NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING AGENDA

Tuesday, October 11, 2005
1:30 – 4:30 p.m. ET
National Press Club Ballroom
Washington, DC

I.	**OPENING OF MEETING**	*Nancy J. Wong,* 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 *Kirstjen Nielsen,* Special Assistant to the President and Senior Director of Prevention, Preparedness and Response, Homeland Security Council *Neill Sciarrone,* Director, Infrastructure Protection Policy, Homeland Security Council
IV.	**APPROVAL OF JULY MINUTES**	NIAC Chairman *Erle A. Nye*
V.	**FINAL REPORTS AND DELIBERATIONS**	NIAC Chairman *Erle A. Nye* Presiding
	A. FINAL REPORT ON SECTOR PARTNERSHIP MODEL IMPLEMENTATION	*Martin G. McGuinn,* Chairman & CEO, Mellon Financial Corporation, NIAC Member *Marilyn Ware,* Chairman Emerita, American Water, NIAC Member
	B. DELIBERATION AND APPROVAL OF RECOMMENDATIONS OF FINAL REPORT	*NIAC Members*

C.	**FINAL REPORT ON 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
D.	***DELIBERATION AND APPROVAL OF RECOMMENDATIONS OF FINAL REPORT***	*NIAC Members*
VI.	**STATUS REPORTS ON CURRENT WORKING GROUP INITIATIVES**	NIAC Chairman *Erle A. Nye* Presiding
A.	**INTELLIGENCE COORDINATION**	NIAC Vice Chairman *John T. Chambers*, Chairman & CEO, Cisco Systems, Inc. and *Chief Gilbert Gallegos*, Chief of Police (ret.), Albuquerque, New Mexico Police Department, NIAC Member
B.	**WORKFORCE PREPARATION, EDUCATION AND RESEARCH**	*Alfred R. Berkeley III*, Chairman & CEO, Pipeline Trading, LLC., NIAC Member *Dr. Linwood Rose*, President, James Madison University, NIAC Member
VII.	**NEW BUSINESS**	NIAC Chairman *Erle A. Nye*, *NIAC Members*
A.	**REVIEW OF REVISED NIAC CHARTER/EXECUTIVE ORDER**	*Nancy J. Wong*
B.	**STATUS REPORT ON IMPLEMENTATION OF RECOMMENDATIONS**	*Nancy J. Wong*
C.	**DELIBERATION AND VOTING ON NEW INITIATIVES**	*NIAC Members*
D.	**HURRICANE RESPONSE**	*Robert B. Stephan*, Assistant Secretary, Office of Infrastructure Protection, DHS
VIII.	**ADJOURNMENT**	NIAC Chairman *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Chairman Nye, Mr. Barrett, Mr. Berkeley, Mr. Davidson, Chief Denlinger, Chief Gallegos, Ms. Grayson, Ms. Marsh, Mr. Peters, Mr. Rohde, and Dr. Rose.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Vice Chairman Chambers and Mr. Hernandez.

MEMBERS ABSENT:
Mr. Conrades, Lt. Gen. Edmonds, Governor Ehrlich, Commissioner Kelly, Mr. McGuinn, Mr. Noonan, Mayor Santini-Padilla, Mr. Thompson, and Ms. Ware.

STAFF DESIGNEES PRESENT MONITORING PROCEEDINGS:
Mr. Allor (for Mr. Noonan), Mr. Blanchette (for Ms. Marsh), Mr. Ellis (for Mr. Conrades), 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), Mr. Shannonhouse (for Chief Denlinger) Ms. Vismor (for Mr. McGuinn), and Mr. Watson (for Vice Chairman Chambers).

STAFF DESIGNEES MONITORING PROCEEDINGS VIA CONFERENCE CALL:
Sgt. Mauro (for Commissioner Kelly).

OTHER DIGNITARIES PRESENT:
U.S. Government: Michael Chertoff, Secretary of the Department of Homeland Security, Robert B. Stephan, Assistant Secretary, Office of Infrastructure Protection, DHS, Ms. Neill Sciarrone, Director, Infrastructure Protection Policy, Homeland Security Council, Mr. R. James Caverly, Director, Infrastructure Coordination Division (ICD) of the Department of Homeland Security, Ms. Nancy J. Wong, Director, Infrastructure Programs Office and Designated Federal Officer (DFO) for the NIAC, and Ms. Jenny Menna, Designated Federal Officer (DFO), NIAC.

I. OPENING OF MEETING

Ms. 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, Robert B. Stephan, Assistant Secretary for Infrastructure Protection, Ms. Neill Sciarrone, Director, Infrastructure Protection Policy, Homeland Security Council, NIAC Chairman Erle A. Nye, NIAC Vice Chairman John T. Chambers, and all the members of the Council present or on teleconference. She also welcomed the members' staffs and other federal government representatives. She extended a welcome on behalf of DHS to the members of the press and public attending. Ms. Wong reminded the members present and on the teleconference 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 thirteenth meeting of the National Infrastructure Advisory Council and the fourth 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

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

Chairman Nye thanked Ms. Wong and said the Council was pleased at her return. He thanked everyone in attendance, both in person and on the phone. He praised the Council for their accomplishments since the last meeting and said he was pleased to report on them.

The Chairman also praised Secretary Chertoff and stated that although there was a lot to learn from the recent hurricane disasters, the Secretary, DHS, and the entire government did an excellent job, especially when comparing the recent Gulf hurricanes to the October earthquake in Pakistan that killed 79,000 people. Chairman Nye said the experience in dealing with such a tragedy is necessary for preparing for similar events in the future. Hurricanes Katrina and Rita also showed how all Americans came together to help their fellow citizens in a time of great need. Chairman Nye then asked Vice Chairman John Chambers if he had any further comments.

Vice Chairman Chambers echoed Chairman Nye's praise of Secretary Chertoff and DHS during the hurricane catastrophe. He also lauded the Council's effectiveness; it presented two reports and intends to present one more during this meeting. Vice Chairman Chambers also asserted that setting an agenda for the coming year is necessary. He concluded his statements by thanking the industry sectors, the Partnership for Critical Infrastructure Security (PCIS), and NIAC members for their time and the high quality of their efforts.

Chairman Nye thanked the Vice Chairman for his comments. He then introduced the DHS Secretary Michael Chertoff.

Secretary Chertoff thanked the Chairman and Vice Chairman for their praise. The Secretary said the spate of recent natural catastrophes, Hurricanes Katrina and Rita, the earthquake in Pakistan, and the devastating Central American floods are all sober reminders of the challenges faced by the U.S.. Clearly, some of these challenges are natural, but it is important to remember many are man-made.

He stated the Council's work is crucial in making America safer. Specifically, the Sector Partnership Model and Intelligence Coordination Working Group are both topics that have become increasingly important in light of last quarter's events. Intelligence sharing is a vital subject and is

being discussed by the Council for reasons such as the July 7, 2005 London subway bombings and the recent mass transit scare in New York City. In situations like the London bombings, it is imperative that information flows accurately and freely between everyone with a role. At the same time, Hurricanes Katrina and Rita indicated how deeply bound the national response capability is to the private sector. This illuminates the importance of the Sector Partnership Model. One important facet of Infrastructure Protection is resilience. Part of what protects infrastructure is the ability to work around damage and to bounce back after it has been inflicted**.** It is obvious that studying this issue and developing fluid and robust relationships are critical to handle a wide range of threats. The ability to restore electricity to the gulf coast has been pivotal in enabling evacuees to return to their homes. The return of power to the region has a cascading effect across the country; the sooner the Gulf Coast regains electricity, the faster people can get back to their homes. When the displaced are able to return, this alleviates the concern for temporary shelter and relocation to other parts of the country.

Secretary Chertoff said there are other challenges ahead. As most are aware, there have been some reports about avian flu as a potential pandemic. Of course, while no one knows if and when a pandemic like this might occur, it is certainly sobering to contemplate the direct medical impact along with sustaining operation of critical infrastructure to actually deal with these challenges**.** The Secretary said these are some of the issues this kind of partnership will address.

Next, Secretary Chertoff discussed preparedness activities at DHS. At the July 12, 2005 NIAC meeting, he described DHS' Second Stage Review (2SR). One of the key findings was there was much work to be done in terms of preparedness, particularly relating to planning. He was pleased the 2006 appropriations bills budgeted funds allowing DHS to dedicate a robust, accountable component focused on preparedness.

The President gave DHS a charge in his Jackson Square address from New Orleans. He wanted DHS to meet with state and local governments to understand disaster planning and ensure every level of government is satisfied with its ability to confront the observed challenges. This process has already been initiated and DHS will soon be deeply engaged.

Secretary Chertoff wished to leave the NIAC with one thought. One great lesson from Hurricanes Katrina and Rita and the London subway bombings is that preparedness is not a top down issue. It is an issue demanding deep engagement at every level. Anyone trapped in a house with several days' supplies of water and food was in a far better position to wait and be rescued than someone lacking those amenities. Likewise, any business with a continuity plan, redundancy, resiliency, or the ability to continue work around damage was better prepared than those without it. As the preparedness issue is scrutinized, it is necessary to remind the public that preparedness must occur at every level. Those who remain unprepared are essentially placing a greater burden on others. For those who believe in the spirit of sacrifice and patriotism, personal responsibility for preparedness is an obligation; citizens owe this not only to themselves and their families, but also to their fellow citizens, as those who do not or cannot prepare themselves will call upon others to do it for them. The next time there is a big catastrophe, what each individual person does is absolutely critical to preparedness and protection.

Chairman Nye thanked Secretary Chertoff for speaking to the Council and said his presence indicates the importance he places on the NIAC and its work. He added the NIAC continues to receive good marks on its reports and has another report to present with the Secretary in attendance.

Chairman Nye said approximately 60 heads of trade associations and non profit associations were invited to visit with the NIAC in the morning before the business meeting to familiarize themselves with the Council's work and to solicit their support and input. Gaining the support and knowledge of trade and non profit associations will help the NIAC make better recommendations and generate better results. He was extremely pleased with the turnout and thanked some of the association members for also attending the NIAC's business meeting. A key to effectively integrating the nation's response to these critical issues is to reach out and engage industry organizations that have been handling their respective areas for quite some time.

IV. APPROVAL OF JULY 12, 2005 MINUTES — NIAC Chairman, *Erle A. Nye*

Chairman Nye thanked the Council again and opened up the minutes from the July 12, 2005 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.

V. FINAL REPORTS AND DELIBERATIONS — NIAC Chairman, Erle A. Nye, Presiding

A. FINAL REPORT ON SECTOR PARTNERSHIP MODEL IMPLEMENTATION — *Martin G. McGuinn,* Chairman & CEO, Mellon Financial Corporation, NIAC Member; *Marilyn Ware,* Chairman Emerita, American Water, NIAC Member

Chairman Nye stated that one of the more significant reports being presented concerns the Sector Partnership Model. The request for this undertaking came from DHS when it asked the NIAC to recommend a structure for addressing important security issues in all of the elements of the critical infrastructures that are recognized by the Council. The question being answered by this Working Group is how the government and different organizations integrate with one another to make the most effective response.

The NIAC is bringing forward recommendations balancing the interests of open government with necessary, appropriate security. Chairman Nye stated that neither co-chair was able to attend this meeting and were both very apologetic. They did send their two colleagues, Mr. Bruce Larson of

American Water and Ms. Susan Vismor of Mellon Financial Corporation. These two Study Group members represent a substantial body of knowledge on this topic.

In order to allow the Study Group members to present the final report in their place, Chairman Nye asked a NIAC member to formally sponsor the Sector Partnership Model report in the absence of the two co-chairs**.** He told the council that Chief Denlinger and Mr. Berkeley have both been very active members of the Working Group, and he asked Mr. Berkeley to sponsor the report.

Mr. Berkeley offered his sponsorship of the report and described the Sector Partnership Model Working Group as one of the Council's most interesting and important Working Groups due to its interactions between the public and private sectors. He then asked Study Group members, Susan Vismor and Bruce Larson, to present the report.

Mr. Larson thanked Mr. Berkeley and the Council for allowing Ms. Vismor and himself the opportunity to present the findings of the Sector Partnership Model Working Group. The initial findings come at a very opportune time; the U.S. has been witness to significant emergency response challenges recently faced in the Gulf Coast disasters. The sobering scope and scale of the impact from these storms brings exceptional clarity to the need for effective emergency management processes in order to respond adequately to the disasters of this magnitude.

Mr. Larson continued, saying that the goals set forth in the Interim National Infrastructure Protection Plan (I-NIPP) for protecting the national critical infrastructure span the full spectrum from Prevention and Preparedness to Response and Recovery. As stated in the plan, "protecting our Nation's critical infrastructure and key resources is vital to our national security, economic vitality and way of life." Although DHS is ultimately responsible for the success of the Critical Infrastructure Protection program, implementation will require integrated processes involving all of the key stakeholders, including federal, state, and local governments as well as the private sector. The private sector must be effectively integrated into the national disaster response efforts in order to respond effectively and recover quickly from events of the magnitude of Hurricanes Katrina and Rita. The public-private partnership is the critical path to protecting our infrastructure and preparing for catastrophic events.

The NIAC was asked to assess the validity of the partnership model for Critical Infrastructure Protection proposed in the I-NIPP. There was an opportunity for representatives from all Sector Coordination Councils to participate in an integrated Study Group, ensuring comprehensive representation across the sectors. Robust participation is critical. The overwhelming consensus in the Study Group helped to produce the recommendations submitted to the Council**.**

The goal of public-private partnerships is a complex challenge; key factors in developing successful partnerships must include complete equity amongst the stakeholders, independence for private sector organizations to self organize and retain separation from government, and flexibility in the partnership framework to allow for great diversity in scope and scale across the sectors. Partnerships formed with these factors at their core will be lasting and adaptable over time. An effective public-private partnership must:

- Implement a consistent structure, applicable to all sectors, clearly defining roles and responsibilities.
- Allow Sector Coordinating Councils to self organize and develop appropriate governance processes within their sector.
- Provide appropriate mechanisms for SCCs to provide advice to the Government on protecting critical infrastructure. Such interaction may trigger the Federal Advisory Committee Act and the SCCs should be exempted from the act.
- Provide appropriate protections for sensitive information to be shared between the stakeholders in the partnership. Effective collaboration between the stakeholders is imperative and the framework must enable timely and open communication.
- Permit the SCCs to be fully engaged in the development of the Sector Specific Plans and be able to provide direct input to the National Infrastructure Protection Plan (NIPP) and National Response Plan (NRP).
- Create a framework that is able traverse all sectors and levels of Government and with the private sector. Katrina and Rita show that disasters happen at the local level.

An effective partnership can only be achieved through long-term engagement and support of stakeholders; the success of this Working Group is evidence of this sentiment and shows again the resolution of the public and private partnerships of the sectors. Mr. Larson then said that he and Ms. Vismor would brief the NIAC on the findings and recommendations.

Ms. Vismor thanked Mr. Larson. She continued by stating that 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. As discussed previously at NIAC meetings, the majority of key resources that comprise national critical infrastructure are owned or operated by the private sector. The Sector Partnership Model is intended to establish a framework for an unprecedented level of public-private cooperation to secure these assets.

