT:
Mr. Barrett, Mr. Davidson, Governor Ehrlich, Chief Gallegos, Commissioner Kelly, Mr. Martinez, and Mayor Santini-Padilla.

STAFF DESIGNEES PRESENT MONITORING PROCEEDINGS:
Mr. Allor (for Mr. Noonan), Mr. Blanchette (for Ms. Marsh), Mr. Holmes (for Mr. Davidson), Mr. Larson (for Ms. Ware), Ms. Deb Miller (for Ms. Grayson), Mr. Muston (for Chairman Nye), Mr. Rose (for Mr. Barrett), and Mr. Watson (for Vice Chairman Chambers).

STAFF DESIGNEES MONITORING PROCEEDINGS VIA CONFERENCE CALL:
Sgt. Mauro (for Commissioner Kelly) and Ms. Vismor (for Mr. McGuinn).

OTHER DIGNITARIES PRESENT:
U.S. Government: Michael Chertoff, Secretary of the Department of Homeland Security, Robert B. Stephan, Acting Under Secretary Information Analysis and Infrastructure Protection (IAIP) and Assistant Secretary, Office of Infrastructure Protection, DHS, Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security/Counter Terrorism (APHS/CT), Ms. Kirstjen Nielsen, Senior Director, Prevention, Preparedness and Response Directorate, Homeland Security Council, Mr. R. James Caverly, Director, Infrastructure Coordination Division (ICD) of the Department of Homeland Security, and Ms. Nancy J. Wong, Director, Infrastructure Programs Office and Designated Federal Officer (DFO) for the NIAC.

I. OPENING OF MEETING

Ms. Nancy Wong introduced herself as the Designated Federal Officer (DFO) for the National Infrastructure Advisory Council (NIAC) and the Infrastructure Protection Directorate of the Department of Homeland Security (DHS). She welcomed DHS Secretary Michael Chertoff, Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism, Robert B. Stephan, Acting Under Secretary for Information Analysis and Infrastructure Protection (IAIP), NIAC Chairman Erle A. Nye, NIAC Vice Chairman John T. Chambers, and all the members of the Council present or on teleconference. She also welcomed the members' staffs and other Federal Government representatives. She extended a welcome on behalf of the Department to the members of the press and public attending. Ms. Wong reminded the members present and on the teleconference line that the meeting was open to the public and, accordingly, to exercise care when

discussing potentially sensitive information. Pursuant to her authority as Designated Federal Officer, she called to order the twelfth meeting of the National Infrastructure Advisory Council and the second meeting of the year 2005. Ms. Wong 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.

Michael Chertoff, Secretary, Department of Homeland Security

Frances Fragos Townsend, Assistant to the President for Homeland Security/Counter Terrorism (APHS/CT)

Robert B. Stephan, Acting Under Secretary Information Analysis and Infrastructure Protection (IAIP)
Assistant Secretary, Office of Infrastructure Protection, DHS

Cheryl Peace, Director, Cyberspace Security, Homeland Security Council

Chairman Nye thanked Ms. Wong and everyone in attendance. He added he was very proud of the Council's work, but the July 7th, 2005 London subway attacks make it clear the NIAC must intensify its efforts. In respect to the casualties inflicted by the terror attacks in the United Kingdom, Chairman Nye asked the meeting attendees to observe a moment of silence in memory and honor of those victims. He thanked all in attendance.

Chairman Nye said the Council's charter requires review every two years by both DHS and the White House in order for the NIAC to continue. He was pleased to inform the Council the charter had now been reviewed and included some minor amendments. One of the amendments to the charter grants the Council more leeway in addressing physical security issues, giving the matter somewhat greater parity with cyber security. This issue has been discussed at Council meetings before, and the Chairman thought most members would agree this is a beneficial change.

Chairman Nye said the Council is privileged to have a number of prominent government representatives attending the meeting, including DHS Secretary Michael Chertoff. He thanked the Secretary for attending the meeting and lauded him for the way he addressed the unfolding

developments in London. Chairman Nye also expressed his gratitude to the Secretary for his assistance in renewing the NIAC Charter.

Chairman Nye then introduced Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism. He said he appreciated Ms. Townsend's attendance and said she will formally introduce the NIAC's three newest members.

He also welcomed Robert B. Stephan, Acting Under Secretary for Information Analysis and Infrastructure Protection and Infrastructure Coordination Division Director R. James Caverly. He finished his introductions by welcoming back Ms. Cheryl Peace, Director of Cyberspace Security in the Homeland Security Council. He was disappointed to report Ms. Peace will be leaving her current position at the end of September to take a brief leave before assuming other responsibilities. The Council had enjoyed its association with Ms. Peace and valued her counsel and guidance.

Chairman Nye also noted the return of the Council's DFO, Ms. Wong. As most in attendance know, she was in a serious accident in San Francisco and has undergone a number of medical treatments in order to return to Washington for this meeting. He welcomed her back and thanked her for being with the Council. The Chairman then asked Vice Chairman John Chambers if he had any remarks.

Vice Chairman Chambers thanked the Chairman and welcomed Ms. Wong's return. He also thanked Ms. Peace for the time she has put in and for what she has been able to do at the White House.

Vice Chairman Chambers said the NIAC has been able to make a difference because of the involvement of leadership from many different sectors. He challenged the members to remain involved and provide direct guidance to the Working Groups, in addition to relying on their staffs. He then turned the floor back to Chairman Nye.

Chairman Nye thanked the Vice Chairman for his comments.

He said Secretary Chertoff has accomplished many things over the past few months in his new role. The Council would be very pleased to hear any remarks he might have.

Secretary Chertoff thanked Chairman Nye for his kind introduction and thanked both him and Vice Chairman Chambers for their leadership. He also wanted to thank Ms. Wong for her remarkable resilience in returning to the job so quickly after her accident. He expressed his gratitude for Ms. Townsend's leadership at the White House. He said her work is very important and the events in London remind the nation that the threat of terror remains. At the same time, DHS always wants to remain focused on the big picture. A large component of this overarching theme is critical infrastructure and the recognition of how interdependent the US actually is. Much of America's ability to be resilient as a society and country in the face of terrorism requires careful planning and networking with federal, state, local, and private partners.

Secretary Chertoff also thanked each and every one of the members for taking the time to attend. He said he was well aware everyone had very busy schedules and were leaders in their own right. The fact the members are willing to devote their time to these issues is an important testament to the weight of the Council's task and the seriousness with which each member takes his or her responsibilities. The Secretary said he thought the combined expertise brought to bear by the Council has been a very important part of developing strategies to protect and recover from attacks on critical infrastructure.

Secretary Chertoff continued by saying he knew the Council had a number of reports forthcoming. He was particularly eager to hear the Working Group presentation on intelligence requirements. It is important to know how providing actionable intelligence can help DHS to better serve the private sector and those responsible for critical infrastructure. With respect to the Sector Partnership Model, the Secretary said there was the clear issue of how DHS can better implement the partnership concept. The Council will also address an area of personal interest for him, how the public sector might adopt the private sector's method for developing a risk management model. This is a particularly important issue because much of what DHS is doing in the National Infrastructure Protection Plan (NIPP) involves using the risk management model based on the private sector's models.

The Secretary said he knew from his experience preparing for the Y2K problem that the public and private sectors do have the capability to cooperate. By working together, the two sectors enhance DHS' ability to prepare itself and take steps to mitigate risk and damages. The fact this state of preparedness can be achieved is a constant reminder that DHS should follow the same model in respect to acts of terror.

Secretary Chertoff said he wanted to provide the Council with a preview of what is on the horizon. Shortly after the Secretary's appointment, he initiated a top-to-bottom departmental review. DHS reviewed the organization and redefined five key issues:

- What is DHS' principal mission?
- What results is it trying to reach?
- Where has DHS reached its goals?
- Where has DHS not reached its goals?
- What are the gaps and how can DHS correct those gaps?

This review formed an agenda for the next few months in a variety of policy areas. Secretary Chertoff stated he was going to further address these issues during a speech on July 13th. He thought a large part of the review was informed by DHS interactions with private sector groups like the NIAC. One thing the study indicated is DHS must have a great deal of expertise. The Council is an important part of this effort as it is one of DHS' partners and its perceptions are very important. The speech he intended to give on July 13th would be more of an agenda-setting effort and will indicate DHS' efforts to organizationally position itself to drive serious, highest priority policy issues. He thanked the Council for the opportunity to speak with them and turned the meeting back to Chairman Nye.

The Chairman thanked Secretary Chertoff and said the Council valued his comments and support. He stated the NIAC is always interested in hearing directly from DHS, citing the example of the Council's Sector Partnership Model Working Group as a direct response to a specific departmental request. He said the Council wants DHS to be responsive and direct with its feedback.

Chairman Nye remarked the Council is also celebrating the presence of three new members. These three individuals attended the April 12th meeting, but it is still appropriate for the Council to congratulate them on their appointments. He introduced Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security/Counter Terrorism (APHS/CT), to officially present each new member.

Chairman Nye said he would then introduce the three members. He began with Chief Rebecca F. Denlinger of the Cobb County, Georgia Fire and Emergency Services. She has had a tremendous career where she has rapidly advanced through the ranks. She has served twenty years with the Cobb County Fire and Emergency Services and was named Chief eight years ago. Recently, Chief Denlinger was named Georgia Fire Official of the Year. He asked the Council to join him in welcoming her.

The Chairman then introduced Mr. Gregory J. Peters, President and CEO of Internap Network Services Inc. He said Mr. Peters is in a very interesting, innovative business. He has served as President and CEO of Internap since 2002 and has a wealth of leadership experience in telecommunications and network areas that will be invaluable to the Council's work. He said the NIAC is very pleased to have Mr. Peters as a member.

Chairman Nye introduced the last new member, Mr. Bruce Rohde. Mr. Rohde has served as Chairman and CEO of ConAgra Foods for the last eight years. Mr. Rohde's leadership record in combination with ConAgra's size and reach makes him a valued addition to the Council. Additionally, Mr. Rohde comes from a sector the NIAC previously did not have representation in. Chairman Nye thanked Ms. Townsend for helping to greet the new members.

Chairman Nye stated that there are some vacancies on the Council due to retirements and other circumstances. Chairman Nye said he understood the White House is aware of these vacancies and there are candidates in consideration from sectors not currently represented.

IV. APPROVAL OF APRIL 12, 2005 MINUTES

NIAC Chairman, *Erle A. Nye*

Chairman Nye thanked the Council again and opened up the minutes from the April 12th meeting for discussion and review. He asked if there were any additions, deletions, or corrections that need to be made. He stated if there were not, he would entertain a motion to approve the minutes.

Mr. Berkeley motioned for a vote and it was seconded. The minutes were voted upon and unanimously approved.

Chairman Nye thanked the Council and said Ms. Townsend intended to make some comments.

Ms. Townsend thanked the Chairman and the Council and said it was a pleasure to be back at a meeting of the NIAC. She also said that Ms. Wong's return was extraordinary. Ms. Townsend also thanked Ms. Peace for all her work at the White House.

Ms. Townsend said the July 7th tragedy in London was a horrible reminder of the importance of infrastructure protection. It was a reminder of the vulnerabilities the nation faces and how enemies seek to exploit these vulnerabilities. She continues to be impressed with the Council's high quality reports and recommendations. Most recently, the NIAC provided the President with reports and recommendations on Hardening the Internet and the Prioritization of Cyber Vulnerabilities. The White House continues to work with DHS to review reports, and together they are laying out the next steps for actually implementing some of these recommendations.

Ms. Townsend said she looks forward to the NIAC playing an increasingly important role by lending expertise, studying DHS-critical topics such as national infrastructure protection planning, public/private engagement, partnership, and information sharing. She thanked the Council for taking on the challenge of validating the Sector Partnership Model and developing recommendations for its effective implementation.

Ms. Townsend said she wanted to address the Council's work on intelligence coordination, an effort that will help educate the ongoing intelligence reform effort. She has had the privilege of sharing the interagency cross-government review with Secretary of State Dr. Condoleezza Rice. This partnership led to the administration's position on the Intelligence Reform Act. Ms. Townsend said President Bush requested she undertake a review of the Silverman-Robb Commission Report related to Weapons of Mass Destruction (WMD). The President adopted some of the recommendations stemming from this review, further strengthening the intelligence community. This included the reorganizations of the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) to expand on reforms now underway. This is an opportune time for the NIAC to help the Federal Government examine the importance of its relationship with the private sector. In the wake of September 11th, the nation heard about the connection of these two spheres. She suspected this will be the case after the latest attacks in London. The government will work on the systems and information that is needed to bridge the gap between the public and private sectors.

Ms. Townsend stated the reason it is so important to effectively share information between private and public sectors is that one may unwittingly possess critical data to potentially prevent what recently occurred in London or in the United States on September 11th. This clearly is an important responsibility and is a burden the sectors jointly share. Members of this Council understand the private sector in ways the government cannot. This understanding can help identify those pieces of information that might make all the difference. It is crucial to remember this charge, how very important information itself is in preventing the next attack.

Ms. Townsend thanked the Council and said she was eager to hear its response and recommendations on intelligence coordination in particular. She continues to be impressed by the high quality of the Council members, especially looking at the credentials of the three newest members. The NIAC's experience and expertise is vital to the President and the country. She thanked them again for the time each member commits to this effort and said it is always a pleasure to work with them.

Chairman Nye thanked Ms. Townsend and said the Council is also very appreciative of her efforts and ardently follows all of her activities. The NIAC is very anxious to be responsive and seeks her regular, candid guidance and feedback.

He thanked her again and said there were four presentations for the Council. He thought they were making strong progress, but it is still important to review these reports in detail. He turned the floor to Vice Chairman Chambers and his status report from the Intelligence Coordination Working Group.

V. STATUS REPORT ON CURRENT INITIATIVES

A. INTELLIGENCE COORDINATION WORKING GROUP

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

Vice Chairman Chambers thanked Chairman Nye and the Council for the opportunity to present the Intelligence Coordination Working Group's status report He said chief executives around the world now stress the ability to move with speed and flexibility and the ability to adjust to change. At the heart of these capabilities lies the need to maintain data in accessible architectures. It is important this accessibility is on a need-to-know basis and the information is actionable. To survive, business leaders must have the capability to literally close their books in 24 hours, not in 30 or 60 days, as was the standard a decade ago. In addition to this capacity to rapidly close down, there must still be the capability to gain access. The intelligence community also feels this need. It needs to move away from its old mentality of information silos to an ability to share necessary information with the appropriate security measures.

Vice Chairman Chambers said the Working Group has gotten off to a solid start. He introduced Mr. Ken Watson, Study Group member and Senior Manager at Cisco Systems, Inc., to summarize this progress thus far and the interim steps that must be taken. Additionally, the Working Group also seeks more volunteers in order to meet its ambitious goal to conclude by the October NIAC meeting. Vice Chairman Chambers then turned the meeting over to Mr. Watson.

Mr. Watson thanked Vice Chairman Chambers and the Council. He said he would review the purpose of the Study Group, move on to its current status, and close by addressing the Study Group's next steps.

Mr. Watson said the Study Group started by temporarily grouping the law enforcement and intelligence communities together for the sake of combining domestic and foreign intelligence collection and analysis. The Study Group does understand law enforcement is a part of the

Emergency Services sector and will separate them later in the study. This collaboration is already achieving a great understanding of both communities' processes, capabilities, and needs across sectors and between the private sector and the intelligence community. The greatest benefit from this will be making policy recommendations aimed at institutionalizing optimum information sharing.

Mr. Watson stated the Study Group continually reminds itself of the two basic questions it started with:

- In what ways can the intelligence community help the private sector (owners and operators of critical infrastructures)?
- In what ways can the private sector help the intelligence community?

The Study Group is beginning to use one-page requirements documents from each sector and from many of the intelligence communities to get a high-level view of what their priorities are. The Study Group will focus on the NIPP to perform a more detailed analysis determining what changes are required. Private sector leaders and intelligence communities have provided these informal sets of requirements.

The Study Group asked DHS Information Analysis (IA) to review all existing information sharing mechanisms used for intelligence information, including law enforcement. This review will examine the possibility of using or modifying existing processes before recommending new measures. Mr. Watson asserted the first meeting between the private sector and intelligence agencies on June 13th was very successful. Besides reviewing the one-page requirements documents, he said he thought this was the first time multiple agencies have met with critical infrastructure owners and operators to address each other's needs. The Study Group plans to hold two additional meetings before the October NIAC meeting. The first meeting is scheduled in late July, and the second will be scheduled in September for intelligence community executives and NIAC members. The Study Group will look at preliminary recommendations intended for the Working Group's presentation to the NIAC in October. The Study Group recognizes its aim is to finish by October but also recognizes it is even more important to complete this task properly.

Addressing the next steps, Mr. Watson said the Study Group will continue collecting the intelligence requirements documents. Currently, there are two more sectors and several more intelligence agencies to gather information from. The group will dig deep to analyze and group the information into strategic or tactical categories to fit into the NIPP. By knowing both the private sector needs and their justifications, the intelligence community can better refine its analysis. Additionally, knowing what the private sector considers to be critical, the intelligence community can further hone its collection methods. Understanding the functions of each agency, each sector also clarifies its understanding of what information needs to be shared. DHS is looking into all information-sharing mechanisms to see if it is possible to modify what already exists before recommending something new.

The Study Group is also looking into the Protected Critical Infrastructure Information (PCII) program. It was not designed for intelligence processing; it was designed for the voluntary sharing of vulnerability information and therefore might not fit this process. This is just one of several mechanisms the Study Group is looking at. The Study Group is also examining the possible need of additional security clearances for some relevant private sector representatives. Rather than assume that this intelligence sharing will all be conducted within classified controls, the Study Group is endeavoring to recommend that it be done in the unclassified realm as much as possible; however, there may be the eventual requirement for security clearances.

Mr. Watson continued, saying the Study Group may recommend some form of virtual sharing through networks. He said the overall objective is to change or balance a need-to-know mindset with a need-to-share mindset. The Study Group is continuing to work on the requirements until it gets a broad sampling from all sectors and agencies. Once there is a broad sampling, the Study Group will map the requirements to the NIPP. After the Study Group receives the sharing mechanism information from DHS, it can then develop direct recommendations. At this point, Mr. Watson returned the floor to Vice Chairman Chambers to go over the next steps.

Vice Chairman Chambers thanked Mr. Watson and the rest of the Study Group for their hard work. He said he thought the entire Council understands how important this information actually is and what a difference it can make. He stated the Working Group is off to a strong start and he has been pleased by the group's openness.

He added the Working Group would likely ask a few more members to participate as the group seeks members from different backgrounds. By September, the Vice Chairman said that he would like to have a larger, more broad-based Working Group analyze the findings. By that time, the Working Group will have draft recommendations. If the Working Group is comfortable with the presentation's format, they will then bring it before the Council at the October meeting. He asked if anyone else from the Working Group wanted to make any further comments.

Mr. Alfred Berkeley, III said he wanted to make a few points. He thanked the Vice Chairman for his presentation. He said he wanted to focus on getting NIAC members from different sectors to participate in this particular Working Group. He said his expertise is in the Financial Services sector and Ret. Chief Gilbert Gallegos is a member of the Emergency Services sector.

The Working Group would benefit from sector-specific input, and the intelligence piece is being added by Mr. John MacGaffin, a veteran of the Intelligence Community, who is helping DHS staff with this project. Mr. MacGaffin was formerly a career intelligence officer in operations at the Central Intelligence Agency (CIA) and at the Federal Bureau of Investigation (FBI).

Mr. Berkeley thought this effort will evolve into a working-level group, then an executive level group where CEO-level input is needed. He added this was about the right time in the evolution of this particular work product to engage other members of the Council. He closed by saying he hoped the members would be responsive if Mr. MacGaffin contacted them.

Chairman Nye said he hoped the Council would be eager to volunteer.

Vice Chairman Chambers asked if there were any more questions from the Council before he closed.

Chairman Nye said as he watched how DHS responded to the bombings in London, it really appeared there was a genuine outreach to the private sector as well as the local and regional transportation authorities. He said he was impressed with the breadth and timing of the outreach. The mechanisms to do this kind of exchange either on a short-term emergency basis or an ongoing planning basis currently do not exist. But at least with what DHS has to work with, he was impressed with the effort and the commitment to it. He asked out of curiosity if Mr. Watson knew how DHS handled this.

Mr. Watson said he can discuss what was going on a little before the events in London. DHS has been very involved and interested in this project from the beginning. He had also been very impressed by the involvement across the board. At DHS, Mr. Bob Beecher, Ms. Gail Kaufman, and others have dug in and started examining existing processes. They have already begun the analysis phase to look at information sharing mechanisms. DHS has been very open and candid on what they can and cannot do. Everyone has been very eager to talk about what is important to them and about what has worked or not worked well with intelligence. There has been a great deal of cooperation on both sides.

Chairman Nye asked Assistant Secretary for Infrastructure Protection Bob Stephan if he had any comments. He said it seemed DHS really made an effort to open up to all involved parties, particularly within the transportation sector.

Assistant Secretary Stephan said over the past few years, DHS has developed an extensive stakeholder coordination and communication network that begins with the intelligence and law enforcement communities and includes international outreach. In the case of the July 7th bombings, DHS worked with its counterparts in the UK to develop an initial situational awareness to map against what the information the news networks had provided. Additionally, DHS tried to establish high-level initial outreach to governors, mayors, and key private critical infrastructure sector owners and operators. This was generally in the form of oral communication to expediently provide whatever pertinent information was available and describe the current situation. This was then followed by deliberations about adjusting the Homeland Security Advisory System. With evolving threat conditions, the Homeland Security Council (HSC) came to a conclusion it would lean on its partnership with industry before making the final decision. It would like to maximize outreach to state and local communities as well as the private sector to determine how changes would initially be received and what impact they might have.

Upon making a decision, DHS followed up with a formal announcement and a detailed information bulletin containing any additional threat-related information that the broad stakeholder community requires. DHS also incorporated very specific protective measures that had been worked beforehand with the Secretary of Transportation and the national mass transit community. The color-coded

system gets a lot of attention in the media, but that change is only the first step. Approximately 95% of the change is in the communications processes, protocols, and outreach underpinning the alert level. These pieces and the specific intelligence, information sharing, and protective measures take place in concert with the color change.

Mr. Watson said that Information Sharing and Analysis Centers (ISACs) have also assisted the private sector. Furthermore, communication between ISACs is also going very well. Immediately following the first news on the London incident, the Surface Transportation and Mass Transit ISAC was sharing information with the Information Technology ISAC and other ISACs. This served two purposes: keeping those needing information aware of what was happening and minimizing the extra traffic that could potentially be generated to find this information.

Vice Chairman Chambers said that when things work well, everyone seems to take the success for granted. He added DHS' communications effort was impressive.