DHS requested the NIAC form a Working Group to develop advice and recommendations for the structure, function, and implementation of the Sector Partnership Model. To accomplish this, the NIAC established the Sector Partnership Model Working Group. This included an Integrated Study Group consisting of NIAC members and/or their points of contact, and the Chairs of the Sector Coordinating Councils. The Group has met on a weekly basis via conference calls since May, doing a large amount of work related to model validation and generating recommendations. Additionally, most sectors have formed sector-specific study groups that have worked in tandem with the Integrated Study Group to review its recommendations and provide input from the sector's perspective.

The Sector Partnership Model needs to be a collaborative effort of equals. Each partner, as an independent organizational entity, has a sovereignty of its own. 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 both partners create value because they are working together. The real value of the relationship is created from the groups working together.

The Core Deliverables that DHS asked the Working Group to provide are as follows:

1. Review the conceptual structure, and validate the composition and representation of the councils in the model
2. Review and validate the roles and responsibilities of coordinating bodies
3. Review options concerning how to implement the framework
4. Define the principles of operations and key processes

The Integrated Working Group reached a consensus agreement on accepting the conceptual structure of the model, with the following modifications:

- The group agreed Sector Coordinating Councils and the corresponding Government Coordinating Councils are the appropriate bodies to comprise the base level of the model.
- There was a consensus agreement that the Partnership for Critical Infrastructure Security (PCIS) should assume the role of the Private Cross-Sector Council. The PCIS has been in existence for over five years and is tasked with coordination of cross-sector initiatives in support of public and private efforts to promote assured and reliable provision of critical infrastructure services.
- Recommended that the top level of the organization, originally named the NIPP Leadership Council, be eliminated.
- Engagement of the State Homeland Security Advisors will be through the Government Cross-Sector Council.
- In general, communications flow will be between the Sector Specific Agencies and the Sector Coordinating Councils. If DHS, or any other government agencies have requests of the sector councils, they will be generally communicated through the Sector Specific Agencies.

Ms. Vismor continued, pointing out the slide illustrating the modified framework. It also shows a box for Under Secretary of Preparedness for information flow, not subordination.

The composition of the sector councils vary. Some councils consist of owners and operators or trade associations. Other councils include both owners and operators and trade associations. Some of these councils have also put in place governance processes that assure checks and balances to ensure representation of the entire sector.

The Working Group recommends that DHS recognize all Sector Coordinating Councils equally, in the manner in which they choose to organize.

In turn, the sector councils should constitute themselves in a way that provides for appropriate governance processes that assure checks and balances, and ensure representation for the sector as a whole.

As a part of the review process, the group requested DHS specifically define the roles and responsibilities that government would like the Sector Coordinating Councils to perform with regard to critical infrastructure protection.

In order to provide a clear understanding to all, DHS defined a typical set of functions to be performed by the councils. To lend clarity, each function description included specific definitions and a list of examples. Ms. Vismor noted this set of functions is somewhat flexible and could be expected to change over time. She also noted sectors are not identical, and not all functions may apply to all sectors.

As a part of this analysis, the Working Group determined that, at both the sector coordinating council level and at the cross sector council level, fulfilling some of these functions could constitute giving advice to the government. Some examples that illustrate these roles and responsibilities include:

- Provide a point of entry for government into the sector for addressing the entire range of critical infrastructure protection activities.
- Serve as a focal point for communication and coordination between owners and operators and with the government during response and recovery efforts.
- Facilitate information sharing capabilities and mechanisms that are the most appropriate for the sector.

The Working Group and its Study Group spent a considerable amount of time on the third deliverable, implementing the framework. The potential legal implications of various organizational structures within the Sector Partnership Model were debated. Effective critical infrastructure protection requires the ability to have real time, continuous communications and open dialogue among the public and private partners in the model. Such interaction could trigger the Federal Advisory Committee Act (FACA). FACA requirements could inhibit the dialogue between the private sector and government. Examples of these requirements include:

- Notification of meetings 15 days in advance.
- Meetings must be open to the public (An exception may be made to have a closed meeting, but in general, this requires a request be made 30 days in advance) .
- Publication of meeting notes.

In a critical situation, timeliness is essential and not all relevant information is suitable for public disclosure. Fortunately, Section 871 of the Homeland Security Act authorizes the Secretary to establish advisory committees exempt from FACA. Ms. Vismor asserted that the NIAC believes that this clause applies to the current situation in mind.

The Sector Partnership Model Working Group reached a consensus recommendation that the operational framework for the Sector Partnership model be based on an unconditional 871 exemption. The exemption should be granted at the sector coordinating council level, as well as the cross-sector level. This action will establish a known and understood framework that facilitates the

flow of advice and information concerning Critical Infrastructure Protection. Not doing so would inhibit information sharing, risk publicly disclosing critical vulnerabilities, and suppress ad hoc communication during emergencies.

Mr. Larson again addressed the Council, stating that in order to have an effective public-private partnership, a number of key operating principles must be addressed:

- Implementation of a consistent structure, applicable to all sectors that provides for equity amongst the stakeholders.
- Allowance of the Sector Coordinating Councils to self organize and retain separation from government.
- Facilitation of communication between the government and the sectors through the established sector coordinating councils and appropriate government counterparts as well as any information sharing mechanism.
- Sector Coordinating Councils will be involved in the full development of the Sector Specific Plans and able to provide direct input to the NIPP, the NRP, and other appropriate Homeland Security plans.
- The framework needs to provide a means for facilitating public and private cooperation at the regional and local levels, since past experience has proven that disasters tend to be local in nature.

When speaking about tools for information sharing, appropriate mechanisms must be in place to ensure protection of sensitive information. Both the Protected Critical Infrastructure Information (PCII) and the Homeland Security Information Network (HSIN) are tools to enable effective information sharing.

The group provided a number of recommendations to further clarify and enhance the protection of information provided via these tools. The Sector Partnership Model Working Group understands PCII is undergoing revision and recommends that the concept of originator control, where the submitter has the capability to limit how the information is used, be included and the concept of retained ownership for information housed on Homeland Security Information Network is also used.

Outside of the four principle deliverables, some other recommendations came to light. If 9/11 was the wake up call for homeland security and preparedness, Hurricanes Katrina and Rita are the wakeup call for the full continuum of the partnership model – federal, state, local and private sector environments – these events only emphasize the need with all due haste to establish the partnership model.

Like the Sector Partnership Model, other previous NIAC recommendations for crisis management coordination need to be more fully implemented to help enhance the nation's resiliency to disasters and ability to recover from them. The Group recommends a continuing focus on improving these capabilities be undertaken by the department.

In summary, the public/private partnership is vital to the protection of our nation's critical infrastructure. To create an effective partnership, the interests of all stakeholders must be acknowledged. This includes that the government recognizes that much of the information required to formulate critical infrastructure planning is both confidential and sensitive in nature. Means must be devised for protecting this information and controlling its dissemination. The Section 871 Exemption is a necessary step toward achieving this goal.

Mr. Larson closed by saying that the Working Group believes that it is imperative that the partnership model be implemented and the Section 871 exemption is granted. This, in turn, will enable further development of national response plans and ensure efficient and effective flow of critical information sharing so needed for protection of critical infrastructure. Mr. Larson thanked Chairman Nye and Secretary Chertoff and told the Council that he and Ms. Vismor would entertain questions.

Chairman Nye asked Mr. Berkeley if he wished to comment further. Mr. Berkeley told the Council he wanted to emphasize the Working Group's hard work and that all the work they have done has linked back to prior NIAC work and built upon it. Chairman Nye asked Chief Denlinger if she had any comments. Chief Denlinger said the Working Group invested a lot time and there has been a lot of substantial work done in all of the Study Group sessions.

Addressing Secretary Chertoff, Chairman Nye spoke again about the meetings the NIAC held in the morning for the association leaders. He said that those at the meeting were very anxious to support the national effort, but they were also nervous about sharing confidential corporate information at critical facilities. They expressed their concerns about vulnerabilities around critical facilities as well. To create a successful Sector Partnership, there must be rules in place. One of these rules must deal with FACA exemptions. Chairman Nye stated FACA has a strong political base and ideological support in this country and the NIAC is committed to it. They do think exemptions are applicable in some cases. Chairman Nye made the point this relationship is a partnership based on trust and mutual respect. Chairman Nye and the NIAC felt the framework and legal structure of the Sector Partnership Model is sound. Chairman Nye also recognized there will continue to be discussion on this topic because the group has not yet dealt with some of the more practical aspects of finding the right representation for each sector. The Council thinks each sector and each coordinating council needs to have a large say in that. Reliance on existing structures of the private sector will benefit the partnership more than imposing a model on the various sectors. He then asked the Secretary for comments.

Secretary Chertoff said he wanted to meet with the other senior DHS officials to reflect on it. He said the report was very thoughtful and outstanding. It really brings value to the table, demonstrating fluid interaction between the public and the private sector. It has been demonstrated time and again that there are only minutes and hours, not days and weeks to make decisions and arrangements in the midst of a dynamic event. The easier the dialogue between private and public sectors, the better off the situation will be**.** There is considerable amount of merit to the idea of letting the private sector organize itself in a way accommodating its own particular culture and prior arrangements. As long as DHS gets an optimal way to gauge industry's stance on these issues, there

should not be a problem with the Model. He said he understood the powerful argument NIAC made for a free flow of confidential information. Secretary Chertoff informed that Congress and the Homeland Security Act do provide for exceptions and DHS obviously wants to use those judiciously, but said he will weigh very carefully the interests expressed when DHS addresses the recommendations.

Chairman Nye thanked Secretary Chertoff. Chairman Nye voiced the Council's understanding that provincialism is a problem that both the government and the sectors have attempted to eliminate. The associations gave their support to this effort at the association meeting**.** Chairman Nye also emphasized that industry and non-profits affect infrastructure, and they are prepared to bring the decision makers to the table and be well represented. Chairman Nye then asked Secretary Chertoff if the Department of Homeland Security would reciprocate where there are aspects of the government that need to be represented in the government-sector relationship. The Chairman and the rest of the NIAC hoped the government would have a person in place to make these important decisions and give the partnership direction. Chairman Nye made a point to say that he meant these comments in the spirit of cooperation. The Chairman then deferred to Vice Chairman Chambers.

Vice Chairman Chambers supported the approach and looked forward to feedback from the Secretary and his team.

Chairman Nye asked the rest of the NIAC if they wished to address this topic.

Mr. Rohde asserted that the power of the exemption is immense, and he would not want that lost in how industry looks at the flow of information.

Chairman Nye said the exemption process needs to be prudently exercised. The Council believes the application of exemptions should be selective, but not restrictive. Much of the work of this organization can be open, but there are certain aspects that clearly, in the national interest, must be preserved. Chairman Nye informed the NIAC there were no further comments and they needed to consider the approval of the recommendations. The Chairman stated the Sector Partnership Model Working Group did not have a final report, but the NIAC would like to consider the recommendations with the understanding that the Working Group will present a complete report at a later time.

Mr. Berkeley motioned for the NIAC to accept the recommendations and said he would expect to have a chance to look at the final report. Mr. Rohde seconded the motion.

Chairman Nye called for a vote, and the motion carried unanimously. He then thanked Mr. Larson and Ms. Vismor for their presentation.

Mr. Larson thanked Chairman Nye and addressing Secretary Chertoff, added that the overwhelming participation from all the sectors in the Integrated Study Group enabled the Working Group to gain consensus on the clarity of the recommendations.

Chairman Nye thanked Secretary Chertoff for his time and input at the NIAC meeting.

Secretary Chertoff thanked the council for the tremendous contribution on this project and everything else, after which he departed.

B. FINAL REPORT ON 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

Ms. Marsh thanked Chairman Nye for his introduction and thanked the members and other distinguished guests for the opportunity to present the Working Group's findings and recommendations before the Council. The Working Group hopes its efforts will generate some valuable deliberation and ultimately gain the Council's approval. Prior to the meeting, the Working Group circulated a much longer and more detailed brief that provided greater insight into its approach, findings and recommendations. She said the Working Group will present a shorter version of that same brief in the hopes the NIAC can spend more time discussing the specifics of the initial findings and recommendations.

Ms. Marsh said there is an early draft white paper included in the pre-NIAC binder materials. While the approach, findings and recommendations within the paper are consistent with the Working Group's presentation, there is still work to be done before the draft is well-honed and prepared for consideration by the White House. Accordingly, the Working Group would like to focus its presentation on the briefs; they represent the findings and recommendations with which the Working Group intends to move forward.

At the July 13, 2004 NIAC meeting, the Council identified private sector risk management experience as an attribute that could strengthen existing government efforts geared towards protecting national critical infrastructure. The private sector actively engages in numerous inherently risky activities to improve each entity's competitive position. This form of risk management is a core competency of successful corporate executives and is central to the ongoing success of the corporate enterprise.

In October 2004, the Council convened a Working Group to better compare and contrast risk management practices in the public and private sector. Along this path, risk managers from DHS and the Department of Defense provided substantial contributions to both the Working Group and its Study Group. These discussions allowed the Working Group to better benchmark existing federal plans, programs, and progress. The Council's broad industry representation relies upon formalized, scientific, and tested risk management methodologies to produce three tangible and actionable recommendations of value.

The Study Group anticipates the Council's discussion and consideration of these findings and recommendations.

Ms. Marsh continued, saying part of the Working Group's efforts included analyzing risk management methods across a broad landscape. The group's survey included an assessment of risk management in public and private sectors, as an academic discipline, and the Working Group complemented this body of knowledge with an examination of a number of high-profile risk management studies.

Through this process, the Working Group defined risk management and developed a fundamental set of assumptions. It will discuss some of these assumptions as it gives its subsequent findings and recommendations the appropriate context. These definitions and assumptions likewise define the scope of the findings and recommendations.

The Working Group defined risk management as a systematic, analytical process to determine the likelihood that a threat or vulnerability will compromise an asset or resource and the accompanying process to identify actions reducing risk and mitigating an event's consequences. The Working Group agreed that risk generally cannot be eliminated, but bolstering protection from known or potential threats can reduce it. Historically, the most effective forms of risk management are predicated upon the manipulation of significant actuarial data. Actuarial data is the most complete, accurate and preferred form of risk management data. However, in the absence of actuarial data, multiple forward-looking risk management projections or analyses are available. Some of these forward-looking models have historically yielded highly accurate results. The third form of risk management data comes in the form of expert opinion. Finally, it should be noted there are a number of special challenges testing the limits of contemporary risk management, including catastrophic events and some sector interdependencies. These special scenarios represent areas for more advanced study in future endeavors.

At this point, Ms. Marsh moved into the Working Group's initial findings. Through the course of the Working Group's assessment, it identified three high-level findings:

- Risk management methodologies
- Risk management leadership
- Risk management oversight

The first finding centers on identifying robust, standardized risk management methodologies. These methodologies are supported by both advanced technologies and infrastructure and also maximize risk management program effectiveness. Investments in risk management methodology improve reporting standardization and enhance the effectiveness of risk management data. Investments in technologies for risk assessment, modeling, aggregation, analysis, and reporting is critical to complex risk management. Finally, investments in infrastructure that improve the aggregation, analysis, dissemination, reporting, or communication of usable risk information are critical to the distribution of necessary information in a timely and thorough manner.