Chairman Nye agreed, but said there still need to be more systems and planning. He had been watching the bulk of this effort from the outside and had been impressed with the breadth of involvement across the board. He asked if unrepresented sectors had been identified to help out the Working Group.

Mr. Watson said he did not want to single out sectors but the Working Group had enjoyed a solid beginning. He thought it was unprecedented because it was the first time all of these sectors sat down with members of the intelligence community. This kind of interaction will become more commonplace across all sectors as the Working Group progresses.

Chairman Nye thanked Vice Chairman Chambers and Mr. Watson for their presentation and asked if there were any questions for either the Working Group or the Study Group. There weren't any, so he thanked them again and introduced Ms. Martha Marsh, President and CEO of Stanford Hospital and Clinics, and Mr. Thomas Noonan, Chairman, President and CEO of Internet Security Systems, Inc., for their presentation on the Risk Management Approaches to Protection Working Group.

B. RISK MANAGEMENT APPROACHES TO PROTECTION

Martha Marsh, President & CEO, Stanford Hospital and Clinics, NIAC Member and *Thomas E. Noonan*, Chairman, President & CEO, Internet Security Systems, Inc., NIAC Member

Ms. Marsh thanked Chairman Nye for his introduction and the opportunity to provide the Council with a progress update on the Risk Management Approaches to Protection Working Group. She said the Working Group would address the Council on four key items:

- The Working Group's timeline and near-term objectives

- An overview of the Working Group's approach
- Outline of the Study Group's initial findings
- Initial thoughts on recommendations from the Study Group

Following these updates, the Working Group anticipates some discussion around logical next steps and will welcome questions and comments from the NIAC. At the July 13, 2004 NIAC meeting, the Council identified private sector risk management experiences and attributes that might strengthen existing government efforts to protect national critical infrastructure.

While the private and public sectors seek reduced exposure to undesirable consequences, the manner in which these entities assess risk management, manage risk, and deal with risk are slightly different. Accordingly, the Council convened a Working Group to explore the risk management philosophies, methodologies, and outcomes used by the private sector. The Working Group will look for ways to include these strategies in government's infrastructure protection planning programs. The Council relies upon formalized, scientific, and tested risk management methodologies to produce tangible and actionable items for the NIAC to recommend.

Ms. Marsh explained the Working Group can provide value to the NIAC in many different ways. First, the Working Group can analyze different risk management strategies from a very high level. The private sector relies upon three basic risk management drivers:

- Probability
- Impact
- Efficiency

These drivers are a core component of the job description for nearly all private sector leadership. As industry remains focused on cost efficiency and effectiveness, failure to manage these bounds can be critical and sometimes fatal if improperly balanced.

The public sector is undergoing a risk management transformation. For nearly half a century, the Federal Government focused its resources to defend the nation against risks inherent in a bilateral world. As was made obvious in London, this is a different world now. The Federal Government continues to make the risk management transition to a world presenting higher probability threats, perhaps on a scale not previously seen in the U.S.. Ms. Marsh said the transition brings into very specific relief the challenges the Federal Government will continue to face to reduce this distributive risk.

Ms. Marsh said she continues to believe effective risk management, efficient resource allocation, and a focus on all tenets of the private sector risk management model can become core methodologies of federal practice over time. Within the framework of the original timeline, the Working Group's efforts focused on providing recommendations for NIAC consideration at the October 11th, 2005 meeting. The Working Group will continue to work toward that objective and will ask the Council to consider the adoption of the recommendations.

She said the Working Group will present its initial findings and recommendations from its Study Group. These initial findings and recommendations are in the formative stage and will continue to be honed and polished before the October meeting. For a more detailed discussion of this approach, the Study Group's initial findings and recommendations will be presented by Mr. Scott Blanchette of Stanford Hospital and Clinics.

Mr. Blanchette thanked Ms. Marsh for her introduction and said he wanted to provide the NIAC with an overview of three items:

- The Study Group's approach
- An assessment of risk management across both the private and public sectors
- Initial thoughts on potential recommendations

Working toward the October NIAC meeting, the Study Group would like to be in a position to present more formalized recommendations and findings at that time.

The Study Group's mission is five-fold:

1) It engages resources to aggregate and assess existing public and private sector risk management methodologies, practices, and decision models.
2) It seeks to identify risk management commonalities and differences at both strategic and operational levels in both public and private sectors.
3) It seeks to identify private sector risk management maturity trends.
4) It will benchmark them against public sector risk management efforts.
5) The Study Group intends to make recommendations of value to the NIAC to strengthen federal risk management practices.

Mr. Blanchette said the Study Group, as it stands today, is broadly representative of the risk management profession. From the outset, the Study Group engaged NIAC resources across many sectors where effective risk management is a key component to corporate livelihood. Secondarily, it has benefited from the substantial contributions of a number of academics who either teach or research risk management. The third component to the Study Group are industry association contributions that either focus and promote effective risk management practices or include risk management as a core competency of the broader mission. Finally, the Study Group greatly benefited from its public sector counterparts who have provided the Study Group with maturity and prevalence of existing federal risk management programs.

As a brief indicator of where the Study Group is within its plans, it has been successful in assembling a sizable body of knowledge on risk management and continues to use this knowledge as the basis of its continued efforts. The Study Group has likewise circulated an index of this knowledge to ensure it is on the right track and has the right scope and scale of resources from which to work. To date, all feedback suggests the Study Group is appropriately positioned from a knowledge perspective.

Mr. Blanchette said he wanted to address components of risk management's daily mission in corporate America. However, the Study Group's work to date suggests some departments are doing some, much, or even all of this, while others are not. There is the fundamental assumption many of its findings are not pervasive, not core competencies, or not effectively translated into action across some components of the government. The nature of discussion really defines a more specific course of action.

As the Study Group was conducting its research, it noted a general discrepancy between risk acceptance and risk tolerance between the public and private sector. The causes for this are still under investigation amongst the Working Group, although the Study Group identified that there is a significant disparity between what levels of risk the public and private sectors are willing to tolerate.

Mr. Blanchette continued by saying that there are nine attributes of effective risk management. Not all of these attributes exist at all times and in all scenarios. However, they do tend to dominate the Study Group's backward looking analysis of risk management successes. At the same time, significant risk management failures tend to lack many of these attributes. In the first cut of the Study Group's findings there are nine elements of effective risk management:

- Existence of highly actuarialized data and a mature understanding of failure mechanisms and failure indicators.
- The effective use of actuarial data--the generation of actionable information between actuaries, indicators, and decision makers.
- Competition and consumer choice often encourages effective risk management. This component of the corporation risk management model is not as easily translated into recommendations for our federal counterparts.
- A mature understanding and appreciation of legal precedent often provides a foundation for the qualitative nature of risk management.
- The existence of risk management culture across an organization and the existence of a single, senior, accountable individual for risk management often improves outcomes.
- Aligned incentive factors often encourage risk management and quality metrics.
- The existence of mechanisms in the form of training, technologies, and procedures to reduce human error and improve outcomes.
- Insurance mechanisms allow the private sector to improve their risk tolerance.
- A substantiated business case that accompanies risk management investments, improves risk management resource allocations.

Chairman Nye said he had been under the impression that particularly large American businesses are increasingly holding themselves accountable to a single source for risk management review and action. He asked if this was a trend and if it also was taking place in government.

Mr. Blanchette said the Study Group had determined that the Chief Risk Officer position, or a single, senior accountable individual within corporations, was becoming increasingly prevalent. There are also academic studies verifying this. Many members of the Council could also confirm the recent growth in this area. That same single, senior, accountable individual has not been seen in

the federal framework. There are some agencies, DHS and the Department of Defense (DOD), which tend to be leading that particular respect. There are many agencies in which the focus of risk management at the senior-most, or the senior-most executive levels is not yet there.

Vice Chairman Chambers added it is not only important to have someone to hold accountable but also for him or her to have an operational understanding of risk management and the capacity to implement these measures. The mere act of appointing someone does not automatically accomplish these goals.

Mr. Blanchette moved on to discuss the attributes of ineffective risk management. He wanted to give the Council an opportunity to review these attributes. The risk management failures the Study Group looked at frequently possess many or all of these attributes of ineffective risk management.

Mr. Blanchette discussed the Study Group's potential recommendations to the broader Working Group and the NIAC for further consideration. He asserted the government continues to use its resources to address enhancing risk management. The development of a national agenda, an educational message, and a national communication platform is clearly something the government is ideally positioned to do. At the same time, the Study Group considered endorsing the public/private partnership model to be the most effective means to enlisting the broader resources of all sectors to meet the collective risk management challenge.

The Study Group also suggests the further development of a robust risk management infrastructure, mechanisms, and methodologies. A logical next step is developing risk management standards as a means to collect, analyze, and disseminate risk data. Additionally, the development and implementation of incentive mechanisms to maximize contributions from all stakeholders might also be beneficial. The Study Group found that many departments, agencies, or bureaus do not have a single, senior, accountable member of their organization responsible for risk management like a Chief Risk Officer. While this function may be one or multiple persons, depending on the magnitude of the risk management mission, the key component of this recommendation is the assurance that risk management data is being made available to senior government executives who need this information to make effective decisions.

Mr. Blanchette continued, saying the Study Group would suggest this senior accountable member of an organization dedicate time, attention, and resources to the development and implementation of an enterprise-wide risk management plan. In the early stages of this effort, an organization may look to external entities to provide a risk management methodology framework, but it should become a core competency of all government organizations to take on this strategic planning effort on their own accord. The study again suggests that ownership of the problem, in addition to accountability, significantly improves outcomes. Finally, a key tenet of corporate life is board oversight of an organization's risk management plans and the ability to execute those plans. This oversight function provides a number of valuable functions for an organization including the establishment of a risk management culture at the senior-most level and the implementation of metrics. Mr. Blanchette reasserted the Study Group will continue to solicit feedback from the broader NIAC with the intention of presenting it for consideration at the Council's October meeting.

Lt. Gen. Al Edmonds said when a corporation discusses risk management, it oftentimes discusses these risks from a financial perspective. It will build the infrastructure to protect its own individual investment. Beyond that, industry does need help from government. The government's piece of risk management is not motivated by profits and has a tendency to consider risk management as a kind of backup. For example, the Strategic Air Command (SAC) had a backdoor/frontdoor approach to ensure that there were always communication links with the missile field. During the time AT&T had a monopoly on the telephone business, government actually paid AT&T to install infrastructure risk management. They also did the same for GTE to ensure operations during a crisis. Going forward, the Council needs to define what industry needs from government and what government needs from industry to ensure collective risk management for U.S. infrastructure.

Mr. Blanchette thanked Lt. Gen. Edmonds. Mr. Blanchette said Lt. Gen Edmonds highlighted some key points including the components of the risk management formula. These components are different for the public and private sector and need further investigation around risk tolerance elements between the sectors. Clearly, financial risk tolerance is very different in private organizations versus public ones like the Assistant Secretary's. The Assistant Secretary is tasked with protecting lives. There are very different components in the risk management formula. Another difference is the risk management decision; DHS does not have an insurance mechanism for people's lives. He then turned the floor back to Ms. Marsh.

Ms. Marsh asked Mr. Noonan if he wanted to make any comments before she presented the Council with the Working Group's next steps.

Mr. Noonan thanked Ms. Marsh and said he wanted to recognize the hard work of both the Working Group and its Study Group, particularly from Mr. Blanchette and Mr. Peter Allor from Internet Security Systems, Inc. There is solid information out there based upon actuarial data and real life experiences that will help the Council work between both the private and public sector models and methodologies. This holds a lot of promise, not just for the government, but also for industry. He said he was very pleased with the progress and he thanked Ms. Marsh for her leadership.

Ms. Marsh thanked Mr. Noonan and said there were a number of next steps to bring the Working Group efforts to a close. The Study Group will meet over the coming weeks to gain consensus on the Study Group's initial findings and thoughts on potential recommendations and advance those to represent the position of the Working Group. Once there is a Working Group consensus, they will work with the Chairman and Vice Chairman to ensure the product meets the expectations of the NIAC and represents a deliverable of value to DHS and the White House. Finally, the Working Group will seek the input of the NIAC members to position its findings and recommendations for approval at the October meeting. She said the Working Group appreciates the significant efforts and contributions for all those who provide support. She asked the Council if there were any questions or concerns.

Vice Chairman Chambers added that progress to date had been very inclusive, thorough, methodical, and easy to follow. The challenge the NIAC faces with each of the Working Group efforts is to focus on doing three to five things well. It is important not to overreach.

Mr. Gregory Peters said many members have recently undertaken a large amount of work involving the Sarbanes-Oxley Act. There is the belief that much of the risk around internal threats from internal sources has been eliminated. Many threats come from internal avenues within a company. As the Study Group interfaces with other private sector entities, Mr. Peters asked if there was a feeling these private businesses have done the heavy lifting with Sarbanes-Oxley. He also asked if it was possible that due to Sarbanes-Oxley, many firms simply do not want to hear about more risk management initiatives. He inquired if it was possible Sarbanes-Oxley promoted a better awareness of various threats and, therefore, a greater awareness of risk mitigating mechanisms.

Mr. Blanchette said this is a timely question for the healthcare sector, especially as the sector was recently required to comply with HIPAA (Health Insurance Portability and Accountability Act of 1996). There generally has been a heightened sense of risk awareness and acceptance of the risk management culture for a number of reasons, whether it is HIPAA, Sarbanes-Oxley, or just corporate America's competitive nature. The key objective for the Study Group is to translate lessons learned from risk management experiences into some usable recommendations for the White House to improve federal initiatives.

Mr. Peters added that both from involvement with the Working Group as well as industry experience, many, if not most executives see Sarbanes-Oxley and its Section 404 as necessary, but insufficient, when it comes to overall risk management. While it has helped publicly-traded firms codify many of the processes and controls, the experience from this Working Group is viewed as necessary but not totally adequate from a broader risk management perspective. This is good for the Council, the American people, and for American business.

Chairman Nye admitted to chafing a bit under Section 404, but said he felt better for having worked to comply with it. He thanked the Council for the discussion and said they needed to move forward to the Status Report on the Education and Workforce Preparation Working Group from Mr. Berkeley and Dr. Linwood Rose.

C. EDUCATION AND WORKFORCE PREPARATION	*Alfred R. Berkeley III*, Chairman, Pipeline Trading, LLC., NIAC Member *Dr. Linwood Rose,* President, James Madison University, NIAC Member

Mr. Berkeley thanked Chairman Nye and said the Working Group had been a very active one. The Working Group had been meeting about once a week via telephone. The reason for the sheer number of meetings is the broad set of topics addressed by the Working Group. There are representatives from many different parts of the workforce and from the community of people who know about these issues. The Working Group and its Study Group have had presentations from

government, academia, and industry experts to pull together presentations and potential recommendations.

Mr. Berkeley said the Working Group hopes to have the recommendations for the October meeting. He began by discussing how the Working Group was originally organized. It was initially split up into two subgroups because the subject is so large. One group focuses on Research and the other centers on cyber education. The Working Group very rapidly picked up on Vice Chairman Chambers' suggestion of sticking with the broader issue of what an educated workforce means to long-term national security. There is a very significant goal of having specific short-term recommendations relating to research and cyber security. In addition, the Working Group wants longer-term educational issues affecting global competitiveness to have a place at the NIAC. He then turned the floor over to Mr. Rick Holmes to provide a briefing on the Study Group.

Mr. Holmes thanked Mr. Berkeley and said the Study Group evaluated the efficacy of the Cyber Corps program. Presidential Decision Directive 63 (PDD-63) set in motion a number of actions to address the shortfalls in the nation's critical infrastructure protection efforts. One of the problems illuminated very early on was cross-sector interdependencies and their over-reliance on information systems. This interdependency and over-reliance impacts the protection of these assets. A frequently discovered problem was the lack of a well-trained, competent, and capable information security workforce. Consequently, the actions to remedy this shortfall run through most of the plans and implementation strategies that followed PDD-63. As a result, the National Science Foundation (NSF) was tasked and funds were appropriated to establish the Federal Cyber Space Service Scholarship for Service initiative commonly known as Cyber Corps. The offer gives financial support for the last two years of undergraduate or graduate study for information security students at any of the National Security Agency (NSA) Centers of Academic Excellence in exchange for the student's commitment to serve in a civilian agency for two years. Since the program's inception, 20 Centers of Excellence have awarded scholarships to 628 students and produced 373 graduates. Funding for the program has averaged $15 million annually with a high of $30 million in 2003 and an expected decline to $10 million in 2006.

Chairman Nye asked if the Study Group had done any sort of appraisal on the quality of those Centers of Excellence. He asked if this quality was uniform across the board.

Mr. Holmes said the Study Group cannot directly assess the quality of these centers, but the implementation of these standards has been considerable among the 20 institutions. The Study Group cannot at this time say if any school was better or worse than the other.

Chairman Nye thanked Mr. Holmes.

Mr. Holmes said the central question being investigated is to what extent does the Cyber Corps program address infrastructure's information security needs. The answer is "no," inasmuch as students are not permitted to work in the appropriate organizations that control or manage critical infrastructure. Students find it very difficult to obtain internships and permanent employment within civilian federal agencies. Delays in obtaining security clearances reduce the effectiveness of

these graduates when entering the workforce. Allocation methods sub-optimize the number of graduates produced and there is a shortage of faculty with actual hands-on experience within the various schools.

He continued by saying the first question asks if the program addresses critical infrastructure's security needs. The Cyber Corps program produces students who are required to serve in federal agencies for two years. However, the agencies to which these students are assigned control very little of the critical infrastructure. 85 percent of critical infrastructure is owned and operated by the private sector. The very best students could directly impact only 15 percent of the critical infrastructure. The vast majority of these students are actually being hired by the National Security Agency (NSA); the impact on that subset is very small. Finally, the infrastructure maintained by the government is actually subcontracted to private firms. These students cannot satisfy their obligation by working for the contracting agency. So these graduates are not able to work in the areas that can directly affect the problem space.

Mr. Holmes said the Study Group also considered the actual program of study. The educational basis for the Cyber Corps program is based on the NSA Center of Academic Excellence, and those requirements are set forth in the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) standards 4011 through 4015. These standards are currently in the process of being revised. There is wide variation for how these centers deliver content. The standards are very inclusive and if a student were to master all the content described in these standards, they would be uncommonly well-versed in the subject matter. However, it requires considerable effort to actually analyze various academic programs, determine just how standards are being covered, and know what kind of experience there is. The Study Group concluded the experience varies considerably but cannot determine if there are any definitively good or bad at this time. Consequently, the students come out with varying degrees of qualification. In addition, the Study Group noticed considerable effort by Centers of Excellence to continually develop new curricula when existing curricula would probably be satisfactory if consistently implemented.

Mr. Holmes continued and said the next area considered was the shortage of information security for practitioners. Conventional wisdom suggests the path to security is actually doing the work. There are some 50 Centers of Excellence with three faculty members at each center; this puts the faculty requirement at 150. In trying to determine where this faculty was coming from, the Study Group discovered there was not enough faculty to meet this requirement.

There was another surprising, unintended consequence with the program--the reduction in people entering Ph.D. programs. The Cyber Corps program is pulling the best and brightest graduates and undergraduates. Upon completion, these students go into the workforce instead of entering Ph.D. programs, and programs are needed to build capacity for other ongoing initiatives.

The next item considered was the appropriate funding level for the Cyber Corps program. The funding level for the 2006 fiscal year is expected to be $10 million. The easy answer is to allocate more money to the program. However, there are a few complications that make that too simple of an answer. Another unintended consequence is the funding structure of the program. The program

pays all actual costs, tuition, books, room, board, and fees. It also includes a stipend for each student. This stipend is flat rate, but the variable costs across various universities differ by as much as 400%. If one could argue the programs of the more expensive schools were four times better than somewhere else, they might be able to justify the expense. However, the Study Group's assessment is the program is sub-optimizing the maximum number of graduates these schools produce with the current funding mechanism.

The next question the Study Group examined is how students are placed in agency positions and if they are being placed in appropriate positions. When the program was first offered, the Office of Personnel Management (OPM) was chartered to work with the NSF to find these students and ultimately place them. Since that time, the burden has been shifted primarily to principal investigators at each Center of Excellence. This has resulted in a very difficult time for students to find actual placement inside the agencies. To their credit, OPM and NSF have held a variety of job fairs to find these students jobs. In the winter of 2005, there was a job fair in Washington, DC connecting 350 cyber scholars with agency recruiters. One university sent ten students, with only one obtaining a position while each one of the ten met with over 40 different people. They stood in line for hours only to find out these agencies did not really have a position to offer. The Study Group believes one of the reasons for this is that these agencies simply do not have the billets or job authority to offer a position.

Mr. Holmes said the last area the Study Group looked at was clearances. An undetermined variable was who exactly handles these students' clearances. They do not actually obtain their clearances until after they have been employed. When they go to work, they must wait for months for clearances before they can become effective. One of the awkward consequences of the program is that the Centers for Excellence are actually asked to vet scholarship students for clearance, despite not being legally permitted to gather such necessary private information from the students.

The Study Group is still evaluating various recommendations. The first one is in the area of placement. Every scholarship student should graduate with a billet in hand so they can go to work in any agency and not have an impediment to their placement. Secondly, agencies need to reevaluate the way the funding mechanism is implemented. The NSF should find approaches to give it better leverage with its limited and declining budget. They cannot afford the cost skewing mechanisms currently in place. In terms of the security clearances, OPM should sponsor students before their graduations so when they arrive in the workforce they can immediately begin work. In terms of faculty experience, NSF can continue to invest in capacity-building with the intent of developing curriculum among the Centers of Excellence.

Mr. Holmes said the Study Group thinks that if a university is already certified by the NSA as a Center of Excellence, additional curriculum really would not be required and those funds could be reallocated to obtaining real-life experience. One recommendation would be to partner with the private sector to have the faculty work on sabbaticals or summer projects subsidized by NSF so they can tackle real-world critical infrastructure problems while simultaneously gaining experience. Probably the most important problem to be addressed is getting the students to work in critical infrastructure areas that might impact risk reduction. The Study Group's assessment is that the

students be allowed to work in the private sector and for contracting firms working on the federal agency problem space. This program should expand where it can remain focused on critical infrastructure protection. With that, Mr. Holmes turned the floor over to Dr. Rose.

Dr. Rose thanked Mr. Holmes and said he wanted to make an important point. This is the first time a Working Group has returned with observations of how things could actually work a little differently. He asserted that the Working Group does not think these problems are present in any one agency. Everyone the Working Group has talked to is doing the best they can and understand the problem. The Working Group is working in an extremely complex adaptive system and its recommendations will be tweaks to make the entire process flow more efficiently. This is important because it is not meant to be criticizing any participant in the cyber education business or any agency.

Dr. Rose commented to Mr. Berkeley that in many ways the main obstacle was people's resistance to change itself.