Risk management leadership makes up the second finding. This includes a supporting organizational structure and the development of a risk management culture to enhance risk

management program effectiveness. Organizations known for highly effective risk management identify and empower leadership at the most senior levels. Organizations frequently facing and managing risks develop effective corporate cultures aligning employee and management incentives with risk mitigation. Organizations confronting significant risk management challenges also develop and implement structures promoting standardization, disseminating methods, and providing necessary sustenance through training support and education programs.

Independent risk management oversight enhances strategic direction, focus, and accountability. At the Board of Directors level, independent risk management input enhances risk management program robustness and yields fully vetted risk management priorities. Establishing risk management as a core competency of organizational leadership at the most senior levels ensures enterprise-wide focus on risk management plans and programs. Lastly, independent input and accountability on key risk management functions yields the appropriate level of attention, priority, and outcomes. Ms. Marsh then turned the floor to Stanford Hospital and Clinics' Information Technology Security Officer, Mr. Scott Blanchette. Mr. Blanchette continued the presentation.

The Study Group concluded three attributes were most commonly displayed in organizations with successful risk management records and were commonly omitted by organizations with risk management failures:

1. Create and standardize risk management methodologies and mechanisms for national planning and programs
2. Establish risk management leadership across the government for homeland security functions
3. Establish an independent risk management oversight function

In order to create and standardize risk management methodologies and mechanisms for national planning and programs, the Working Group recommends incorporating methodologies successfully developed and employed in the private sector into a national risk management system. This would include the adoption of existing "best of breed" risk management methodologies currently in use for each industry. The Working Group further recommends implementing forward-looking risk management models.

To enhance the adoption and use of these standardized risk management methodologies, the Working Group recommends continued development of risk management data identification, acquisition, and collection mechanisms. For example, there must be a continued effort to develop a national risk management database. To maximize this solution's effectiveness, effort is needed to expand the database's scope and scale and ensure tight integration between in-development database and risk management standards. The government should consider possible incentives to improve voluntary private sector contributions to this database and address existing barriers to success that currently limit participation.

Mr. Blanchette continued, saying much work is being done to develop standardized and more advanced risk management methodologies. This effort should be applauded, and support for initiatives should be continued, if not expanded.

Once mechanisms and methodologies have been established, we need to disseminate these methodologies across the government. This could be accomplished in a manner consistent with Homeland Security Presidential Directive-7 framework where DHS serves as cross-government coordinator and facilitator for this process.

A subsequent step in this process is identification of experts in the field of risk management and the inclusion of those experts in this process. These resources may come from within government, academia, or industry, and should have sector-specific expertise. They will be tasked to ensure standardized risk management methodologies are distributed across government and are adequately tailored to the needs of the sector.

These experts' secondary role will be creating risk management assumptions that are currently nonexistent and validating assumptions where they exist today. A number of forward-looking risk management models rely heavily upon assumptions. Creating and validating assumptions and the assurance the assumptions yield accurate results are critical to the risk management process. This activity will require contributions from recognized experts with substantial experience in this process.

Continued investment in the technical infrastructure will aid the dissemination of actionable information to all stakeholders. Once the risk management process reaches maturity, it is imperative usable information be distributed to stakeholders in a timely, repeatable manner. Components of this infrastructure are either currently under development or are functioning today. The Study Group recognizes the progress made on this rather substantial undertaking and recommends continued investment in this communications infrastructure.

The Working Group's second recommendation is establishing risk management leadership across government for homeland security functions. Elements of this leadership are presently in place; however, successful risk management programs identify and empower that leadership as a core component of the management team. Our recommendations on establishing risk management leadership are two-fold, focusing on both the national program level and the sector-specific agency level.

At a program level, DHS should continue to take the government-wide risk management program lead for homeland security matters. This role is similar to the corporate Office of the Chief Risk Officer. As the program lead, DHS should define and disseminate standardized risk management methodologies. Establishing and coordinating a government-wide Risk Council helps support the implementation of these methodologies. Within this framework, DHS would function as government-wide Risk Acceptance Authority.

At the sector-specific agency level, a sector-specific risk management program lead must be established. This lead would serve as the single, senior focal point for sector-specific risk management and have access to senior decision-makers for timely risk management decision-making. This lead would be responsible for defining organizational risk management assumptions, and function as the organizational Risk Acceptance Authority. The risk management lead would employ standardized risk management methods and infrastructure tailored for the sector as part of the risk mitigation strategy. Finally, this resource would assume responsibility for risk assessment and management coordination with owner and operator stakeholders.

To successfully build upon the technical and methodological capabilities identified in the first recommendation, implementation of an empowered and focused risk management leadership function across government is critical to realizing the value of this investment.

The Working Group's final recommendation is the establishment of an independent risk management oversight function. At a program level, this body would provide risk management oversight and function similar to a corporate Board of Directors. This will establish a risk management culture and identify the requisite metrics and incentives for successfully meeting programmatic objectives. This body would be responsible for validation of risk assessment and management methodologies as well as risk management assumptions and priorities.

At the sector-specific-agency level, a similarly functioning body would provide sector-specific risk management oversight and ensure compliance with strategic risk management program activities, goals and objectives. This body would function much like a corporate Board Audit Sub-Committee. They would validate decisions and assumptions and, at an operational level, establish risk management metrics, including incentives and penalties. This entity would be tasked with ensuring alignment between the national risk management program and the sector-specific agency's operational efforts.

Within the corporate environment, risk management oversight at the Board of Directors level provides much needed direction or validation that risk management decisions are being made with the appropriate priority, speed and effectiveness. With some degree of effort, it is possible to establish structures similar to those identified in the second and third recommendations to fully utilize the methods and technologies identified in the first recommendation. While there are many challenges to fully implementing these recommendations, a failure to address all three recommendations suggests the lack of a mature risk management program.

Mr. Blanchette thanked Chairman Nye and the Council for the opportunity to discuss Risk Management Approaches to Protection as well as the chance to work on this valuable project. Mr. Blanchette said both the Working Group and its Study Group believe the recommendations, if adopted, would produce tangible gains for national risk management planning and preparedness. He said he and Ms. Marsh would like to entertain questions from the Council as time permits.

Chairman Nye thanked the Working Group and said he thought the presentation was both thorough and thoughtful. This report has now moved forward for deliberations concerning the approval of

the recommendations. Although the report itself is incomplete, the recommendations are complete. He said he wanted to consider if the Council is inclined to adopt the recommendations with the understanding that the report will be coming forward.

Chief Gilbert G. Gallegos moved to accept these recommendations.

Mr. Berkeley seconded.

Chairman Nye said he did not want to foreclose discussion and wanted to hear the views of the Council.

Mr. Richard K. Davidson inquired about what kinds of incentives and penalties are envisioned.

Mr. Blanchette responded that there currently are no incentives to contribute to existing information sharing and analysis centers capabilities. He said that he thought a build-out of an effective risk management database would be crucial to capture large amounts of data, especially at sector-specific levels. Incentives are something that could be discussed as the Working Group gets further into the specifics of recommendation implementation. The Working Group certainly would entertain technical infrastructure support which has been provided especially within the healthcare sector today. DHS has provided significant contractual support to help build-out capabilities within certain sectors. Healthcare is a perfect example of a sector that has benefited greatly from those types of incentives.

Chairman Nye asked if there was anything in mind pertaining to penalties.

Mr. Blanchette said there were not any specifics.

Chairman Nye asked Mr. Peter Allor, a Study Group member, if he had any comments.

Mr. Allor thanked the Chairman and said some tax-type incentives would be broad-based incentives; the Working Group is also looking at items that are more tangible for sectors. Another corresponding issue, Exemption 871, is also addressed by the Sector Partnership Model Working Group. There is a bit of corresponding difficulty in bringing information together. This leaves a few things the Working Group needs to continue to look at.

Chairman Nye said at this point the Council wanted to see if Ms. Neill Sciarrone from the Homeland Security Council had any comments.

Ms. Sciarrone thanked the Chairman and all the members of the Council. She said Ms. Kirstjen Nielsen asked her to pass along her regrets for not being able to attend. She added the White House is appreciates the Council's active engagement and is continually impressed with the quality of the reports and recommendations brought forth.

Chairman Nye thanked her for her comments and said the Council appreciates having a representative from the White House.

Mr. Berkeley stated there are two dimensions to this report. One is the development of a way to measure risk information at an aggregated level at the government. The other is the ability to have individual companies and owners and operators learn something and get something out of this effort, so they can actually implement things on the ground. He said he thought it was important these recommendations address both aspects of this issue.

Chairman Nye said policy recommendations have all kinds of operating implications and the Council hopes the policy direction will facilitate the operational development of these plans. There are limits, however, regarding how deep the report can actually go at this level. He added it was likely well advised the Council stay away from implementation, as there are other people who have a better understanding on how to implement these recommendations. He asked if Assistant Secretary Stephan had any comments on the presentation.

Assistant Secretary Robert Stephan said that he regretted Secretary Chertoff was unable to stay for this session, because risk management is the flagship issue of his Second Stage Review and his entire approach to homeland security in general. He said both he and the Secretary appreciated the effort and leadership that went into this particular endeavor. The Assistant Secretary said one of the most intriguing things is the methodologies and technologies that help develop a culture of risk management within an organization, especially one as diverse as DHS. He asked the Working Group if they had a recommendation for creating a risk management culture across this very diverse network of communities.

Mr. Blanchette said this was an excellent question. One of the key facilitators to implementing a risk management culture is two-fold. The first is development of standardized methodologies. This could be risk assessment, risk management methodologies, or even a common nomenclature across the government. Secondary to this is the identification and empowerment of leadership who will be responsible for owning the implementation and use of those methodologies. The Study Group's research studies indicated there are pockets of excellence within the government's risk management field. There are groups doing a terrific job, but this does not necessarily translate between existing stovepipes, within DHS as well as across government. Methodologies and leadership will help knock down those stovepipes and make risk management a more permeable activity across government.

Chairman Nye thanked Mr. Blanchette for his comments. He said he hoped the events of the last few years would increase the motivation of all players to be more collaborative and receptive to maintaining their consistency. The Council has stressed this point. Chairman Nye asked if these efforts for consistency overcome the traditional philosophy.

Mr. Blanchette said he thought it must. It has to because there is no other solution. He said he also had great hopes for Total Quality Management when it was introduced about 10 or 15 years ago, but that resulted in a focus effort. He asserted the business of securing the homeland is ever changing

and has a very real threat landscape. Without implementing risk management protocols in place, there is no way to succeed. Success requires cooperation between government and industry to determine an effective risk management program. Risk management cannot just become another buzzword because the stakes are far too high.

Chairman Nye said this needs to be instilled as a basic cultural and operational attribute at every level.

Ms. Marsh added that this effort really adds to Secretary Chertoff's earlier comments. In order for something like this to work, there needs to be a concerted effort for every party to cooperate. The steps to get to this point involve leadership, communication and standard-setting. There is not a quick fix to that kind of change.

Chairman Nye asked Vice Chairman Chambers if he had any comments.

Vice Chairman Chambers said the presentation was very sound. He congratulated Ms. Marsh, Mr. Noonan, the entire Working Group, and the Study Group. He said the Council appreciates Secretary Chertoff's emphasis on risk management and his advocacy of prioritizing these risks. He thought one thing being stressed repeatedly is there is a need for an organization-wide approach with oversight and accountability trickling down from the top. There has to be a way to affect the culture so as to better emphasize the sheer importance of risk management. He then reiterated that the presentation was nicely done.

Chairman Nye thanked Vice Chairman Chambers and asked if there were any other comments. He said there already was a motion on the floor and asked if this motion was seconded.

The motion was seconded.

Chairman Nye asked if the motion had any opponents. Hearing none, he stated the motion carried.

He thanked the members and said the Council would hear status reports on two of its other initiatives. He invited Vice Chairman Chambers and Chief Gallegos to present their update on the Intelligence Coordination Working Group.

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

Vice Chairman Chambers thanked Chairman Nye and congratulated the Working Group on the progress they have made. He then turned the presentation over to Chief Gallegos and Mr. Ken Watson.

Chief Gallegos thanked the Vice Chairman for his leadership, as well as Mr. Watson and the DHS staff for their assistance. He continued, telling the NIAC that the morning briefing on the importance of intelligence from Assistant Secretary for Information Analysis Charles E. Allen underscored the significance of this Working Group. Chief Gallegos believed one of the challenges confronting the Working Group is gathering an understanding of intelligence in this context. He told the Chairman the Working Group was not ready to present any recommendations but would present a status report. He turned the floor to Mr. Watson to begin the presentation.

Mr. Watson said he would review the Working Group's purpose, speak about their actions to date, present some initial findings, and outline the Working Group's next steps. The Working Group is striving to accomplish three objectives:

- The Intelligence Community must understand the private sector's critical needs; this understanding should drive requirements, analysis, and information dissemination, and should capitalize on the private sector's capabilities to assist in information sharing.
- The private sector must understand how the intelligence community works, in order to have input into their processes, particularly as they apply to threat assessments.
- Policymakers must understand both sides, e.g., what is critical to the intelligence community and to the private sector that can help inform decisions.

The team developed a unique approach to understanding the issues. The obvious first step was to get everyone around the same table. To date, the Study Group has had three in-person meetings with representatives of the Intelligence Community and the private sector. The next meeting is slated for some time in December. The process was developed to solicit input on ideas about information needs from all stakeholders, validate those inputs through teleconferences and face-to-face meetings, and develop single-issue papers and redistribute those for comment. The Working Group is now recombining the results of those issue papers to develop findings, conclusions, and recommendations.

Mr. Watson said the Working Group keeps returning to law enforcement as essential to coordination. This coordination involves foreign, domestic, private, public, national, state, and local information. The focus of the effort over the upcoming months will be looking at law enforcement, communications, and information sharing as the coordination hub. So far, the Study Group has developed four tightly interrelated initial findings.

The first finding is the need for a national-level fusion center. The term "fusion center" is defined differently depending on the background and experience of the individual. The Study Group has validated the need to coordinate requirements, analysis, and dissemination at multiple levels and for multiple audiences**.** Whether that fusion center belongs in DHS, the National Counterterrorism Center, within some other organization, or if it is virtual or partially virtual is still to be determined**.**

Second, trusted relationships are essential to success. Part of the enthusiasm in those face-to-face meetings is due to simply meeting counterparts from various agencies and sectors. The education process is also a two-way street. The community needs to better understand private sector critical issues and the private sector needs to better understand intelligence processes.

The third finding is the need to streamline the request for information (RFI) process. The success of RFIs hinges on who can ask for something from the other side, who must vet that question, who can answer the question, and also how to distribute, vet, and provide access to the information. There are no easy answers to these questions, and that is why there is still a bit of work to do.