Mr. Berkeley responded that in some ways, this was the case. He reminded the Council that this impediment is not from the people who are doing the job.

Chairman Nye said he understood where the Working Group was coming from, but this was a tough litany of issues. He asked what it cost the government to produce a graduate.

Dr. Rose said the lower end of the range was $10,000 and the higher end was $40,000. On top of these costs, there also is the $8,000 stipend for undergraduate students.

Dr. Rose said he wanted to transition to the research portion of the presentation. Thus far, the Working Group has identified four topics related to research and cyber security. Secretary Chertoff and John Marburger, Director of the Office of Science and Technology Policy, have said the science and technology base of the nation play an important role in helping reduce critical infrastructure vulnerabilities, protect key assets, mitigate the effects of disruption and degradation, and recover from catastrophic events.

Homeland Security Presidential Directive-7 (HSPD-7) required the development of an annual plan for research and development in support of critical infrastructure protection. The first plan was published in April 2005. Dr. Rose recommended Council members review the document, especially those who had not yet had the chance to look at it. HSPD-7 addresses cyber security and calls for:

- New methods to be developed for automated protection of, response to, and recovery from attacks on critical infrastructure systems.
- Advancements in the security of basic internet communication protocols.
- Migration to a more secure internet infrastructure.
- Guide development of next generation security for IP-based process control systems and services.

- Development of software engineering methods, tools to support software assurance, and secure software development.

Unlike previous work that tended towards physical and cyber research and development, HSPD-7 correctly recognizes the interdependence of physical and cyber areas and regards them in an integrated fashion.

In the National Strategy to Secure Cyberspace, three strategic objectives were identified:

1. Prevent cyber attacks against America's critical infrastructure.
2. Reduce national vulnerability to cyber attacks.
3. Minimize damage and recovery time from cyber attacks that do occur.

Following some fairly extensive report review and consultation with a number of government officials, the Working Group can clearly see that it is on the right track. Further progress is required to coordinate cyber research priorities, plans, and funding into established progress report metrics across federal departments.

Dr. Rose said the Working Group's preliminary thoughts are not rooted in criticism, but rather in recognition. As post-9/11 strategic thinking matures and as fiscal infrastructure protection needs are better met, greater priority and funding needs to be allocated to cyber security research to address the challenges spelled out by the National Strategy to Secure Cyberspace. This is a difficult position to evaluate, articulate, and ultimately to reach, but that really is the fundamental issue. Dr. Rose stated that the priority is protecting physical assets and lives. In order to protect all of those assets, the nation needs to have the fundamental long-term research to address immediate needs and problems. At the October meeting, the Working Group will suggest the Council needs to figure out a way to properly fund and prioritize cyber security research.

Dr. Rose said the Working Group will continue cooperating with several key offices and interagency working groups over the course of the next several months. By the October meeting, the Working Group will sharpen its thoughts into recommendations. He said there are a number of groups working hard over the summer to develop a hard list of cyber security research priorities. They are analyzing funding gaps between priorities and actual commitments to those priorities. Dr. Rose said the Working Group wants to become familiar with this work to incorporate it into its proposed recommendations. He asked Mr. Berkeley if he had any further comments.

Mr. Berkeley said he wanted to invite Mr. Watson to discuss the cyber security certification programs.

Mr. Watson thanked Mr. Berkeley and said the cyber security certification area is applicable to improving the critical infrastructure workforce. There already has been a substantial amount of work done in this area. DOD commissioned the Institute of Defense Analyses (IDA) to map all the applicable industry and information security training certifications to DOD job classifications. DHS has also worked with DOD and National Institute of Standards and Technology (NIST) to see if this

could be applicable across federal agencies. This might also be a way to provide generalized job descriptions for critical infrastructure industries. The IDA study looked at 150 certifications provided by 50 vendors and mapped them across six different job categories. They recommended standardizing the job descriptions to have an entry-level, intermediate level, and advanced level in the technical and managerial fields, and DHS is considering adopting a similar recommendation for application across the federal government. This study was very methodical and resulted in matrices outlining each knowledge, skill, and ability in each of the certification programs needed by DOD employees.

Mr. Watson said DHS used those to map across their areas, too. Some of the challenges in this approach are that not all agencies use the same job classifications. Also, industries are pretty varied in how they classify people who work in information security. If there is going to be an effort to standardize position attributes, it will take an extraordinary and unprecedented level of cooperation. DHS is working toward recommending a training certification standards program administered by the private sector with government review. To implement such an industry-administered program for certification with government oversight would be challenging. The third challenge is in testing. Current testing methods don't adequately measure the knowledge, skills, and abilities that are present in each of these courses. The Study Group will propose some recommendations to try to develop modular or online testing to determine skill levels before and after taking specific courses. With this, Mr. Watson thanked the Council and returned the floor to Mr. Berkeley.

The Working Group is very eager to highlight the actions in the "No Child Left Behind" Act. The "No Child Left Behind" Act proposed what the Working Group thought a very good solution: evidence-based curriculum and pedagogy. The public has not embraced education as a national priority. There is a lot of talk, but it has not really been raised to the level of a national goal. It needs to be raised to that level and provided the attention it deserves. There must be a way to engage the public on this issue's sense of urgency, because the lead time on producing an educated person is long: 16, 20, or 24 years. As time goes by, the opportunity is lost.

Mr. Berkeley said there are "reading wars" and "math wars" going on within the educational profession that are counterproductive and are sapping resources away from the task of improving education. This opens the door for recommendations on how to resolve this situation.

Chairman Nye asked Mr. Berkeley what those terms entailed.

Mr. Berkeley said there are highly polarized and highly different ways of looking at how reading or mathematics is best taught. At one pole is the concept that every child will discover knowledge if they are put in the right environment. This thinking follows that there is a creative essence to every child and, if properly nurtured, they will all be Einsteins, Galileos, or Newtons. At the opposite end, there is a bootcamp mentality. This is highly repetitive drilling on areas like phonics or arithmetic basics. It could sort of be compared to a Marine Corps for first grade reading and math. These polar opposites exist both for reading and math and have been at the heart of a lot of wasted money and wasted time. There needs to be a NIAC recommendation calling for a resolution to this conflict. The fundamental basis of education should be research-based. A parent would not allow his or her

child to take a pill that had not been tested by the Federal Drug Administration (FDA)'s scientific process. Why would anyone let their children be subjected to twelve or more years of an unproven curriculum?

As for pedagogy, the way a curriculum is taught is the other key variable. One of the threads of the Working Group's research is to identify systems that actually work. At the October meeting, the Working Group should be able to share more thoughts on this. There is little evidence of what actually works in teaching math, science, and reading, particularly math and science. There is a role for federal research just as was done by the National Institutes of Health (NIH) for reading. There is far greater scientific evidence on how reading is taught effectively than there is in terms of math or science. There needs to be greater transparency on the effectiveness of different ways students are taught.

Mr. Berkeley said the final point he wanted to discuss is that there is a tradition in the U.S. for having a significant level of educational control. He thought this was a positive. There is a role for transparency in how the standards of one state map to the standards of another. There is tremendous variability at the state standards level, setting the state tests. It is important to watch for the insidious trap of where the curriculum and the pedagogy align--to teach solely to a test. He said that concluded his remarks and he wanted to open up for some questions from the Council.

Chairman Nye thanked Mr. Berkeley and Dr. Rose for their presentation. He said it was extremely well done. One would think the educational system had progressed further. He asked if there was anything further. He said the Council needs to move on to one of the more challenging undertakings, the Sector Partnership Model Working Group.

Chairman Nye called on Mr. Martin McGuinn, Chairman and CEO of Mellon Financial Corporation, and Ms. Marilyn Ware, Chairman Emerita of American Water, for their presentation.

D. SECTOR PARTNERSHIP MODEL IMPLEMENTATION	*Martin G. McGuinn*, Chairman and CEO, Mellon Financial Corporation, Working Group Chair, NIAC Member *Marilyn Ware*, Chairman Emerita, American Water, NIAC Member

Mr. McGuinn thanked Chairman Nye and said he would like to review the background of the project, the Working Group's approach, its findings to date, and its preliminary thoughts concerning recommendations.

The conceptual framework of the Sector Partnership Model is laid out in the Interim National Infrastructure Protection Plan (I-NIPP) and has its foundation in NIAC recommendations from previous studies. The majority of key resources that comprise the national critical infrastructure are owned or operated by the Private Sector. The Sector Partnership Model is intended to establish a framework for the unprecedented level of public-private cooperation necessary to secure these assets.

Mr. McGuinn said DHS requested the NIAC form a Working Group to develop recommendations for the structure, function, and implementation of the Model. To accomplish this, the NIAC established the Sector Partnership Model Working Group (SPMWG). This is an Integrated Study Group consisting of NIAC members and/or their Points of Contact, as well as the Chairs of the Sector Coordinating Councils (SCCs). The group is currently meeting on a weekly basis via conference calls. It is doing the bulk of the work regarding model validation and is generating recommendations that may result from the process. Additionally, each sector has formed a Sector Specific Study Group that is working in tandem with the Integrated Study Group to review its recommendations and provide input from the sector's perspective.

He continued by stating a true partnership is a collaboration of equals. The Sector Partnership Model is the tool or mechanism for government and private industry to work together toward addressing critical infrastructure protection issues. As an independent organizational entity, each partner has its own sovereignty. For the partnership to succeed there needs to be a very clear definition of roles and responsibilities. Each partner brings something to the table, and all partners create value because they are working together.

Mr. McGuinn said DHS must be attuned to the perspective of critical infrastructure owners and operators, in order to work with them on issues of Homeland Security. Once a collaborative structure is in place, DHS needs private sector cooperation during the various stages of planning and preparation for critical infrastructure protection. These stages include:

- Private industry and government working together to reach consensus on planning and goal setting for critical infrastructure protection.
- Once goals are set, cooperation is required to define and coordinate implementation procedures.
- Coordination is required between the parties as the agreed upon goals are actually executed.

The approach taken to validate the model and provide deliverables to DHS is to establish an Integrated Study Group that is responsible for reviewing the issues, vetting the views of the various parties involved, and then providing specific feedback to the Working Group. This approach will allow the Working Group to provide DHS with the requested core deliverables as well as any other recommendations that may result from the ensuing discussions.

The structure of the Working Group includes the Integrated Study Group. This Study Group consists of the various SCC Chairs as well as the participating NIAC members or points of contact. The SCCs are working in tandem to address issues or questions that the Integrated Study Group refers to them.

Mr. McGuinn said a formal invitation was sent to every member of the SCCs, including the leaders, requesting their participation in this effort. This chart depicts sector participation, currently at 87 percent. DHS is still working to obtain 100 percent participation; it should be noted that those sectors not yet participating are still in the early phases of SCC development.

He said the Working Group is seeing healthy representation from the NIAC, their respective points of contact, and very good participation from the SCC Chairs. He thanked the Study Group for their efforts, especially Mr. Don Donahue from the Financial Services Sector and Mr. Clay Detlefsen and Mr. Gary Weber from the Food and Agriculture Sector. Mr. McGuinn also thanked DHS and Mr. Jim Caverly for their support.

The core deliverables DHS asked the Study Group to provide are as follows:

- Review the conceptual structure and validate composition and representation of the councils in the model.
- Review and validate the elements of a charter and the rules of engagement.
- Review options concerning the operational framework.
- Define the principles of operations.

The Working Group will focus on the preliminary findings it has reached to date, though he cautioned these findings are still subject to change.

In terms of the first deliverable, the validation of the conceptual structure can be summarized as follows: The Study Group members accepted the overall organizational structure of the Sector Partnership Model, and agreed with the concept of three layers.

1) At the lowest level of the model, the formation of individual SCCs was agreed to by the majority of the team. However, it should be noted that other alternatives to the current SCCs were discussed:

    - Mr. Berkeley cited the example of the brokerage industry. As a result of the stock market collapse and the Depression, legislation was enacted in the 1930s that enabled everyone in the industry to participate on equal footing. The National Association of Securities Dealers (NASD) has emerged as a successful model.
    - Mr. Bill Muston cited the example of the electric power industry. As a result of the 1965 blackouts, the sector created North American Electric Reliability Council (NERC), a voluntary, self-regulated structure to set standards on reliability.

2) There was consensus around the second level, Cross Sector councils.

3) At the top level, the Leadership Council, the group asked to reserve final judgment until further details were clarified.

The current recommendations for this portion of the first core deliverable are to:

- Change the name from the NIPP Leadership Council to the Cross-Sector Leadership Council.

- Remove directional arrows. The group felt that the arrows were not in keeping with the concept of independent partners, but instead reflected a chain of command that is traditionally seen in corporate reporting relationships.
- The Working Group felt that communication should flow from the Sector Specific Agency to the SCC. If DHS, or other government agencies, have a request of the SCC, the request should go through the Sector Specific Agency via the chair of the Government Coordinating Councils (GCCs).

Another issue debated by the group was the validation of the SCCs' composition. Some participants feel very strongly that the DHS preference for an owner/operator chair is misplaced and may be dependent on the way the sector is organized. Some members of the group believed it may be more logical to have the sector chair come from a trade association, depending on the number of entities comprising a sector.

Mr. McGuinn said that as the Working Group addresses these issues it is cognizant of all perspectives. Obviously, the government has obligations to avoid conflicts of interest and provide equitable access to its resources. The Working Group is still working towards consensus on this issue.

One way to help reach that consensus was to review the roles and responsibilities of the SCCs' charters. Again, this is still a work in progress, but the methodology used for this deliverable is a self assessment by each of the sectors as to whether or not their specific sector meets the criteria specified by DHS. The Working Group also reviewed the template charter for the GCCs.

The Working Group has spent a considerable amount of time discussing the potential legal implications of the various organizational structures possible within the Sector Partnership Model. The group has identified four potential options, and legal counsel is providing the necessary information to help analyze the scenarios, which the Working Group is currently examining.

The original structure envisioned in Interim-NIPP created a Federal Advisory Committee, the Cross-Sector Leadership Council. The operational framework of a Federal Advisory Committee must adhere to the Federal Advisory Committee Act (FACA) and requires certain protocol to be followed. For example, meetings must be open to public observation, and all materials be made available for public inspection. Since the Sector Partnership Model focuses on potentially sensitive Homeland Security issues, the group needs to determine if the federal advisory committee structure is really the best option for the operational framework.

Other issues around the operational framework, that effect whether this structure is subject to FACA include:

- Determining whether the coordinating bodies are operational committees or advisory committees. If the focus of the committees is operational and not advisory, they may not be subject to FACA.

- FACA applies only to advisory committees that are established or utilized by the government. The SCCs are described as self-created entities of the private sector, and some of them have evolved out of pre-existing private sector entities. Therefore, they may not fall under the purview of the Act. This issue needs further research.
- Section 871 of the Homeland Security Act provides that the Secretary may establish, appoint members of, and use the services of, advisory committees, as they deem necessary. An advisory committee established under this section may be exempted by the Secretary from FACA. This exemption authority, however, has never been exercised.

Mr. McGuinn said as the group works through these issues, they may see that there are other options.

Details of the key processes and operating principles are contingent upon the operational framework that is chosen. After this framework is clearly defined, appropriate processes and procedures will be established.

The next steps for the group are to:

- Complete recommendations concerning the first two deliverables
- Determine an appropriate operational framework
- Determine key processes and operating principles based on this framework

He opened the presentation up to the Council for questions.

Vice Chairman Chambers said this is very good work and he asked Ms. Ware and Mr. McGuinn if the Council was pushing the Working Group too hard on the timeframe.

Mr. McGuinn thanked Vice Chairman Chambers and said the October deadline seems appropriate at the moment.

Ms. Ware concurred.

Chairman Nye said this is a tough issue and there are some imponderables in it. He said he was impressed with the progress the Working Group has made and the approach that has been taken.

Mr. McGuinn thanked the Council and said if there is the need for more resources, he would let the Council know. The real issue is understanding what the appropriate framework would be.

Chairman Nye said this effort will presumably lead to an ongoing relationship between government and various sectors, so it is important that it is done well. This was initiated at least in part from a request from the Department, so we need to move as best we can.

Mr. Berkeley said this is something that will take time to set up and be expected to work for a long time. He suggested the Council examine governance issues; there are many advantages of having the private sector handle certain issues themselves and not have direct regulation.

Ms. Ware said the Working Group appreciates the offer of more time and said this is the first step in transitioning to operational mode and then passing it along to the sectors.

Chairman Nye thanked the Working Groups for their reports and said the quality of the work is outstanding. Many people are very engaged and he encouraged everyone to get involved as the groups need broad representation across the board.

VI.	**REMARKS ON THE NATIONAL INFRASTRUCTURE PROTECTION PLAN (NIPP)**	*Robert B. Stephan,* Acting Under Secretary Information Analysis and Infrastructure Protection (IAIP), Assistant Secretary, Office of Infrastructure Protection, DHS

Assistant Secretary Stephan thanked Chairman Nye and said that when he began his job in April 2005, he performed an initial assessment of where the office stands and its accomplishments. He added that the road ahead is very challenging. The mission requires the efforts of everyone across the country. As evidenced by the incidents in London, the threat is still out there. No one knows exactly where it will next manifest itself, but it is clear that the U.S. remains high on the target list.

He said his most important contribution is to provide strategic leadership and find ways to bring those resources together. He applauded the Council's efforts and ambitious timeline as he has tried to get the base plan finished.

The NIPP is the strategic backbone for everything IAIP does. It has an overarching framework that is responsible for how resources flow, how the organizational framework is set up, and how information flows. Every activity IAIP pursues has to be tied to this plan.

This department was created two years ago with no lead time to prepare itself. IAIP needs to step back from that and continue to close the gaps and make sure all activities forward are tied to a strategic plan.

If you map it against HSPD-7 requirements, there are some shortfalls in the Interim -NIPP. The next version will come out at the end of this month and then there will be an at least a two-month timeframe for vetting by state and local governments and private industry. He asked the NIAC to review the next version to ensure that it is on the right track. He also requested that they make sure no one has been missed in terms of coordination and that there are no information gaps or items requiring more details.

Assistant Secretary Stephan said the cyber piece needs to be integrated into each sector and integrated cross-sector. It has to do with how the nation lives and breathes every day. The plan has to better address international cooperation efforts and finalize information sharing once and for all.

DHS must establish the baseline in this document with an open door to integrate new technologies, so it is not frozen in time.

The research and development component needs detailed examination. Sector-specific annexes will be added one by one; some are easier than others. DHS looks for NIAC comment on these as well.

By the end of July, the base plan in the final draft will be released. However, this is only one of many components that need to be incorporated into the final version. DHS must be sure it incorporates the entire nation so it isn't just the Secretary's or the President's plan.

This document will put core leadership principles and the guidance mechanism into writing. This cannot be done without the Council's help. He said he was very excited by these briefings as the NIAC is well on its way to greatly assisting DHS with this endeavor. He thanked the Council again and asked if there were any questions or comments.

Chairman Nye said the Council is very encouraged by the report and vowed the NIAC will participate as fully as it can.

Assistant Secretary Stephan said his personal goal is to gather input from as many Council members as possible.

Chairman Nye said the Council appreciates the opportunity to get involved.

Chairman Nye thanked Assistant Secretary Stephan for his presentation.

Chairman Nye said he thought the NIAC had made a significant amount of progress. The Council has completed seven reports that have been delivered to the White House. Generally, the feedback to the Council has been positive. He said he was encouraged by the fact some of these reports are actually catalyzing some change. He added the four reports underway also show promise and that he was pleased by the status updates. There were still some holes, but if the Council stays on schedule, there is the possibility that two or three of these will be finished this year.

The completion of these Working Groups also marks the time that the Council begins to look at new items. There are a multitude of projects the members could all come up with, this is a question of prioritization and determining what fits best with what DHS and the White House want.

He asked the Council to consider what it has already done and what it might need to do in the future. He wanted them to formulate these ideas in whatever fashion suited them. He asked the Council to voice these recommendations either to him or Vice Chairman Chambers, in writing or over the telephone. Mr. Muston or Mr. Watson can help pull these suggestions into a cohesive format. These recommendations will be vetted through various parts of the government, certainly through DHS, and ultimately, the White House will need to make decisions on how the NIAC should move forward. Chairman Nye stressed that time is of the essence and these ideas need to be gathered as quickly as possible. He asked the Council if they had any questions or comments about this.

Chief Denlinger asked if there was a timeline for this.

Chairman Nye responded that the Council was operating under the direction that these suggestions are returned as soon as possible.

Vice Chairman Chambers recommended that once the ideas are collected, they can be distributed to members. Once members have a list of these potential topics, they might then be able to rank them in terms of priority.

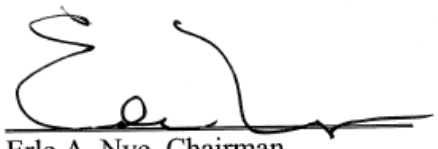
Chairman Nye agreed and thanked the Council for their hard work. He thanked everyone in attendance and said he looked forward to the October meeting.

VII. NEW BUSINESS *Chairman Erle A. Nye*, NIAC Members

There was no new business.

VIII. ADJOURNMENT *Chairman Erle A. Nye*

He reminded the NIAC that the October 11, 2005 is an in-person meeting. He encouraged all the members to look at how they can more effectively participate, especially those who have not been as active. With that, Chairman Nye closed the meeting and said the NIAC will stand adjourned.

By: 
Erle A. Nye, Chairman

Dated: 10/11/05

ATTACHMENT A
Intelligence Coordination Working Group

National Infrastructure Advisory Council (NIAC)

Intelligence Coordination Working Group

Status Report
July 12, 2005

John Chambers
President & CEO,
Cisco Systems, Inc.

Gilbert Gallegos
Retired Chief of Police
Albuquerque, NM

To Review……

- Purpose
- Working Group Focus
- Pending Actions

Purpose

Develop policy recommendations that ensure:

- Intelligence Community (IC) (including Law Enforcement) understands private sector's Critical Infrastructure Protection (CIP) domain expertise, intelligence requirements, and dissemination capabilities
- Private sector understands IC responsibilities, objectives and processes in CIP, especially regarding threat assessments
- Improvements in IC and private sector interaction for CIP are understood and considered by policymakers

NIAC IC Working Group Focus

- In what ways can the Intelligence Community (IC) help the private sector?
- In what ways can the private sector help the IC?