Finally, there is a need to protect information for the originator, but also a need to share it. So, concepts like originator control, proprietary information, the entire Protected Critical Infrastructure Information (PCII) Program, and other information and protection schemes are being considered. Some information still must remain compartmentalized for certain audiences. This includes law enforcement-sensitive information.

The Study Group is currently gathering input on its issue papers. They will map the results to existing capabilities and those include items like HITRAC, Homeland Information Security Network (HISN), Information Sharing and Analysis Centers (ISACs), and other capabilities. He added that DHS Information Analysis (IA) is doing a very thorough job of identifying those capabilities**.** Finally, the Study Group will be developing conclusions, recommendations, and a report. Mr. Watson asserted the goal is to provide a draft report to the NIAC members well before the next meeting to give them a chance to examine the recommendations and put them to a vote at the February 13, 2006 meeting. However, the Working Group is holding out for quality over timeliness; if these recommendations end up in further deliberations, it will have no qualms about delaying the final presentation to the next meeting. Mr. Watson concluded his remarks and turned the presentation back to Chief Gallegos.

Chief Gallegos thanked Mr. Watson and said the Working Group had hoped to deliver a complete report and recommendations sooner, but decided it was best to present quality recommendations instead of delivering a rushed project**.** He said this explained why the Working Group is spending more time on the issue papers. Working with the intelligence community, the Working Group will focus its efforts in the next few months on the law enforcement perspective**.**

If the Working Group is going to mesh the information and really develop a partnership, it must be able to interact with people in both the private sector and in law enforcement. He said the Working Group has reached out to law enforcement and received a briefing from the Los Angeles Police Department (LAPD) on Operation Archangel, which the Chief designated as a good model. While the models have to fit every agency, there are over 17,000 law enforcement agencies nationwide with 700,000 officers; it is difficult to develop a composite recommendation to suit everyone**.** Chief Gallegos asserted the Working Group will come up with interesting models, develop these conclusions, and make recommendations at that time. Law enforcement must become more involved with the Intelligence Coordination Study Group, and the Working Group is reaching out to

them. Chief Gallegos thought the Working Group will have a substantial report along with recommendations at the next meeting. He turned the presentation over the Vice Chairman Chambers.

Vice Chairman Chambers summarized the presentation by saying this initiative is really about finding seams between:

- Intelligence agencies
- Local, state and national law enforcement
- Law enforcement and intelligence
- Private sector and public sector

Once these seams are identified, the idea is to smooth them out**.** The concept of a fusion center, developing trusted relationships, streamlining requests, and protecting information all take their requirements from this goal. Vice Chairman Chambers then deferred to Chairman Nye.

Chairman Nye thanked the Vice Chairman and Chief Gallegos and said the Council appreciated their hard work He moved on to Mr. Alfred R. Berkeley and Dr. Linwood Rose for the Workforce Preparation, Education and Research Working Group's status update.

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

Dr. Rose thanked the Chairman and said the Working Group will present some initial findings that will eventually lead to recommendations. He said the Working Group had made considerable progress since the July meeting. This progress has been achieved through weekly conference calls that allow the Study Group a chance for discussion. He anticipated a distribution of a draft narrative report and findings in the near future to allow the Council sufficient time for review and approval, hopefully in February.

Dr. Rose said the Working Group has been motivated by its desire to ensure that the American education system and training processes prepare a workforce of sufficient quality and quantity to address national critical infrastructure protection needs. Additionally, it is extremely important that sufficient cyber-security research is conducted efficiently and effectively to protect computer communications networks. Dr. Rose said he wanted to briefly share where the Working Group is in its studies with cyber-security research, its review of the Scholarship for Service programs, and its review of information assurance certification programs. Mr. Berkeley will then comment on the Working Group's progress to date, particularly focusing on math and science competency. The Working Group will complete its draft for distribution to the members and will offer recommendations in the following areas:

- Research and development priorities to improve cyber security

- Efficacy of the Cyber Corps Program
- Cyber Security Certification Programs
- K-12 math and science competency

The Working Group will present its findings on cyber security research and proposed recommendations related to topics addressing coordinating cyber research efforts, prioritizing the national cyber security research agenda, obtaining adequate research funding and a sufficient researcher talent pool. The Working Group also anticipates recommending additional studies to reduce time-to-market issues for research products.

Dr. Rose said Mr. Richard Holmes, General Director of Security and Quality Assurance at Union-Pacific Railroads, provided the Study Group with a thorough report on the National Science Foundation's (NSF) Scholarship for Service program. Before distribution to the NIAC, the Working Group will also review comparable programs operated by the Department of Defense and the National Security Agency (NSA). Certifying knowledge, skills and abilities for cyber security personnel is particularly challenging given the pace of change associated with the field. However, the Working Group feels a movement toward position standardization relative to position requirements and qualifications would be beneficial. The creation of a privately-administered information assurance certification body with modular computer-based testing and metrics is viewed as a desirable step towards making the cyber security workforce. At this point, Dr. Rose turned the floor to Mr. Berkeley for his presentation on Education and Workforce Preparation.

Mr. Berkeley thanked Dr. Rose and said the Working Group will likely return to the NIAC with a series of recommendations, probably in 13 areas. He said there have been about 30 participants from various sectors of education join in on the Study Group's conference calls. These participants have backgrounds including school district administrators, teachers, textbook publishers, and education academics. The first area the Working Group is particularly interested in is bringing transparency into areas where it may actually be the catalyst for positive change for the good. This can balance issues between what the Federal Government can and should do in education with what states and local districts can and should do with education.

Mr. Berkeley said there is real political tension and emotion around this issue. Some of these topics and issues resonate around the country, and one way the Working Group thinks it can address them is by simply shedding light on the issue. It is important to understand issues like curricula (or what is being taught), pedagogy (or how it is taught), and the role of state standards. These standards can vary a great deal from state to state or district to district.

Another issue is the idea American schools teach students in an "inch deep, mile wide" manner; they focus on many different things while not providing substantial depth. This breadth and depth issue is of special significance particularly as it relates to how other nations are developing educational criteria. In many cases, they tend to extend their instruction deeply into fewer areas and, consequently, produce real competency instead of a smattering of knowledge across many disparate topics.

He continued, saying the second area the Working Group is looking to generate recommendations on is the role of teacher colleges and teacher preparation, particularly as they are funded and linked to curricula or a pedagogy that is proven to work or not work.

Mr. Berkeley stated the third area attempts to make parents, students, and teachers aware of what a student should know at a particular age. This effort is being done well in other countries. The Working Group has used the United Kingdom's math curricula as an example of what is being done successfully in other nations. British math curricula makes parents aware of the base level of knowledge expected of a child at a particular age.

The next issue relates to how tests and curricula are developed. In the United States, tests and examinations tend to be developed by educators. In other counties with successful math and science programs, mathematicians and practitioners of the particular scientific discipline are included in the development process. In other cases, employers cognizant of what skills are needed in the workforces are also involved.

Another item to consider is the issue of sequence. The Working Group found a successful program called Physics First that reverses the traditional curriculum sequence of biology, chemistry, and then physics. This program advocates teaching physics before the other two subjects based on the theory chemistry cannot be understood until physics has been taught. This thinking also states biology is not comprehensible until chemistry is completed. The science program the U.S. follows stems from an educational model that is 100 years old. This harkens back to a time when biology entailed barnyard animals, chemistry was a jar of vinegar and baking soda, and physics was creating a vacuum by burning a candle in a milk bottle. This is far too elementary for educating a globally competitive workforce.

The Working Group also has found itself embroiled in the philosophical battle between educational camps. It will return recommendations to the NIAC about the argument between what detractors call "drill and kill" and the other approach called discovery. Discovery is an idea asserting every child can discover the meaning of words, the meaning of math, or reinvent Isaac Newton's or Albert Einstein's inventions. The Working Group thinks there needs to be a neurological basis to formulating educational techniques. There are a certain number of repetitions that are absolutely necessary to create long-term memory. He said the group will address this issue in its recommendations.

There is also a role for automation in education. One of the roles for computers is low-risk, self-testing where web-based programs allow students to independently determine their own levels of knowledge without the high-risk grade system that affects course placement or college admission. In the Study Group's discussions with educators, the proper role of automation has rarely surfaced but it is an item the group will address. He said the group desires to put some transparency on some of the unintended consequences high-risk test taking generates in some schools. There will always be need for accountability in education; however, it is clear the U.S. must recognize some of the side effects of modern testing.

Mr. Berkeley said the Working Group will also examine vocabulary. Vocabulary is an excellent indicator of future academic success and success in the workplace. Surprisingly enough, one of the Study Group's speakers stated vocabulary is not taught after fourth grade. The group will discuss the role of vocabulary and how it can and should be promulgated.

The Working Group will use business terms like market segmentation to address tracking, a politically sensitive topic. There has been a great deal of dialogue around how students are grouped and whether or not this helps. In business jargon, this is considered specialization of labor. This issue also ties into the question of whether there is a need for math and science specialists deeper in school systems.

Mr. Berkeley stated there are other areas unaffiliated with K-12 education, the Working Group's original charter, but were suggested by one of the NIAC members. It is important the U.S. does not drive out PhD recipients from the top American schools by sending them home immediately when their student visas expire. The Working Group will present recommendations about finding the right balance between identifying and retaining high achievers while also taking into account national security interests by understanding the graduates' backgrounds and affiliations.

He concluded by saying the U.S. faces a globally competitive workforce and issues of maintaining the competitiveness of the American industrial base. The national education system must realize, in addition to basic cyber skills, there is a marked need for a workforce literate in math and science. He said the Working Group understands not one of these recommendations is going to be the proverbial silver bullet, but if each of these recommendations made a small difference that would truly be a tremendous contribution.

Mr. Berkeley then asked the Council if there were any questions.

Chairman Nye asked what Mr. Berkeley meant by high-stakes testing.

Mr. Berkeley said the education community refers to tests that mean a lot to a student's future as "high-stakes". An examination determining college admission or placement in a more advanced program falls under this category. Not only are these kinds of tests extremely important to the student, they are also highly significant for the school, the school district, and the teacher. The Working Group has received input that some school districts are essentially asking the better students to study on their own to allow the teacher to spend a tremendous amount of time with students hovering around the passing level. The stakes for an individual school or for a school district are very high and, therefore, they need to maximize their number of passing students.

Chairman Nye asked if the corollary to this is students holding no prospect of passing get no attention at all.

Mr. Berkeley said this was likely the case.

Chairman Nye likened this approach to a triage. Those who are clearly going to pass or fail anyway receive minimal attention, while those who could go either way receive the bulk of the attention.

Mr. Berkeley said this was the testimony of the Study Group.

Chairman Nye asked if this affected the Working Group's views on accountability.

Mr. Berkeley said this is a complex issue and there needs to be accountability and results. The question is whether this accountability centers on the average of the class, school or district, or if it is some measure of accountability for each student. One of the biggest issues the Study Group has discussed is the movement of students from school to school each year. Roughly twenty percent of students are changing schools annually, making it difficult to maintain continuity over time.

Chairman Nye said in the utility business twenty percent of customers move every year. He also said he did not want to belabor the point, but asked Mr. Berkeley about providing green cards to successful science and math students who are in the U.S. on a student visa. He inquired if the Working Group had addressed the current problem of visa availability for foreign students.

Dr. Rose said the topic had not been addressed. He said he served on a national academy's work group specifically on this topic. Mr. Craig Barrett, NIAC Member and Chairman of the Board for Intel Corporation, has been very involved in the topic for several years. He has first hand experience in handling a talent shortage for the semiconductor industry as well as dealing with H1B visa restrictions, the primary and most sought after USA work visa that is typically valid for up to six years and entitles the visa holder's spouse and children to accompany them and live in America; there is knowledge of this issue built in to the NIAC.

Chairman Nye said he knew there is higher education data for science, mathematics, and engineering. Some countries traditionally pour a large number of high talent students into the U.S. for training in certain fields. Because of post 9/11 difficulties in the visa process, Australia has experienced a boom in students from a lack of ability to get visas here. He said this was troubling because he believes the world benefits from having people educated in the U.S. It serves the nation's interest to have high caliber students entering the country for post graduate and graduate education.

Dr. Rose replied that comments to that effect will go in the report.

Chairman Nye asked if there were any other questions. There were none, and he then asked if Vice Chairman Chambers had any further comments.

Vice Chairman Chambers echoed the Chairman's comments thanking Dr. Rose and Mr. Berkeley for an extremely thorough investigation. Educating the next generation of innovators is critical and he shared the Chairman's views that the focus should be on developing and retaining the world's best and brightest. Industry should be able to help greatly with the curriculum. This curriculum should be research and standards-driven. He said he looked forward to seeing the final report.

Chairman Nye thanked the Vice Chairman and said the Council was going to move into new business. The Council has the opportunity to select a few new projects. This always involves some diverse views and, therefore, takes time. On top of this, there is the task of enticing members to take leadership on these new initiatives.

Additionally, the Council will hear from Assistant Secretary Stephan on some recent DHS activities. Before this, Ms. Wong will present a review of the revised NIAC Charter and the Executive Order. At this point, he turned the floor to Ms. Wong.

VII. NEW BUSINESS NIAC Chairman *Erle A. Nye* Presiding

A. REVIEW OF REVISED NIAC CHARTER/EXECUTIVE ORDER *Nancy J. Wong*

Ms. Wong thanked the Chairman and said Ms. Jenny Menna will review the NIAC Charter and the Executive Order for the Council.

Ms. Menna thanked Ms. Wong. She opened by saying the NIAC Charter was renewed by Secretary Chertoff on July 1, 2005. The NIAC Executive Order was renewed by the President on September 29, 2005 under Executive Order 13385. These renewals were part of a regular two year renewal cycle.

As a part of the renewal process, the NIAC Members, DHS, and the White House staff reviewed the charter and executive order. Three areas for update were identified, and have subsequently been addressed in the new documents. The NIAC recognized that cyber and physical security are inseparable. Therefore, the NIAC's scope was slightly expanded to address physical infrastructure. The documents previously stated that the NIAC would "advise the President on the security of the information systems supporting the nation's critical infrastructure." The new version states "with advice on the security of the critical infrastructure sectors and their information systems…" The NIAC's current initiatives reflect this direction. In addition, the NIAC membership has evolved to reflect this broader critical infrastructure direction. The charter and executive order were also amended slightly to allow for representation by all 17 CI/KR sectors designated by HSPD-7, rather than the five listed in the original documents.

To further reflect the new terminology used under HSPD-7, and the Interim NIPP, the documents were slightly modified to update such terms as "lead agencies" to "sector specific agencies," and "sector coordinators" to "sector coordinating mechanisms" References to the ISACs were broadened to refer to "sector coordinating councils and their information sharing mechanisms," in recognition of broader requirements for public-private partnerships and an increased array and diversity of information sharing approaches and needs in each sector, including those where no ISAC exists.