Working Group Approach

- Objective: Make recommendations to the President which will enhance government and private-sector contributions to CIP
- Analyze current information flows among appropriate IC and private sector elements and identify gaps
- Determine how to obtain and share information required (but not yet available) for CIP
- Focus efforts around the seven stages of the Infrastructure Risk Management Spectrum of Actions of the NIPP:
  - Deterrence, Prevention, Protection, Preparedness, Crisis Management and Response, Recovery, and Restoration

Update from April Quarterly

Completed/Ongoing Actions:

- Collecting private-sector requirements and analyzing them for IC information-sharing needs and issues
- Collecting and analyzing IC requirements for CIP information and expertise sharing
- Examining Law Enforcement/CIP information and incident reporting mechanisms (DHS/IA lead)
- Hosted unprecedented IC – private-sector CIP working session with over 30 senior executives, key representatives, and working-level staff to delve into issues and continue deeper dialog. Second working session planned for late July timeframe.

Next Steps

Refining Intelligence Information Sharing Needs

- What to share? (how will information be used – context)
- Who should share?
- How to share? (information as well as expertise)
- "Protected Critical Infrastructure Information (PCII)" program issues and gaps
- Additional requirements (clearances, architectures, networks)
- Shift CIP mindset to a "Need to Share" model

Next Steps (continued)

- Complete analysis of requirements collected from sectors and agencies
- Map information-sharing gaps to the seven steps in the National Infrastructure Protection Plan (NIPP)
- Develop draft recommendations for the President

Discussion

- Questions?

ATTACHMENT B

Risk Management Approaches to Protection Working Group

National Infrastructure Advisory Council (NIAC)

Risk Management Approaches to Protection Working Group

Status Report
July 12, 2005

Martha Marsh
President & CEO
Stanford Hospital & Clinics

Tom Noonan
Chairman, President & CEO
Internet Security Systems, Inc.

Agenda

- NIAC Question
- Timeline
- Study Group Approach
- Study Group Initial Findings
- Study Group Thoughts About Potential Recommendations
- Next Steps
- Discussion

NIAC Question

- "Can private sector experience with risk management and prioritization provide meaningful guidance to the President for risk management for national critical infrastructure planning and programs by the government?"
- NIAC cited private sector experience with risk management

  Experience includes managing IT and physical risk
  - Financial/commercial risk
  - Magnitude & duration of consequences
  - Customer & public impact by and acceptance of the consequences
  - Event experience, including:
    - Weather
    - Supply disruptions
    - Network disruptions
    - Commodity volatility

Timeline

- Initiate Working Group (October '04 NIAC)
  - Identify and recruit stakeholders
  - Define scope and timeline; resources and allocation
- Data Aggregation and Assessment (January '05 NIAC)
  - Aggregate raw risk management data
  - Assess state of risk management methods
- Deliverable Development (July '05 NIAC)
  - Report on deliverable development progress
  - Present initial study group thoughts on potential recommendations for review and comment
- Report Delivery (October '05 NIAC)
  - Present final deliverable

Study Group Approach

- Study Group initiated efforts to:
  - Aggregate and assess existing public and private sector risk management methodologies, practices, and decision models
  - Identify risk management commonalities and differences at both the strategic and operational levels
  - Identify trends in private sector risk management maturity; benchmark these trends against public sector risk management
  - Provide thoughts about potential recommendations of value on behalf of NIAC that will strengthen federal risk management practices

Study Group Approach (cont.)

- Stakeholder incorporation:
  - Addressed risk management across multiple industries represented by NIAC (finance, technology, electric, health, etc)
  - Identified and enlisted external stakeholders from
    - Academia (e.g. Stanford, Dartmouth, Maryland)
    - Industry associations (NACD, NERC, IIA)
    - Government agencies (DHS and DoD DCMA)
  - Conducted interviews, captured feedback, and included working papers in the work group document library
  - Addressed risk management at tactical, operational and strategic levels

Study Group Approach (cont.)

- Completed data collection and analysis:
  - Developed document library with contributions from multiple sectors, covering strategic and operational risk management
  - Included input from associations, academia, government and industry. Library covered private and public sectors
  - Validated input with risk management stakeholders (e.g. associations), industry representatives (e.g. NERC); substantial contributions from academia on more technical aspects of risk management (e.g., risk quantification)

Study Group Initial Findings

- Risk management is enhanced when predicated upon past performance
  - Significant actuarial, and historical, risk management data improves the ability of organizations to assess and manage risk
  - Some areas of risk lend themselves well to this type of analysis, others do not
    - Discussion on specific attributes of mature/immature (effective/ineffective) models

Study Group Initial Findings (cont.)

- Across all industries and sectors are examples of mature (effective) and immature (ineffective) risk management
- Contrasting risk acceptance levels between public and private sectors
- Mature (effective) risk management
  - Highly actuarialized data; mature understanding of failure mechanisms and failure indicators
  - Effective use of data; Actionable information; Proximity between actuaries, indicators, and decision-makers
  - Free market forces and consumer choice encourage effective risk management
  - Legal precedent provides foundation for qualitative nature of risk management
  - Risk management culture across organization; single, senior accountable individual
  - Aligned incentive factors
  - Mechanisms to reduce human error (e.g., training, technology, procedures, etc.)
  - Insurance mechanisms to improve risk tolerance
  - Substantiated business case for risk management investments

Study Group Thoughts on Initial Findings (cont.)

- Immature (ineffective) risk management
  - Lack of highly actuarialized data; immature understanding of failure mechanisms and failure indicators
  - Ineffective use of data, or data that is not translated into actionable intelligence; lack of proximity between data points and decision-makers
  - Few (or no) free market forces driving more advanced risk management
  - No legal precedent compelling risk management outcomes
  - Limited (or no) organizational risk management culture; lack of single, senior, accountable risk management leadership
  - Mis-aligned incentive factors
  - Lack of mechanisms to reduce human error
  - Lack of insurance mechanisms to improve risk tolerance
  - Unsubstantiated or poorly developed business case for risk management investments

Study Group Thoughts About Potential Recommendations

- Continue to engage the resources of the government to:
  - Educate both public and private sector on risk management
  - Outline an approach for national risk management
  - Develop and implement a risk management framework
- Continue to promote and expand the public-private sector risk management partnership
- Create a risk management infrastructure, mechanisms and methodologies
  - Develop mechanisms to identify, acquire, collect, and analyze risk management data; create actionable intelligence
  - Develop and implement risk management data warehouse
  - Identify and implement incentive mechanisms to maximize robustness of risk management data warehouse and maximize stakeholder contributions

Study Group Thoughts on Potential Recommendations (cont.)

- Establish risk management leadership function within departments, bureaus or agencies
  - Single, senior focal point for organizational risk management decision-making (similar to corporate Chief Risk Officer role)
- Analyze and prioritize threats to the critical infrastructure
  - Use mechanisms and infrastructure to develop mitigation strategy
  - Establish risk management priorities for the organization
  - Makes risk management recommendations to organizational lead
- Establish risk management oversight function
  - Establish a body responsible for organizational risk management oversight (functions similar to corporate Board of Directors)
  - Establish risk management metrics, including incentives and penalties
  - Establish, at the senior-most level, a risk management culture

Next Steps

- Advance "Study Group" initial findings and thoughts on potential recommendations to "Working Group"
- Working Group coordinate with NIAC leadership to gain consensus on findings and recommendations
- Working Group to align written deliverable to final findings and recommendations and circulate prior to October NIAC meeting
- Position Working Group recommendations to be adopted

Discussion

- Questions?

ATTACHMENT C

Workforce Preparation, Education and Research Working Group

National Infrastructure Advisory Council (NIAC)

Workforce Preparation, Education and Research Working Group

Status Report
July 12, 2005

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

Dr. Linwood Rose
President
James Madison University

NIAC Workforce Preparation, Education & Research Update

- The two subgroups (Workforce Preparation and Education and Research) are rejoining.
- The Study Groups are finalizing inputs so the Working Group can develop recommendations.

Efficacy of Cyber Corps (Scholarship for Service Program)

- Background
- Discussion Questions:
  - Does SFS programs address the information security needs of critical infrastructure?
  - Is the content of the SFS program of study appropriate?
  - Where are COAE's finding experienced faculty?
  - How is the SFS program dealing with the need to obtain security clearances for SFS graduates?
  - What is the appropriate funding level for SFS?
  - How are the SFS graduates being placed in government agency positions?

Efficacy of Cyber Corps (Scholarship for Service Program)

Enhancement Ideas under evaluation:

- Placement
- Security Clearances
- Faculty Experience
- Utilization of SFS graduates in Critical Infrastructure Protection

Research Update

- The Study Group continues to gather data addressing 4 key areas:
  - The need for a critical infrastructure protection and cyber security national research agenda.
  - The adequacy of the funding base for critical infrastructure protection and cyber security related research.
  - Research products "time-to-market" issues.
  - The adequacy of the related research national talent pool.

Research Study Group: Initial Thoughts

- There is a need for a formal coordinating structure for leadership and oversight of a national critical infrastructure security research agenda.
- A National Plan for critical infrastructure security research would provide focus.
- Even though substantial funds have been devoted to homeland security and critical infrastructure, funding for research is still insufficient.
- There is a need to cultivate and nurture the unique expertise represented by critical infrastructure and cyber-security academic researchers

Cyber Security Certification Programs

- DHS goals for Information Assurance (IA) certification program
  - Nationally recognized
  - Privately led
  - At appropriate levels to enhance public and private workforce needs
  - Working with DoD
- Institute of Defense Analyses mapping study
  - Matched commercial IA certification programs to DoD workforce levels and functions
  - 150 certifications by 50 vendors studied
  - Mapped to all applicable job skills and categories across DoD
  - Panel of 21 private, DoD, DHS, and NIST IA certification experts
  - Methodical approach, addressing both managerial and technical skills

Certification: Key Challenges

- Standardizing position attributes across Federal government requires extraordinary cooperation—private sector adds a layer of complexity.
- Issue of standards is complex for privately administered program with government stakeholders.
- Current testing methods may not adequately measure required KSAs (Knowledge, Skills, & Abilities).

K-12 Math and Science Competency

- The Problem we see: The country's long term security truly is tied to the quality of the workforce.
- The Administration has highlighted the problem in the "No Child Left Behind" act.
- The public has not embraced Education as a national priority; especially math and science education.
- We must find a way to engage the public with a sense of urgency.
- The "reading wars" and the "math wars" are counter productive and sapping resources away from the task of improving education.

K-12 Math and Science Competency

- Evidence-based curriculum and pedagogy are essential.
- Federally-funded research in curricula and teaching methods is needed where evidence is lacking.
- Greater transparency of the effectiveness of curricula and pedagogy is needed.
- Greater consistency between what is taught in teacher certification/training programs, in the classroom, and in textbooks is needed.
- There are vast differences in educational standards among the states.

NIAC Workforce Preparation, Education & Research Study Group Update

- Incentives to Attract Students into technical fields
  - A predictable, consistent funding program for cyber education should be effective in training.
  - Billets and clearances are a problem.
- International Competitiveness of US Education
  - This is closely related to the K-12 question.
  - Widespread availability of comparisons between US curricula and foreign curricula will shock most US parents.
  - US teaches "inch deep and a mile wide" versus "narrow and deep" approach in successful foreign competitors.
- Timeliness of Security Clearance Process
  - This issue is being worked by several other groups and we are using other's insights.
  - We will be using information gathered to offer practical recommendations.

NIAC Workforce Preparation, Education & Research Update

- Cyber Security Curriculum Development
  - College Education needs to be less vocational, or training oriented, and more core theory oriented. Provide educators with "summer internships" as a way to receive more "hands on" knowledge.
  - Pay is an issue as private industry pays better. Need to encourage those with the most knowledge to teach.
  - There is a need for more PH.Ds.