Finally, in coordination with the NSTAC, a clause was added to indicate that the NIAC will defer matters pertaining to National Security and Emergency Preparedness (NS/EP) Communications to the President's National Security Telecommunications Advisory Committee (NSTAC). The NIAC will also coordinate issues that affect national security and emergency preparedness (NS/EP) communications policy with the NSTAC. NS/EP communications allow the Federal Government to coordinate immediate response to all emergencies, whether caused naturally, stemming from an act of domestic terrorism, a man-made disaster, or a cyber attack. Ms. Menna concluded her remarks, stating that copies of the updated documents have been provided for the members in their binders and will be provided on the NIAC website.

Ms. Wong thanked Ms. Menna and asked if there were any questions. Hearing none, she moved into the status update on the implementation of the Council's recommendations.

B. STATUS REPORT ON IMPLEMENTATION OF RECOMMENDATIONS — *Nancy J. Wong*

Next, Ms. Wong provided the Council with a status update on the recommendations they have made to the President. This Council is incredibly productive in producing highly regarded reports and recommendations over a relatively short period of time. Some of these reports often intersect with and reinforce one another. As a result, the Secretariat has been working with the White House and Ms Sciarrone's office on an organizational framework and process to facilitate a regular review of the Council's recommendations disposition and progress and report back to the Council on a regular basis. Part of this is to organize the recommendations in such a way that is coherent to report back to the Council.

Ms. Wong stated that the Council has had a strong impact and is effective in contributing to the policy strategy and the government's critical infrastructure program development. Several NIAC studies and recommendations have broken new ground in developing an understanding of some very tough issues. It takes a Council like this to be able to tackle these kinds of difficult issues—it truly is an independent body with the expertise to handle these challenges. The Council has produced a couple of innovative and useful tools to both industry and government. These results could not have been obtained without the active commitments and participation of the Council members and their supporting staffs. Many of the reports have become important references for others outside of government also working on critical infrastructure protection and security issues.

Ms. Wong said she would only provide brief highlights due to time constraints. She began with the independent Internet Protocol Version 6 (IPv6) recommendation for the President to establish a task force and develop the national policy to remain competitive with countries in the Pacific Rim and Europe. DHS and the Department of Commerce co-sponsored the IPv6 task force chaired by National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA). These two units are sub-organizations within the Department of Commerce and delivered a draft report called *The Evolving Internet*, a technical and economic assessment of the IPv6, to the public for comment in January 2005.

The Department of Commerce also held a public meeting on July 28, 2005 with stakeholders to assess the impact of the study results. The Secretariat will provide more detail in giving feedback on the recommendations results. The Council's first report from the Interdependency Risk Assessment Working Group laid out the landscape of the sector coordination responsibilities that has become the conceptual framework for the Sector Partnership Model. Many of the recommendations from this report and from the Evaluation and Enhancement of Information Sharing report were addressed in a briefing given by Mr. Jim Caverly, Director of the Infrastructure Coordination Division, at the January 2005 NIAC meeting. The implementation of the Sector Partnership Model along with new support organizations is recognized and supported by unprecedented cooperation bridging the public and private sector communities. The work of the Council on the Sector Partnership Model over the last six months, culminating in the implementation of recommendations, brings the Council's recommendations from concept to practical reality. This Council has been very intimately involved in core recommendations affecting the execution of that model. DHS' National Cyber Security Division (NCSD) worked to develop a vulnerability management framework to address software vulnerabilities as recommended in the Final Report and Recommendations of the Vulnerability Disclosure Working Group issued last year. DHS is currently considering processes to implement the rest of the recommendations in that report.

Ms. Wong continued, saying the implementation of the Common Vulnerability Scoring System (CVSS), a follow-up report to the Vulnerability Disclosure Framework, is an excellent example of public-private partnership. Since the report was issued, the private sector's Forum of Incident Response and Security Teams (FIRST) has stepped up to be CVSS' custodian. It is an emerging standard in vulnerability scoring but is still in its first generation stage. It has been adopted by at least eight pioneer companies and very influential leaders in their industry.

The Hardening the Internet Working Group's Final Report and Recommendations spurred NCSD into establishing the Internet Disruption Working Group in coordination with the National Communications Systems (NCS) to address the resiliency and recovery of Internet functions in the case of a major cyber incident. As part of this initiative, these two divisions will host a forum later this year with private sector and government subject matter experts to prioritize and develop implementation plans for the Hardening the Internet Working Group's recommendations. An initial focus of the Working Group is to identify near-term actions related to situational awareness, protection, and response steps that government and stakeholders can take to better prepare for, protect against, and mitigate nationally significant Internet disruptions. NCSD has also initiated efforts to better inform consumers across the public-private and academic spectrums so that they are better positioned to request and acquire secure software.

The Prioritization of Cyber Vulnerabilities Working Group advocated cooperation with critical sectors to examine risks and/or vulnerabilities of providing critical services over network based systems. NCSD is providing guidance, expertise, and strategies to the sector specific agencies and developing their part of the national infrastructure protection plan when identifying, assessing, and protecting their cyber assets and cyber elements of physical assets. Consequently, cyber security will be an integral part of the NIPP, critical infrastructure protection, and national and sector risk

calculations. This is a very important point because this council has always presented the perspective that cyber and physical are highly integrated and cannot be separated out. And so the national plan that is in the process of being developed will integrate both into the national risk calculation. Within the context of a large-scale cyber incident affecting critical key sectors such as energy, IT, telecom, and transportation, DHS will be sponsoring a national cyber exercise called Cyber Storm in February 2006 to exercise the public and private national cyber incident response community and highlight available tools and analytic capabilities available for a cyber incident response and recovery and raise awareness of the economic and national security impacts associated with a significant cyber incident.

Ms. Wong stated that the Final Report and Recommendations on the Best Practices for Government Intervention to Enhance Security of the National Critical Infrastructures has also generated a fair amount of feedback. It was deemed more of a best practices report than a document with specific recommendations. It is considered by many inside and outside government as a seminal reference work. For example, a research analyst from the prestigious Conference Board reported this particular report would be quite useful as a reference for their study developing security metrics for private industry. The Council recommended making this report available as a reference to those governmental entities responsible for regulation, and it is publicly available on the DHS NIAC website. The NIAC Secretariat is currently developing protocols and target audiences for proactive distribution of this best practice report. Ms. Wong thanked the Chairman and concluded her remarks.

Chairman Nye asked if there were any questions for Ms. Wong. There were none. He said he had not reviewed this material before but understood the Council had been doing some good work and people are indeed paying attention.

Vice Chairman Chambers reiterated the Chairman's comments and thanked Ms. Wong for her positive words. He stressed the importance of being very direct with the Council in terms of where it is making a difference and where its efforts are not adding value.

C. DELIBERATION AND VOTING ON NEW INITIATIVES — *NIAC Members*

Chairman Nye asked the NIAC to move on to the deliberation on new initiatives. Because of two sets of final recommendations presented at the meeting, Chairman Nye informed the Council they must find two new Working Group initiatives**.** Vice Chairman Chambers, Mr. Bill Muston of TXU Corp. and Mr. Ken Watson of Cisco Systems, Inc. sent possible initiatives to the members and used their feedback to narrow the prospective list. The Chairman told the members they are responsible for not only finding new initiatives but also determining how many initiatives the Council can handle. He then asked Mr. Muston and Mr. Watson to give their presentation.

Mr. Muston thanked the Chairman, and told the Council that he and Mr. Watson will cover the methodology they used to develop these materials, provide an overview for each of the identified topics, and discuss the process for prioritizing those topics. The development of the topics occurred

over the 15 months during which Mr. Muston and Mr. Watson received inputs from members of the Council. They also received input from White House staff and from DHS on topics they thought might be worthy of Council review. This task included reviewing prior submissions as well as the inputs from many Council members in the last quarter. They also considered topics arising from the meeting with the President in July. Those resulted in a total of ten topics sent back out to Council members for review and comment. They were also vetted through DHS and the White House for reduction and prioritization. As a result of this effort, Mr. Muston and Mr. Watson narrowed the field to seven topics. He proposed that Chairman Nye present each topic and then allow a question and answer session on the topic before proceeding to the next one. At this point, Mr. Muston turned the presentation over to Mr. Watson.

Mr. Watson said they started with ten topics to rank. He said they approached the project by looking at each issue's relevance to three different groups:

- Technology sector
- Physical infrastructures
- Government

Vetting the relevance of the ten proposed topics to these groups, he and Mr. Muston were able to narrow the list to seven topics**.** The first of these was the Physical and Cyber Convergence topic. The question before the Council was as physical and cyber technologies converge and network management for both consolidates, are network system vulnerabilities adequately being addressed by industry and government sectors? Furthermore, what are the appropriate actions for government and industry? These systems cover everything from control systems, including supervisory control and data acquisition systems, to distributed physical systems and process controls for production facilities and infrastructure services, and include requirements like reliability, redundancy, and latency, and have various technical and policy considerations associated with them. As the systems migrate to the Internet protocol, what research needs to be done, is adequate research being funded, are there best practices that need to be implemented, what are the architectural issues, and what are the policy issues? Mr. Watson then turned over the presentation to Mr. Muston.

Mr. Muston told the NIAC the next topic is around potential attacks using chemical, biological, or radiological means. In the planning and preparation for those events, an important question is whether the role of critical infrastructures and their employees has been adequately considered in the planning and preparation for these attacks? He said they identified potential issues such as a potential education need for the workers, their supervisors and their families. During any event, both with normal operations continuity, as well as restoration, repair and recovery, are there special protection needs for critical infrastructure workers beyond what they would employ in the ordinary course of their business today? An important question is whether public health authorities recognize and plan for critical infrastructure workers with respect to these events and pandemics and are critical infrastructure managers adequately prepared in order to continue operations during such events and pandemics? Mr. Muston then turned over the presentation to Mr. Watson for the next topic.

Mr. Watson told the NIAC the next topic is the use of technologies to support critical infrastructure protection and explained that it is a combination of two of the original topics. The first topic was using network information systems for critical infrastructure protection and the other was using database correlation for terrorist tracking purposes. There is a very significant policy issue here because this is not only about using emerging technologies effectively for critical infrastructure protection, but asking what those technologies imply regarding privacy issues. Capabilities of remote monitoring and providing assistance continue to expand while their costs decrease. This includes video, intruder and contact sensor, gaseous sensors and databases that can be correlated to track terrorists and other criminals. What capabilities are truly near commercial reality, and, of those, what would be valuable to critical infrastructure protection? Are there values to owners/operators beyond critical infrastructure protection for those systems and does use of those systems raise policy issues that we need to address such as privacy or other issues? Mr. Watson said the work product would be a recommendation on policy around employing these new technologies.

Mr. Watson then addressed the next topic of software assurance**.** The question here is whether special policies and practices are needed in regard to security aspects of software provided to critical infrastructure owners and operators. How can software be improved in order to ensure continued functionality and productivity, with a measure of security for critical infrastructures. Software development processes contribute to improving software quality**.** Many believe improving the formal development methodology will bolster the state of the art in system design, and produce the most effective software. It has been suggested a systems design approach, combined with a new academic software training emphasis, will provide more consistent control over software quality. Some have examined the guild approach with formal apprentice, journeyman, and expert levels as a possible framework to establish and maintain demonstrable competence in both skill and understanding of key concepts. The question would be: what policies would lead to the most beneficial approach for software assurance and what are the proper roles of government, industry, and academia in such approaches?

Vice Chairman Chambers added each software group develops with their own strong views on the value they add. Educating people, especially new software developers, and getting common approaches to teach security being imbedded in software from the beginning would add a great deal of comfort to the consumers of this software regardless of industry, and really taking a look at it, not to say what must be done, but rather here are the best practices and procedures we ought encourage and be aware of, perhaps even with a 'Good Housekeeping Seal of approval' for having the capability.

Mr. Watson said there are several organizations that have proposed a more rigorous point product certification process to assure customers of software quality, and this effort would include examining that approach in the context of a more broad systems design concept to assess the contributions of both.

Mr. Muston said the next topic is a broad topic around interdependencies**.** Mr. Muston said that he and Mr. Watson collected a number of inputs dealing with discrete interdependency issues and those are grouped under this broad heading of interdependencies. He thought interdependencies may exist

that are not evident in normal operations but do become evident in times of stress. Perhaps those interdependencies are not adequately considered in the various planning efforts by critical infrastructure owners and operators as well as by government entities. There has been feedback that the interdependencies with local, state, and national government are not well understood. Localized critical infrastructures often have well-established relationships at the local level and may not be as visible at the national level. The coordination at the local, state, and national level is important for both for national companies with local facilities as well as between the federal, state, and local governments. Another interesting aspect of interdependencies has been geographical concentrations where there may be an unusual concentration of a particular critical infrastructure or multiple critical infrastructures in one area. Mr. Muston said Hurricane Katrina highlighted the dependence on oil facilities in the New Orleans area as well as whether critical infrastructure interdependencies had been adequately considered in disaster planning.

Self-governance is a topic that was also put forward. The Council has already considered its Best Practices Report for Government Intervention in free markets to achieve the requisite critical infrastructure protection. The report indicates there are mechanisms within markets which will self-correct and achieve the changes the government seeks. One of the key questions repeatedly asked is if there are standards and development processes within a sector. Mr. Muston said there is a variety of understanding of self-governance among the sectors. The financial sector has a long experience with self-governance. The National Association of Security Dealers (NASD) was formed in 1937 and is a legislatively authorized self-governance mechanism with oversight by the Securities and Exchange Commission (SEC). The electric sector also has a self-governance mechanism that originated from the 1965 blackout--the North American Electric Reliability Council (NERC) and its regional councils. There is also a joint commission on healthcare organization accreditation in place to provide self-governance among private healthcare organizations in lieu of certain federal oversight. There are some instances where these self-governance mechanisms have been beneficial in sectors. Additionally, a variety of self-governance levels are not necessarily delineated, but range from best practices to standards development by voluntary to mandatory use of standards, compliance audits, and then using legislative authority for self-governance organizations to exercise their authority**.**

Chairman Nye said there is a demonstrated need for this, and the national interest in each industry sector would be apparent. Self-governance models are preferred in most instances to direct government intervention, and it is important to balance government needs under times of stress and yet maintain free enterprise**.** The Chairman told the Council that it is very curious that the electric industry for forty years now has operated under a self-governance system which relied on peer pressure and relied on getting along and going along. But with the introduction of more competition into the industry it became apparent peer pressure was not what it once was. This is a somewhat narrow subject but it's one that probably could be finished in fairly short order.

Mr. Berkeley said this issue touches on his experiences from the financial services sector. It seems if there is going to be more direct government involvement in the sectors most important to the Council, it is then very important to examine a self-governance layer there. In the financial services industry there are approximately 600,000 people in the American broker-dealer community. The

beauty of self-regulation is it allows people to make changes more quickly than a one-size-fits-all approach and allows the SEC, for example, to ask the NASD to resolve certain problems through broad industry participation. It allows for the minor things to be dealt with at a lower level and for circumstances to be taken into account on a case-by-case basis.