NIAC Workforce Preparation, Education & Research Update

- The Working Group continues to collect and analyze information
- On track to complete report and recommendations by October NIAC meeting

ATTACHMENT D

Sector Partnership Model Working Group

National Infrastructure Advisory Council (NIAC)

Sector Partnership Model Working Group

Status Report
July 12, 2005

Martin G. McGuinn
Chairman, President & CEO
Mellon Financial Corporation

Marilyn Ware
Chairman Emerita
American Water

Agenda

- NIAC Question
- Approach
- Findings
- Preliminary Thoughts on Recommendations
- Discussion

NIAC Question

- The Sector Partnership Model represents a new level of collaboration between the private sector and government. The conceptual framework of the Model is laid out in the Interim National Infrastructure Protection Plan (I-NIPP) and has its foundation in NIAC recommendations.
- DHS requested that the NIAC form a Working Group to develop advice and recommendations for the structure, function, and implementation of the Model. Specifically, DHS asked for help to review and validate the following:
  - Structure
  - Roles and Responsibilities
  - Potential Operational Frameworks and Related Issues
  - Processes

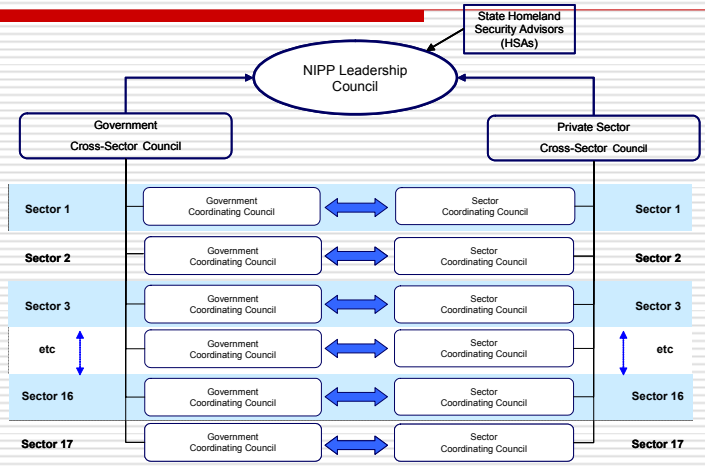
What is the Sector Partnership Model?

- A mechanism for government and private industry to work together to protect the critical infrastructure of the nation.
- The model should be a collaborative effort of equals:
  - Each partner has sovereignty on its own
  - Partners create value when working together

What should the Sector Partnership Model accomplish?

- The Sector Partnership Model should create a mechanism to facilitate collaboration between government and private sector owners and operators so that they can address homeland security issues. Specifically, the Partnership should enable:
  - Planning and goal setting
  - Coordinating how the goals will be executed
  - Establishing the actual execution of these goals

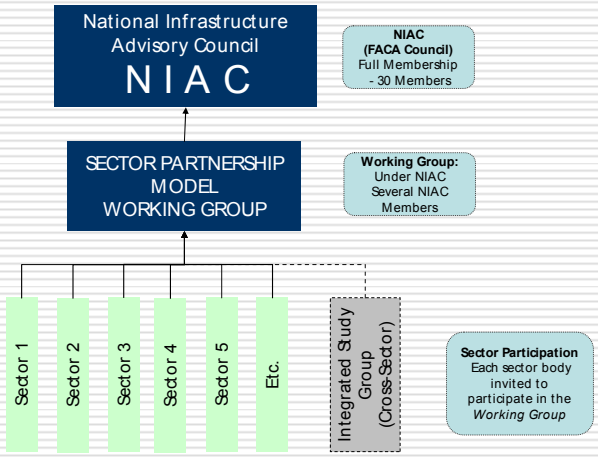
Proposed Framework



Approach

- Establish a NIAC Working Group and a related Integrated Study Group with representation from the NIAC, the Sector Coordinating Councils and DHS to review and assess the model and implementation options.
  - Sector-specific study groups are asked to provide feedback on the integrated group's recommendations
- Complete actions outlined in discussion of Core Deliverables

Structure of Working Group



Sector Participation as of July 12

Sectors:	Invitations	Responded	SCC Exist
1. Food & Agriculture	Yes	Yes	Yes
2. *Public Health*	Yes	Tentative	*In Progress*
3. Banking & Finance	Yes	Yes	Yes
4. Water	Yes	Yes	Yes
5. Energy – Electric	Yes	Yes	Yes
6. Energy – Oil and Gas	Yes	Yes	Yes
7. *IT*	Yes	Yes	*In Progress*
8. *Telecom*	Yes	Yes	*In Progress*
9. Chemical	Yes	Yes	Yes
10. *Transportation*	Yes	Yes	*In Progress*
11. Emergency Services	Yes	Yes	Yes
12. Postal/Shipping	Yes	Yes	Yes
13. Dams	Yes	Yes	*Yes*
14. *Commercial Facilities*	Yes	Tentative	*In Progress*
15. Nuclear	Yes	Yes	Yes

Integrated Study Group
NIAC Representation

- Marty McGuinn – Mellon Financial Services - Chair
  - POC - Susan Vismor
- Marilyn Ware – American Water – Co-Chair
  - POC - Bruce Larson
- Dick Davidson – Union Pacific
  - POC - Rick Holmes
- Al Berkeley – Pipeline Trading
- Becky Denlinger – Cobb County
  - POC – Stu Shannonhouse
- John Thompson – Symantec
  - POC – Rob Clyde
- John Chambers – Cisco
  - POC - Ken Watson
- Erle Nye – TXU
  - POC – Bill Muston
- Thomas Noonan - Internet Security Systems, Inc
  - POC - Peter Allor

Sectors Represented:
Banking & Finance
Water
Energy – Electric
IT
Transportation
Emergency Services

Integrated Study Group
Sector Coordinating Council Representation

Pat Laird	Electric	Exelon Corporation
Stuart Brindley	Electric	Independent Electricity System Operator
Beth Turner	Chemical	DuPont
Gary Forman	Oil and Gas	Columbia Gas
Rick Williams	Oil and Gas	Exxon Mobil
Gary Weber	Food/Ag	National Cattleman's Beef Assoc.
Clay Detlefsen	Food/Ag	International Dairy Foods Assoc.
Don Donahue	Financial	Depository Trust & Clearing Corp.
Lynn Stovall	Water	Greenville, SC Municipal District
Mike Wallace	Nuclear	Constellation Energy
Zane Hill	Postal/Shipping	US Postal Inspection Service
Dan Bart	Communications	Telecommunications Industry Assoc.
Guy Copeland	Information Tech	Computer Sciences Corporation
Garry Briese	Emerg. Services	International Assoc. of Fire Chiefs
Lyman Shaffer	Dams	Pacific Gas and Electric
Andrew Howell	Transportation	U.S. Chamber of Commerce

Integrated Study Group
DHS Participation

- R. James Caverly, Director of the Infrastructure Coordination Division (ICD)
- Nancy J. Wong, NIAC Designated Federal Officer
- Jenny Menna
- Brett Lambo
- Nancy Limauro
- Raghav Kotval
- Craig Bamberger

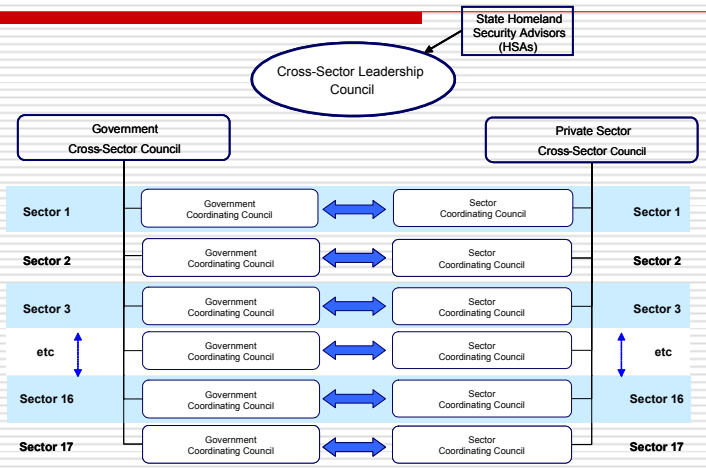
Core Deliverables

1. **Structure**
   - Review conceptual structure and identify & validate composition and representation
2. **Roles and Responsibilities**
   - Elements of a charter (for overall structure and sub-elements)
     - Purpose / Rules of engagement
3. **Potential Operational Frameworks**
   - Assess legal components of possible operational frameworks
   - Identify and review options: FACA/non FACA
   - Review authorities and core requirements to implement
4. **Processes**
   - Key processes to support true "partnership"
   - Principles of operations

Deliverable #1 –
Validate Conceptual Structure

- Validation of organization structure:
  - GCC-SCC Level – Consensus agreement.
  - "2nd" Level, Private and Public Cross-Sector Councils – General consensus is Yes.
  - "Top" Level, Leadership Council – Agreed on concept, but group reserves final judgment until details are fleshed out.
- Preliminary thoughts on recommended changes:
  - The name of the Leadership Council should be changed from the NIPP Leadership Council to the Cross-Sector Leadership Council, to more accurately reflect that the councils are dealing with more than just the NIPP.
  - Remove directional arrows; Arrows give connotation of subordination. SCCs are independent of government. Lines should merely depict information flow.
  - Communication will be from the Sector Specific Agency to the Sector Coordinating Council. If DHS, or other government agencies, have a request of the SCC, they will go through the SSA via the chair of the GCC.

Current Framework



Deliverable #1 –
Validate Composition and Representation

- Sector Coordinating Councils are self-organized bodies, independent of the government.
- SCCs have organized themselves in different ways with varying composition
  - Only owners/operators
  - All trade associations
  - Blend of owners/operators and trade associations – sometimes with trade associations as members and owner/operator as the chair

Deliverable #1 –
Validate Composition and Representation

- Regarding composition, issues arise when the SCCs interact with government.
- The government has obligations related to assuring inclusiveness, avoiding conflicts of interest, and providing equitable access to its resources and capabilities.
- Ongoing Discussion on this topic.
  - Working towards consensus, but still in progress

Deliverable #2 –
Roles and Responsibilities

- Integrated Study Group reviewed template for all GCC charters as well as the charters for all existing SCCs.
  - Sector representatives were asked to compare the functions of their councils to what DHS thought the functions should be
  - Draft results are being tallied and analyzed to detect anomalies or circumstances unique to specific sector

Deliverable #3 – Potential Operational Framework Options

- Detailed descriptions of different potential scenarios for operational frameworks and corresponding legal attributes and concerns have been prepared
- Descriptions will provide the study group a blueprint to facilitate analysis of the scenarios
  - Apply criteria to each scenario in order to determine which is most favorable

Deliverable #3 – Potential Operational Framework Options

- Scenario 1 – FACA structure
  - As originally envisioned in the I-NIPP
  - Private Cross-Sector Council and SCCs will be subcommittees of a parent Federal Advisory Committee (Cross-Sector Leadership Council)
- Scenario 2 – Operational Committees
  - Coordinating bodies are "operational" committees and not advisory
- Scenario 3 - Neither "Established" nor "Utilized"
  - An entity that is neither "established" nor "utilized" by the government is not subject to FACA.
- Scenario 4 – FACA Exemption
  - Granted by DHS Secretary
- Possibility for Others

Deliverable #4 – Key Processes and Operating Principles

- In process
- Ultimately dependent on what operational framework is chosen

Next Steps

- Finalize Deliverables #1 and #2
- Determine which operational framework is most viable from all standpoints (legal, implementation, etc.)
- Finalize Deliverables #3 and #4
- Final Recommendations at October 2005 Meeting