Mr. Muston told the NIAC the last topic was Risk Transfer. Commercial risk transfer mechanisms like insurance are adequate for competitive and market needs and are widely practiced. Insurance mechanisms even address natural disasters. Some larger natural disasters and terrorism risks push damages beyond the ability and experience of private systems. The role of the government is to consider such scenarios and what things like tax incentives, enterprise zones, grants, and loans can do to change the economic calculus associated with risk transfer in the free market. There is a question if government intervention actually increases financial stability and, therefore, improves critical infrastructure protection. After 9/11, there was somewhat of a crisis in the commercial real estate insurance market. Congress took some action that expires at the end of this year. The question is if the federal government can benefit from a decision support process for risk transfer decisions that could be employed in response to a catastrophic natural disaster or terrorist attack. Additionally, would critical infrastructures benefit if the government had such a decision support process?

Chairman Nye said in his understanding of Mr. Muston's presentation, industry should be responsible for it own risk analyses. Chairman Nye saw this as an extension of the planning that must be done in connection with these kinds of events.

The Chairman said the NIAC must recognize the cultures around cyber security and physical security are quite different.

Chairman Nye asked Assistant Secretary Stephan if he had any opinions on the subject. Assistant Secretary Stephan told the Council the President wanted him to note where pieces of infrastructure are being used as weapons of mass destruction or mass effect. The Assistant Secretary wanted the Council to work on initiatives that go along with HSPD-7.

Mr. Caverly suggested the NIAC look into the Chemical, Biological and Radiological events issue because of the current concern of a pandemic created by the avian flu.

Chairman Nye asked the Council if anyone else had any recommendations or comments. Once knowing they did not, the Chairman and Ms. Wong proceeded to begin the voting.

The first item, the physical and cyber convergence received eight 'yes' votes and two 'no' votes

The second item, Chemical, Biological and Radiological events received eight 'yes' votes and one 'no' vote.

Technologies for Critical Infrastructure Protection, received five 'yes' and four 'no' votes.

Software Assurance received no 'yes' votes and nine 'no' votes.

The fifth item, Interdependencies, received six 'yes' votes and three 'no' votes.

Self governance received zero 'yes' votes and nine 'no' votes.

Risk Transfer also garnered no affirmatives and nine negatives.

Chairman Nye said the favorites were the Physical/Cyber Convergence and the Chemical, Biological and Radiological events. The next most popular were Interdependencies and Technologies for Critical Infrastructure Protection. Chairman Nye then said the NIAC should immediately start with the two most popular issues: 1) Physical and Cyber Convergence and 2) Chemical, Biological and Radiological events. When two current initiatives are finalized, the Council should move to the next most popular item, Interdependencies and Technologies for Critical Infrastructure Protection.

Chief Gallegos motioned to accept the vote and Mr. Berkeley seconded. Mr. Berkeley asked that the three topics not chosen at the meeting should be the next topics considered after the four new topics are completed. Chairman Nye agreed with him.

The Council voted on the motion and it carried unanimously.

Chairman Nye told the NIAC they now needed chairpersons for the new initiatives. He told them that he was mindful of the time and hard work everyone on the Council has given thus far and asked if anyone would be interested in chairing the Physical/Cyber Convergence Working Group. Ms. Grayson offered to chair the Working Group and Mr. Peters also offered to co-chair. Chairman Nye asked Mr. Conrades' representative, Mr. Andy Ellis, if Mr. Conrades would be available to help with the Working Group. Mr. Ellis offered to relay the message to Mr. Conrades.

Chairman Nye told the NIAC Chief Denlinger had been recommended for the Chemical, Biological and Radiological Working Group. She told the Chairman she would be willing to lead the Working Group if someone could set her in the right direction. Ms. Marsh offered to act as one of the co-chairs.

Chairman Nye then asked Ms. Wong if she was pleased with the choices for the Chairs.

Ms. Wong replied that she was.

Vice Chairman Chambers concurred, saying he too was pleased.

Chairman Nye thanked the Council for the vote and asked Assistant Secretary Stephan to give his presentation regarding the Hurricane Response.

D. HURRICANE RESPONSE — *Robert B. Stephan,* Assistant Secretary, Office of Infrastructure Protection, DHS

Assistant Secretary Stephan opened his remarks by telling the NIAC he wished to remove the word "interim" from the Interim National Infrastructure Protection Plan, and he needs the Council's help to do this. Assistant Secretary Stephan stated that he will be delivering his team's version of what would be a comprehensive final NIPP to Secretary Chertoff and Deputy Secretary Jackson. Pending the Secretary's agreement, DHS would open up national-level coordination soon after. He said he would need the Council's help in developing this plan. Based upon the Working Group presentations, he found some critical linkages and elements that could factor prominently into that document.

Assistant Secretary Stephan then moved on to address Hurricanes Katrina and Rita. He described the areas affected by the hurricanes as resembling a war zone, likening the hurricanes to a vicious enemy wielding a devastating weapon to destroy the area from Beaumont, Texas to the Alabama-Mississippi border. He recounted his experience in observing extreme devastation in New Orleans and the Biloxi, Mississippi area. Between those locations, there are literally dozens of communities that simply no longer exist. He thought he would be prepared for the situation because of the news reports, but upon landing in New Orleans, he witnessed things that were not shown on the news reports. In a helicopter over the southern part of New Orleans he saw the majority of manmade structures were destroyed or rendered useless. Assistant Secretary Stephan said the destruction was a local and regional problem, but the economic and human impact made it a national problem.

The Assistant Secretary asserted that when he was in an affected area, he saw a great deal of national level solutions being implemented. People, equipment, and supplies from all over the country were being sent to the area to help it recover. The performance by the first responders, organizations delivering food and water, and the pool of law enforcement officers in the region have been integral to the region's recovery effort. Assistant Secretary Stephan said law enforcement officers from the federal and local levels were cooperating with contracted security guards to ensure order was restored.

Hurricanes Katrina and Rita's effect on infrastructure is also of importance to the Council. Some of the physical assets and systems linking service-providing assets were completely devastated. The transportation, telecommunications, chemical, gas, oil, electricity, mail services, banking and finance industries were all affected by the two hurricanes. Hurricanes Katrina and Rita created situations where the private sector and government had to work together. In some instances, the government tried to use the Stafford Act, the legislation enabling federal assistance for affected communities. Enhancements to the Act may be needed to provide the means to help infrastructures critical to restoring public health and safety and maintaining life support for an affected community.

Assistant Secretary Stephan told the NIAC that DHS used the NRP and I-NIPP in a catastrophic scenario for the first time during the hurricanes. He believed, thus far, they have worked well. Using the NRP and I-NIPP for the first time reemphasized the significance of public-private sector

cooperation. Some situations were so isolated that it would have been impossible to get to the area to repair or restore the infrastructure without federal assistance.

The NRP was envisioned as a means to deal with catastrophic scenarios. Assistant Secretary Stephan said DHS has been working hard to do everything it can to identify and assess impacted critical sectors, installations, and services. Once this is complete, DHS will set up processes like credentialing for restoration parties, garnering access permits to certain places, and identifying appropriate security forces using a combination of the National Guard, state and local law enforcement as well as private security guards. The real life situational experience has tremendously improved DHS' ability to locate areas in need of resources. Assistant Secretary Stephan closed by telling the meeting attendees the hurricane catastrophe is not something America can forget because similar situations can happen again and the nation must be prepared.

Chairman Nye asked if the NIAC had any questions for Assistant Secretary Stephan. Chief Gallegos relayed a story of one of his deputy sheriffs describing the nature of the disaster. Chairman Nye commented on how different parts of the infrastructure in the area took many years to create and so much of it is now gone and needs to be reconstructed in a short amount of time.

Assistant Secretary Stephan recalled the pumps used to remove the water from the impacted areas were made in the 1920's. Consequently, when these pumps were damaged, the malfunctioning parts had to be remanufactured because the factories that originally made the pumps no longer exist. He said it will take a great deal of American ingenuity and hard work to get through this national crisis. He thanked the NIAC members for all they have done throughout the crisis.

VIII. ADJOURNMENT NIAC Chairman, *Erle A. Nye*

Chairman Nye thanked Assistant Secretary Stephan for his continued support. He said the meeting went well and the presentations were very informative. Chairman Nye then told the NIAC there is a new meeting schedule. The next meeting is scheduled for February 13, 2006, and it is a teleconference. There will be a meeting on April 11, 2006, in Washington, D.C. The July 11, 2006 meeting will be a teleconference and the October 10, 2006 will be held in Washington, D.C. Chairman Nye said the most integral part of the NIAC is the work they do between the meetings. The Chairman thanked the Council for all their hard work. Chairman Nye thanked the Council again and adjourned the meeting.

By:  Dated: 2/13/06

Erle A. Nye, Chairman

ATTACHMENT A
Sector Partnership Model Implementation

National Infrastructure Advisory Council (NIAC)

Sector Partnership Model Working Group

Initial Report and Findings
October 11, 2005

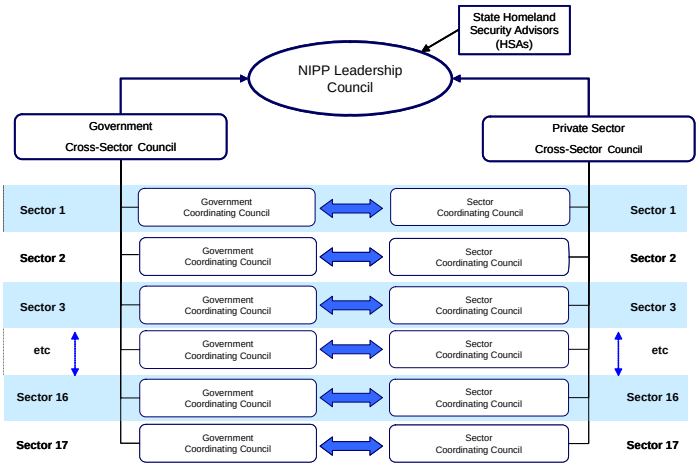
Martin G. McGuinn
Chairman, President & CEO
Mellon Financial Corporation

Marilyn Ware
Chairman Emerita
American Water

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.

Proposed Framework as depicted in the I-NIPP



Core Deliverables

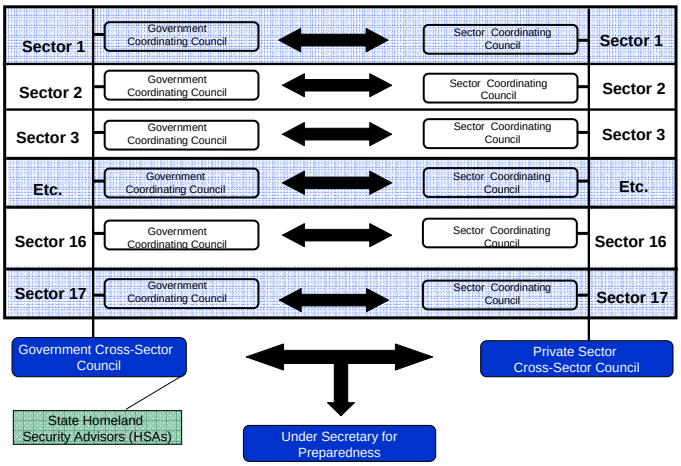
1. **Structure**
   - Review conceptual structure and identify and validate composition and representation
2. **Roles and Responsibilities**
   - SCCs and GCCs
   - "Charter" elements (for overall structure and sub-elements)
     - Purpose / Rules of engagement
3. **Potential Operational Frameworks**
   - 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

Recommendations:

- The conceptual structure of the Sector Partnership Model is acceptable with the following modifications:
  - SCCs and GCCs are the appropriate bodies to comprise the base level of the model.
  - The Partnership for Critical Infrastructure Security (PCIS) should assume the role of the Private Cross-Sector Council.
  - PCIS must have a government counterpart -- the Government Cross-Sector Council consisting of the GCC Chairs.
  - Eliminate the top level of the organization (the NIPP Leadership Council) as it is redundant.
  - The Government Cross-Sector Council must engage the state Homeland Security Advisors in the Model.
  - Remove directional arrows; Arrows give connotation of subordination. SCCs are independent of government. Lines should merely depict information flow.
  - Communication will generally 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.

New Framework with changes



Deliverable #1 –
Validate Composition and Representation

Recommendation:

- DHS should recognize all Sector Coordinating Councils equally, in the manner in which they have chosen to organize themselves.
- SCCs should constitute themselves in a way that provides for appropriate governance and representation for the sector as a whole.

Deliverable #2 –
Roles and Responsibilities

- Roles and Responsibilities of GCCs and SCCs were defined, reviewed and generally accepted.
  - The list is not finite; as CIP evolves so will the functions of coordinating councils
  - Sectors are not identical – all functions may not be applicable to all sectors
- It was determined that some functions of the SCCs and the PCIS could constitute giving advice to the government.

Deliverable #2 – Roles and Responsibilities

Examples of SCC Functions:

- Represent a primary point of entry for government into the sector for addressing the entire range of infrastructure protection activities and issues.
- Serve as a focal point for communication and coordination between owners and operators and suppliers, and with the government during response and recovery.
- Identify, implement and support the information-sharing capabilities and mechanisms that are most appropriate for the sector.
- Facilitate inclusive organization and coordination of the sector's policy development, infrastructure protection planning, and plan implementation activities.
- Advise on integration of State, Local, and Regional Planning initiatives with Federal initiatives, such as the State and Local Role in Sector Specific Plans, the NIPP, and NRP.
- Provide input to the government on research and development efforts.

Deliverable #3 – Potential Operational Framework

- Critical Infrastructure Protection requires continuous and open dialogue among the public and private partners in this Model.
- Such interaction may trigger the Federal Advisory Committee Act (FACA).
- The requirements of the FACA would inhibit the communication, dialogue and advice that must be shared between the GCCs and SCCs and between the PCIS and the Government Cross-Sector Council.
- Section 871 of the Homeland Security Act of 2002 authorizes the establishment of advisory committees as the Secretary may deem necessary and provides that the Secretary may exempt an advisory committee established under this section from FACA.

Deliverable #3 – Potential Operational Framework

Recommendation:

- Consensus agreement was reached that the operational framework for the Sector Partnership Model be based on an unconditional 871 exemption.
- All SCCs and the PCIS should be self-organized, recognized as advisory committees on critical infrastructure protection and response/recovery matters and be exempted from all requirements of FACA:
  - The necessary information sharing and advice from the sectors would otherwise be hampered by legal uncertainty.
  - Protection is needed against the risk of disclosure of critical vulnerabilities.
  - Communication between GCCs and SCCs will need to occur on an ad-hoc basis often at a moment's notice or in response to an emergency.

Deliverable #4 – Key Operating Principles

- A true partnership is a collaboration of equals; all partners bring value.
- SCCs are self-formed entities. The private sector is responsible for and determines group formation, membership, and governance.
- Government communication to the sectors should primarily occur through the established SCCs, supported as necessary by the councils' designated information sharing mechanisms.
  - Exceptions do exist – for example concerning threat based information
- The Sector Specific Agency acts as the lead for coordinating with the sector.
  - Sectors will use the SSA as their government interface. DHS should go through that SSA when interfacing with a sector.
  - Sectors having a DHS office as their Sector Specific Agency will use that DHS office as their government interface.
  - All government agencies should recognize the role of the SSA, and use the SSA as their means to interface with the Sector Coordinating Councils.

Deliverable #4 (cont'd.)– Key Processes and Tools to support the Partnership

- All participants in the Partnership Model must be fully engaged in the development, implementation and continuous improvement of national plans including but not limited to:
  - NIPP
  - SSPs
  - NRP
  - NIMS
- "Disasters happen at a regional level not at a national level."
  - Ensure the Model promulgates the activities down to the regional level.

Deliverable #4 (cont'd.) – Key Processes and Tools to support the Partnership

Recommendation:

- PCII and HSIN-CS are tools that may be used to facilitate information sharing, given the following:
  - The concept of "originator control" must be recognized for all information submitted by the private sector to PCII, allowing the submitter to limit how the information is used.
  - When requesting information, the government must clarify why they need the information and how they will use it.
  - All private sector responses to a government data call should automatically be deemed PCII, when not regulated by law elsewhere.
  - Legal protections must ensure that information voluntarily submitted to PCII will not be used for existing or additional regulation or government mandates.
  - PCII protection must be extended to CIP information voluntarily submitted by industry to agencies other than DHS; time is of the essence when dealing with threat info
  - All information housed on HSIN-CS remains the property of the private sector and cannot be subject to a FOIA request.
  - The HSIN-CS should allow submission of PCII through an automated tool as long as the distinction that it is now PCII is clearly articulated to all users.

Other Recommendations

- The Working Group believes previous NIAC recommendations are relevant to this report as well, for example those delivered on October 14, 2003:
  - Crisis management plans should exist for each sector and be tested. Testing should include validation of cross-sector coordination.
  - Establish a command center that provides a call tree, alerting mechanism, and communication point for use by critical sectors during an emergency.
  - DHS should sponsor crisis management exercises that include the participation of the critical infrastructures.
  - Provide a framework for public and private emergency management interaction including national sector, state, regional and local levels.
  - Explore the potential for creating tax incentives or other instruments to incent the private sector to enhance the resiliency of the critical infrastructures.
  - The national labs should focus their interdependency modeling and research on the regions and sectors whose failure would have the highest impact on the economy and national security.

Summary

- The public/private partnership is vital to the protection of our national critical infrastructure as well as our ability to respond to disasters.
- Ensuring the sovereignty and equality of all stakeholders will maintain a true partnership.
- Hurricanes Katrina and Rita have pointedly demonstrated how critical it is to directly integrate infrastructure providers into the national preparedness and response effort.
  - We must ensure that the partnership is further integrated and embedded into national plans and the framework for engagement be flexible enough to meet tomorrow's challenge's as well as today's.
- It is imperative that:
  - The Partnership Model be implemented immediately and that the HSA Section 871 exemption is granted across the partnership framework.
  - National plans for infrastructure preparedness and response be reviewed to ensure adequate integration of all partnership stakeholders.
  - Information sharing strategies and processes be reviewed to ensure adequate support of both preparedness and response goals.

ATTACHMENT B

Risk Management Approaches to Protection

National Infrastructure Advisory Council (NIAC)

Risk Management Approaches to Protection Working Group

Findings and Recommendations
October 11, 2005

Martha Marsh
President & CEO
Stanford Hospital and Clinics

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

Agenda

- NIAC Question
- Approach
- Findings
- Recommendations

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
- NIAC identified methodological "gaps" for managing risks arising from:
  - Sector interdependencies
  - Catastrophic events
  - Cross-sector technology dependencies (e.g., SCADA)

Approach

- 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
  - Identify recommendations of value for the NIAC working group that will strengthen national risk management practices

Approach (cont'd.)

Contributors to the study group included:

NIAC	Government	Academia	Industry
Finance	Homeland Security	Dartmouth	National Association of Corporate Directors
Technology	Defense	Maryland	North American Electric Reliability Council
Electric and Utilities	Municipal Government (Cobb County)	Stanford	Institute of Internal Auditors
Healthcare			Information Sharing and Analysis Council
Transportation			Partnership for Critical Infrastructure Security
Water			
Defense			
Communications			
Agriculture			
Others			

Risk Management Definition

- Risk management definition
  - A systematic, analytical process to determine the likelihood that a threat or vulnerability will harm an asset or resource and to identify actions that reduce the risk and mitigate the consequences of an event
  - Risk management principles assume that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it
- Historically, the most effective forms of risk management are predicated upon the manipulation of significant, actuarial data
- Multiple forward-looking risk management projections and/or analysis available; some methods yield highly-accurate results
- Catastrophic events and some sector interdependencies present special risk management challenges

Risk Management Methods

- Risk data is generally available in three formats:
  - Statistics (most complete, accurate, and preferred form of data)
  - Models
  - Expert opinions
- In the absence of statistics, modeling and expert opinion historically serve as generally accurate sources of forward-looking risk management mechanisms
- Following slides outline these models, including Bayesian analysis, Stochastic modeling, and Probabilistic Risk Analysis (PRA)

Risk Management Methods (cont'd.)

- **Probabilistic Risk Analysis (PRA)**
  - Relies on Bayesian inference
  - Can be done without heavily populated data stores
- Analyzes system function and failure mechanisms and inputs this data into a systems probability failure formula
- Management capable of identifying technical, human, systematic, or organizations failures that yield risk
- Must overcome basic human tendency to act on complete and perfect information

Risk Management Methods (cont'd.)

- **Stochastic Modeling**
  - Similar to PRA, relies on Bayesian inference
  - Has been used in the past to predict effects of nuclear attack
- Designed to minimize errors of omission and false alerts/false positives
- Designed to acknowledge fundamental assumptions or hypotheses that influence output; provides a contextual risk assessment
- Designed to re-calculate risk assessments as fundamental assumptions change over time
- Heavily weights "expert opinion" as part of assessment

Risk Management Studies

- **1986 Challenger Accident**
  - Investigators concluded that majority of risk management failures were human in nature, not technical
  - Risk mapping analysis
    - Issue: 15% of heat-shield tiles represented 85% of risk; testing done in a random method, consuming time, producing questionable results
    - Resolution: Focused testing on high-risk areas yielded more accurate, risk-weighted, results than previous random testing
  - Human factors analysis
    - Issue: Artificial time constraints and inflexible work structures yielded high-risk workarounds
    - Resolution: Elimination of work structures and flexibility to meet outcomes in a manner consistent with renewed focus on quality, rather than timely, work
    - Issue: Compensation structures for (workers that mapped to high-risk areas) created turn-over and poor quality
    - Resolution: Re-tooled compensation for workers that addressed high-risk of failure components of the orbiter

Risk Management Studies (cont'd.)

- **9-11 Commission Report**
  - Commission identified process, organizational and technical shortfalls
  - Organizational analysis recommended
    - Unify strategic intelligence and operational planning
    - Unify the intelligence community
    - Unify the counterterrorism effort and their knowledge in a network-based information sharing system that transcends traditional governmental boundaries
    - Unify and strengthen congressional oversight to improve quality and accountability
    - Strengthen the FBI and homeland defenders
  - Information sharing analysis
    - "The U.S. government has access to a vast amount of information. But it has a weak system for processing and using what it has. The system of "need to know" should be replaced by a system of 'need to share.'"

Risk Management Studies (cont'd.)

- Studied a number of existing risk management programs or methodologies, including:
- DHS RAMCAP
  - Designed to migrate from intuitive risk assessment to statistical assessment
  - Designed to facilitate comparative risk assessment of assets
  - Three mathematical risk components include consequence, vulnerability and threat
  - Can produce risk assessment by assets, sectors, etc.
- Defense Industrial Base (DCMA) Asset Prioritization Model
  - Efficient ("quick") method to identify and risk-rate assets, determine criticality, and prioritize remediation efforts

Risk Management Studies (cont'd.)

- Studied a number of under-development risk management programs or methodologies, including:
- RAND "Urban Areas Security" Risk Study
  - Includes valuable discussions on uncertainty (expert opinion) and value judgments associated with prioritization
  - Differentiates between risk assessment and resource allocation processes
  - Defines variables associated with consequence-weighting
  - Population-based metrics versus event-based metrics

Commercial Risk Management Attributes

- Example attributes of ***effective*** commercial risk management include:
  - Highly actuarialized data; mature understanding of failure mechanisms and failure indicators
  - Effective use of data; Actionable information; Proximity between actuaries, indicators, and decision-makers
  - Risk management culture across organization; single, senior accountable individual
  - Aligned incentive factors
  - Mechanisms to reduce human error (e.g., training, technology, procedures, etc.)
  - Substantiated business case for risk management investments

Commercial Risk Management Attributes (cont'd.)

- Example attributes of ***ineffective*** commercial risk management include:
  - 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
  - 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
  - Unsubstantiated or poorly developed business case for risk management investments

Findings

- Group identified three high-level findings, including:
  - **FINDING #1:** Robust, standardized ***risk management methodologies***, supported by advanced technologies and infrastructure, maximize the effectiveness of risk management programs
  - **FINDING #2:** ***Risk management leadership***, including implementation of a risk management culture, and a supporting organizational structure enables the standardization of methods, adequate risk management resources, and enhances risk management program effectiveness
  - **FINDING #3:** Independent ***risk management oversight*** enhances strategic direction, focus, and accountability
- Details on each of the findings follow

Findings (cont'd.)

- **FINDING #1:** Robust, standardized risk management methodologies, supported by advanced technologies and infrastructure, maximize the effectiveness of risk management programs
  - **Methodologies:** investments in risk management methodologies (e.g., industry-specific methods such as ISO or COSO, or activity-specific methods such as PRA, Bayesian, etc.) including inter-dependency management, improves standardization of reporting and enhances the effectiveness of data being used for risk management
  - **Technologies:** investments in risk assessment and management, risk modeling, and risk aggregation, analysis, and reporting technologies improves risk management outcomes
  - **Infrastructure:** investments in infrastructure that improves the aggregation, analysis, dissemination, reporting or communication of usable risk information maximizes risk management outcomes

Findings (cont'd.)

- **FINDING #2:** Risk management leadership, including implementation of a risk management culture, and a supporting organizational structure, enables the standardization of methods, adequate risk management resources, and enhances risk management program effectiveness
  - **Leadership:** organizations known for highly effective risk management identify and empower risk management leadership at the senior-most levels
  - **Culture:** organizations that face risk frequently and effectively develop risk management cultures by aligning employee and management incentives with risk mitigation, valuing risk management as a core organizational competency, and ensuring strong risk oversight
  - **Structure:** organizations with significant risk management challenges develop and implement a structure that promotes standardization, disseminates methods, and provides necessary sustainment through supporting training and education programs

Findings (cont'd.)

- **FINDING #3:** Independent risk management oversight enhances strategic direction, focus, and accountability
  - **Strategic direction:** independent risk management input, at the Board of Directors level, enhances the robustness of the risk management program and yields fully-vetted prioritized risk management activities
  - **Focus:** establishing risk management as a core competency of organizational leadership at the senior-most level ensures enterprise-wide focus on risk management programs
  - **Accountability:** independent input and accountability on key risk management functions yields the appropriate level of attention, priority, and outcomes

Recommendations

- The Working Group made three high-level recommendations:
  - **RECOMMENDATION #1:** Create and standardize ***risk management methodologies*** and mechanisms for national planning and programs
  - **RECOMMENDATION #2:** Establish ***risk management leadership*** across the government for homeland security functions
  - **RECOMMENDATION #3:** Establish an independent ***risk management oversight*** function
- Details on recommendations follow

Recommendations (cont'd.)

- **RECOMMENDATION #1:** Create and standardize risk management methodologies and mechanisms for national planning and programs
  - Incorporate methodologies into national risk management system developed and employed successfully by the private sector, adopting "best of breed" for each industry; use forward-looking risk management models
  - Continue to develop mechanisms to identify, acquire, and collect risk management data
    - Continue development of national data warehouse; expand scope and scale
    - Develop incentives to maximize voluntary contributions to data warehouse across all sectors
    - Address barriers to success that minimize participation in current environment, including information sharing protections
  - Continue to develop improved/advanced risk management methodologies
    - Develop and apply more (or more advanced) risk management formularies to data collected

Recommendations (cont'd.)

- **RECOMMENDATION #1 (cont'd):** Create and standardize risk management methodologies and mechanisms for national planning and programs
  - Standardize and disseminate risk management methods across the government (similar to HSPD-7 framework); Develop and implement framework (outlined in Recommendations #2 and #3) to facilitate distribution and use
  - Seek and retain expert opinions in the field of risk management
    - Serve as coordinator for expert opinion in risk management modeling process
    - Create (for government functions) or validate (for private-sector functions) assumptions that represent significant component of risk assessment process
  - Ensure that actionable information is disseminated to all stakeholders
    - Continue to invest in technical infrastructure that will disseminate usable information

Recommendations (cont'd.)

- **RECOMMENDATION #2:** Establish risk management leadership across government for homeland security functions
  - At Risk Management Program Level:
    - DHS should continue to serve as government-wide risk management program lead (e.g. comparable to the corporate Office of the Chief Risk Officer) for Homeland Security matters
    - Define and disseminate standardized risk management methodologies
    - Coordinate government-wide Risk Council
    - Analyze and prioritize threats to the critical infrastructures and establish priorities
    - Function as government-wide Risk Acceptance Authority

Recommendations (cont'd.)

- **RECOMMENDATION #2 (cont'd.):** Establish risk management leadership across government for homeland security functions
  - At Sector-Specific Agency Level:
    - Serve as single, senior focal point for sector specific risk management (similar to corporate business unit Director of Risk Management role); define organizational assumptions; function as the organizational Risk Acceptance Authority
    - Employ standardized risk management methods and infrastructure tailored for the sector to develop mitigation strategy
    - Make risk management recommendations to organizational lead
    - Assume responsibility for risk assessment and management coordination with owner and operator stakeholders

Recommendations (cont'd.)

- **RECOMMENDATION #3**: Establish independent risk management oversight function
  - At Risk Management Program Level:
    - Establish a body responsible for risk management oversight (functions similar to corporate Board of Directors); establish, at the senior-most level, a risk management culture
    - At a strategic level, establish risk management metrics, including incentives and penalties
    - Validate risk assessment and management methodologies
    - Validate decisions (assumptions) of the Risk Acceptance Authorities; validate priorities

Recommendations (cont'd.)

- **RECOMMENDATION #3 (cont'd.):** Establish independent risk management oversight function
  - At Sector-Specific Agency Level:
    - Provide sector specific risk management oversight; ensure compliance with strategic risk management program (functions similar to Board Audit Committee)
    - Validate decisions (assumptions) of the organizational Risk Acceptance Authority; validate priorities
    - At an operational level, establish risk management metrics, including incentives and penalties

Contributors

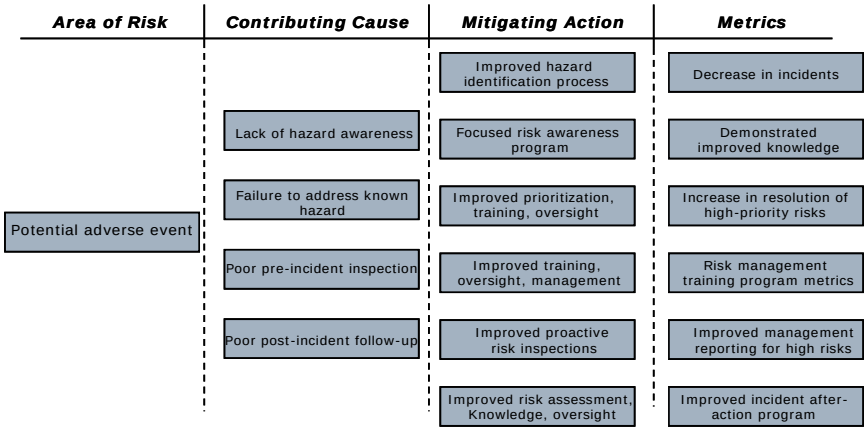
- **Working Group Members:**
- Martha Marsh, President and CEO, Stanford Hospital and Clinics
- Thomas Noonan, Chairman, President and CEO, Internet Security Systems
- Erle Nye, Chairman, Emeritus, TXU Corp., NIAC Chairman
- John T. Chambers, President and CEO, Cisco Systems, Inc., NIAC Vice Chairman
- Alfred Berkeley, Chairman and CEO Pipeline Trading, and former President and Vice Chairman
- of NASDAQ
- Richard K. Davidson, Chairman, President and CEO, Union Pacific Corporation
- Chief Rebecca Denlinger, Fire Chief Cobb County, Georgia
- Martin McGuinn, Chairman and CEO, Mellon Financial Corporation

Contributors (cont'd.)

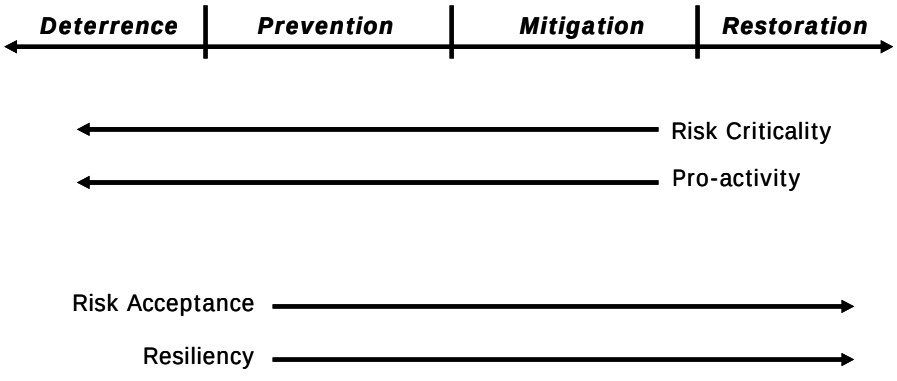
- **Study Group Members:**
- Scott Blanchette, Stanford Hospitals and Clinics
- Peter Allor, Internet Security Systems, Inc.
- William E. Muston, TXU
- Kenneth C. Watson, Cisco Systems, Inc.
- Bill Aimetti, Depository Trust and Clearing Corp.
- Rick Holmes, Union Pacific, Corp.
- Stuart Shannonhouse, Cobb County Georgia
- Susan Vismor, Mellon Financial
- Adam Golodner, Cisco Systems, Inc.
- Lawrence A. Gordon, University of Maryland
- M. Eric Johnson, Dartmouth College
- Stanley Johnson, NERC
- Alexandra R. Lajoux, National Association of Corporate Directors (NACD)
- Charles Le Grand, CHL Global Associates
- E.W. Stowe, PEPCO

- **Additional Study Group Resources:**
- William Flynn, Department of Homeland Security (DHS) Protective Security Division (PSD)
- Gail Kaufman, DHS Infrastructure Coordination Division (ICD)
- Dennis M. McKnight, Defense Contract Management Agency
- Jenny Menna, DHS, ICD
- Keri Nusbaum, DHS, ICD
- Elizabeth Pate-Cornell, Stanford University
- Susan I. Smith, DHS, PSD
- Lawrence M. Stanton, DHS, PSD
- John S. Tritak, CEO of Good Harbor Consulting, LLC.
- Henry H. Willis, RAND Corp
- Nancy J. Wong, DHS, ICD

Example Risk Mapping and Measurement



Risk Management Spectrum



ATTACHMENT C
Intelligence Coordination

National Infrastructure Advisory Council (NIAC)

Intelligence Coordination Working Group

Status Report
October 11, 2005

John Chambers
President & CEO,
Cisco Systems, Inc.

Gilbert Gallegos
Retired Chief of Police
Albuquerque, NM

Overview

- Purpose
- Actions
- Initial Findings
- Next Steps

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 community interaction and optimum contribution to CIP are understood and considered by policymakers

Actions

- Hosted three IC–private sector CIP working sessions with key representatives and working-level staff to analyze and validate requirements and draft findings
- Circulated Issue Papers for comment and initial recommendation ideas for key issues identified in the working sessions
- Analyzing IC and private sector requirements; developing key findings
- Engaging with Law Enforcement to clarify roles and interactions with the private sector for domestic coordination

Discussion

- Questions?

Initial Findings

- National-level fusion center is required to:
  - Gather, analyze, and disseminate information and intelligence relevant to critical infrastructure protection
- Trusted relationships are key to effective critical infrastructure protection
  - Key owners and operators develop relationships with key IC analysts
  - Educate the IC analysts about U.S. critical infrastructures
  - Leverage private sector expertise for better analysis as appropriate
- Need streamlined Request For Information (RFI) mechanism
  - Improve open and timely exchange of information between the IC and the private sector
- Special information protection needs for IC and private sector
  - Need for a common sensitive (unclassified) information protection mechanism across the private sector and IC
  - Need to improve dissemination of classified information

Next Steps

- Review and consolidate comments on Issue Papers
- Map requirements to existing capabilities
- Develop conclusions and recommendations
- Write and review final report

ATTACHMENT D

Workforce, Preparation, Education and Research

National Infrastructure Advisory Council (NIAC)

Workforce Preparation, Education and Research Working Group

Status Report
October 11, 2005

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

Dr. Linwood Rose
President
James Madison University

NIAC Workforce Preparation, Education & Research Update

- Presented initial findings at July 12 NIAC meeting.
- Since then, the Study Group continues to collect data to support those initial findings.
- Additional recommendations will be delivered to NIAC members to review before the end of 2005.
- The NIAC will be able to deliberate for approval during the January 2006 meeting.

Mission

- Determine what can be done to ensure the current and future workforce is able to meet the nation's needs to secure cyber-based critical infrastructures.
- Motivating Themes:
  - Making Math and Science a National Priority
  - Empowering Families
  - Rigorous Research
  - Setting Up Teachers to Succeed

Initial Findings

- The Working Group will develop final recommendations in the following areas:
  - Research and Development Priorities to Improve Cyber Security
  - Efficacy of Cyber Corps
  - Cyber Security Certification Programs
  - K-12 Math and Science Competency

R&D Priorities for Cyber Security

- Develop a national research agenda to prioritize cyber security research efforts.
- Increase the funding base for critical infrastructure protection and cyber security-related research.
- Conduct additional studies to find solutions for reducing "time to market" with respect to cyber security research products.
- Address critical problems by increasing and stabilizing funding for fundamental research in civilian cyber security to attract an adequate talent pool.
- Designate a coordinating body to oversee cyber security research efforts.

Efficacy of Cyber Corps (Scholarship for Service Program)

- Expand internships and employment options to include owner/operators of Critical Infrastructures.
- Re-invigorate the Information Assurance (IA) research community.
- Restructure NSF capacity development concept to encourage, enable and promote the opportunity for faculty to gain actual experience.
- Begin clearance investigations on each SFS student at the start of their last semester.
- Consider alternative funding allocations.
- Allow each SFS student a free billet applicable for any civilian agency.

Cyber Security Certification Programs

- Develop and maintain standardized IA position descriptions, including required and recommended Knowledge, Skills and Abilities for each level/position within all Federal departments and agencies.
- Establish and fund a privately administered, public-private IA training certification body.
- Review and reform IA testing procedures as required, providing outcome-based, modular computer-based testing and metrics whenever possible.

K-12 Math and Science Competency

Recommendations will be presented on:

- Transparency into:
  - Effectiveness of various curricula
  - Effectiveness of various pedagogical approaches
  - State education standards
  - State tests
  - Depth and breadth of US vs. international curricula

K-12 Math and Science Competency (continued)

- Teacher Preparation and Teacher Colleges
- Suggested bodies of knowledge--what students should know at various age levels
- Test and curricula development using mathematicians and scientists, in addition to educators
- Pedagogy development by educators
- Sequencing subjects for best effect
  - "Physics First"

K-12 Math and Science Competency (continued)

- "Drill and Kill" vs. "Discovery"
- Role of automation in education
  - Low Risk Self-Testing
- Unintended consequences of high stakes testing
- Role of vocabulary
- Market segmentation and "tracking"
- Specialization of labor – math specialists and science specialists

Other Areas

- Green Cards for High Achievers
  - Ph.D. candidates from top schools could be given a Green Card upon graduation instead of sending them home to work when their student visas expire.
  - American companies would be able to hire these students immediately.
  - Safeguards can be placed for obvious homeland security reasons.

Summary

- American students are falling behind their international peers in math and science, affecting the nation's ability to produce a quality cyber security workforce.
- Any one of these recommendations will not be a silver bullet to immediately solve all deficiencies, but even small improvements in several areas can make a difference at the national level.

ATTACHMENT E
New Topics

National Infrastructure Advisory Council (NIAC)

New Topics

October 2005

Erle A. Nye
Chairman Emeritus
TXU Corp.

John T. Chambers
Chairman & CEO
Cisco Systems, Inc.

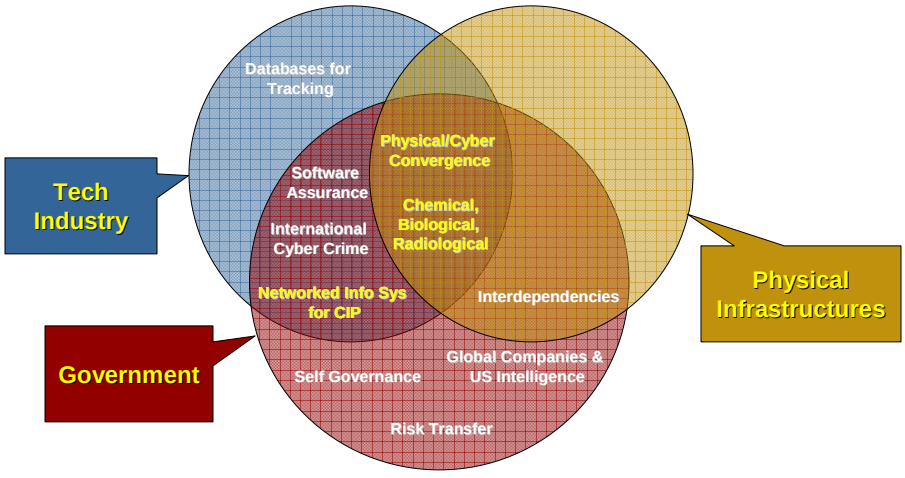
Overview

- Methodology
- Topic overviews
- Recommendations and voting

Methodology

- Solicited inputs from members, DHS, and White House
- Reviewed previous submissions
- Considered ideas from July meeting with President
- Vetted ten topics through members, DHS, and White House for reduction and prioritization
- Narrowed field to seven for presentation today
- Today:
  - Discuss each topic
  - Chairman will ask for votes to prioritize list

Intersecting Relevance



Topic Overviews

- Physical/Cyber Convergence
- Chemical/Biological/Radiological Events
- Technologies for CIP
- Software Assurance
- Interdependencies
- Self-Governance
- Risk Transfer

Physical/Cyber Convergence

- Physical and cyber technologies converging
  - Control systems (SCADA) via internet protocol
- Business case for control system security
  - Profitability vs. perceived risk
- Sufficient research into combined architectures?
  - General business systems w/ control systems
- Managerial & organizational approaches?
- What are appropriate government/industry actions?

Chemical/Biological/Radiological Events (CBR)

- CBR event issues
  - Education for workers, supervisors & families
  - Restoration/repair/recovery critical-infrastructure-worker protection
  - Pandemic preparation/defenses
  - Priorities for vaccines, medical treatment, protective equipment
- Do public health authorities recognize and plan for critical infrastructure workers with respect to CBR events & pandemics?
- Are CI managers adequately prepared in order to continue operations during CBR events & pandemics?

Technologies to Support Critical Infrastructure Protection

- Remote monitoring and sensing capabilities are expanding as costs decrease
  - Video + sensors for intrusion, contact, gases, etc.
  - Increasing awareness through networked systems
- Databases on people are multiple, and emerging techniques allow correlation across databases while protecting personal information.
  - Could be used for terrorist tracking and crime prevention
- As information becomes omnipresent and pervasive, who should have access?
  - Law enforcement?
  - Owners and operators?
  - DHS, FBI, other federal agencies?
- Civil liberty/privacy issues
  - Does the use of such technologies impinge on privacy, or can technology help protect privacy while meeting CIP needs?

Software Assurance

- Maintaining and securing software-driven critical infrastructures increasingly expensive
- Rigorous software design and development processes are in development and use
  - SEI-CMM (Carnegie Mellon)
- Third-party assessments attempt to ensure minimum assurance levels
  - Common Criteria, ICSA, BITS, FIPS 140
- "Guild" approach has been suggested
  - System design, training, apprentice-journeyman-expert framework
- Are special policies and practices needed for software applied to critical infrastructure operations?

Interdependencies

- Interdependencies exist that are not often evident except in times of crisis, and include interdependencies among CI's, and between CI's and law enforcement and local, state and federal governmental organizations
- Local, state and national interdependencies poorly understood
  - Therefore, contingency/business continuity plans incomplete
- Geographical concentrations of critical infrastructures may not be adequately addressed
- Local, state, and regional planning and exercises may not have included adequate critical infrastructure experts in planning phases
- Do existing contingency plans, computer modeling efforts, and exercises require policy changes to adequately address critical infrastructure interdependencies?

Self-Governance

- NIAC addressed considerations for government intervention in markets to achieve protection
- Several sectors have workable self-governance models that simplify government investigation into the need for intervention
  - NERC, INPO, NASD, JCAHO
- Range from sharing best practices through consensus standards to compliance authority with penalties
- Could self-governance models offer value?
  - To industry to aid in CIP organization
  - To government as it considers its role in CIP

Risk Transfer

- Commercial risk transfer mechanisms (eg. insurance) adequate for competitive and market needs
- Terrorism or natural disasters may push risk beyond ability of private system to handle
- Government role (tax incentives, enterprise zones, grants, loans) changes economic calculus
- Does government intervention increase financial stability? Does it improve protection and stability?
- Would the federal government benefit from a decision support process for risk transfer decisions in response to catastrophic natural disasters or terrorist attacks? Would critical infrastructures benefit if the government had such a decision support process?

Voting and Priorities

- Physical/Cyber Convergence
- Chemical/Biological/Radiological Events
- Technologies for CIP
- Software Assurance
- Interdependencies
- Self-Governance
- Risk Transfer