NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING AGENDA

Tuesday, April 12, 2005
1:30-4:30 p.m.
National Press Club
Washington, DC

I.	**OPENING OF MEETING**	*Nancy J. Wong,* U.S. Department of Homeland Security (DHS) / Designated Federal Officer, NIAC
II.	**ROLL CALL OF MEMBERS**	*Nancy J. Wong*
III.	**OPENING REMARKS AND INTRODUCTIONS**	NIAC Chairman, *Erle A. Nye,* Chairman of the Board, TXU Corp. NIAC Vice Chairman, *John T. Chambers,* Chairman and CEO, Cisco Systems, Inc. *Michael Chertoff,* Secretary, DHS *Thomas G. DiNanno,* Acting Assistant Secretary for Infrastructure Protection, DHS *Ken Rapuano*, Deputy Assistant to the President for Homeland Security, Homeland Security Council *Cheryl Peace,* Director, Cyberspace Security, Homeland Security Council
IV.	**APPROVAL OF JANUARY 2005 MINUTES**	NIAC Chairman *Erle A. Nye*
V.	**STATUS REPORTS ON CURRENT WORKING GROUP INITIATIVES**	NIAC Chairman *Erle A. Nye* Presiding
A.	**REPORT ON COMMON VULNERABILITY SCORING SYSTEM (CVSS) PLACEMENT STATUS**	NIAC Vice Chairman *John T. Chambers,* Chairman & CEO, Cisco Systems, Inc. and *John W. Thompson,* Chairman & CEO, Symantec Corporation, NIAC Member

	B. INTELLIGENCE COORDINATION	NIAC Vice Chairman *John T. Chambers,* Chairman & CEO, Cisco Systems, Inc. and Chief *Gilbert Gallegos (retired),* NIAC Member
	C. RISK MANAGEMENT APPROACHES TO PROTECTION	*Thomas E. Noonan,* Chairman, President & CEO, Internet Security Systems, Inc., NIAC Member; *Martha Marsh,* President & CEO, Stanford Hospital and Clinics, NIAC Member
	D. EDUCATION AND WORKFORCE PREPARATION	*Alfred R. Berkeley III,* Pipeline Trading LLC, NIAC Member *Dr. Linwood Rose,* President, James Madison University, NIAC Member
VI.	**NEW BUSINESS**	NIAC Chairman *Erle A. Nye, NIAC Members*
	A. IMPLEMENTATION OF THE SECTOR PARTNERSHIP MODEL	*Martin G. McGuinn,* Chairman and CEO, Mellon Financial Corporation, Working Group Chair
VII.	**ADJOURNMENT**	NIAC Chairman *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Chairman Nye, Mr. Peters, Mr. Rohde, and Dr. Rose

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Vice Chairman Chambers, Mr. Barrett, Mr. Berkeley, Mr. Conrades, Mr. Davidson, Chief Denlinger, Lt. Gen. Edmonds, Chief Gallegos, Ms. Marsh, Mr. McGuinn, Mr. Noonan, Mr. Thompson, and Dr. Rose

MEMBERS ABSENT:
Mr. Carty, Governor Ehrlich, Mr. Hernandez, Ms. Katen, Commissioner Kelly, Mr. Martinez, Mayor Santini-Padilla, and Ms. Ware

STAFF DESIGNEES PRESENT MONITORING PROCEEDINGS:
Mr. Muston (for Chairman Nye), Mr. Larson (for Ms. Ware), Mr. Schrader (for Governor Ehrlich), Mr. Holmes (for Mr. Davidson), Ms. Miller (for Ms. Grayson)

STAFF DESIGNEES MONITORING PROCEEDINGS VIA CONFERENCE CALL:
Mr. Watson (for Vice Chairman Chambers), Mr. Allor (for Mr. Noonan), Sgt. Mauro (for Commissioner Kelly), Ms. Vismor (for Mr. McGuinn), and Mr. White (for Ms. Katen)

OTHER DIGNITARIES PRESENT:
U.S. Government: Michael Chertoff, Secretary of the Department of Homeland Security, Mr. Ken Rapuano, Deputy Assistant to the President for Homeland Security, Homeland Security Council, Mr. Thomas G. DiNanno, Acting Assistant Secretary for Infrastructure Protection, Ms. Cheryl Peace, Director of Cyberspace Security for the Office of the Special Assistant to the President for Critical Infrastructure Protection and the Homeland Security Council, Mr. R. James Caverly, Director, Infrastructure Coordination Division (ICD) of the Department of Homeland Security, and Ms. Nancy J. Wong, Infrastructure Programs Office and Designated Federal Official (DFO) for the NIAC.

I. OPENING OF MEETING

Ms. Nancy Wong introduced herself as the Designated Federal Official for the National Infrastructure Advisory Council (NIAC) from the Information Analysis and Infrastructure Protection (IAIP) Directorate of the Department of Homeland Security (DHS). She welcomed Secretary Michael Chertoff, Mr. Rapuano, Ms. Peace, Acting Assistant Secretary DiNanno, and other officials from DHS, Chairman Erle A. Nye, Vice Chairman John T. Chambers, all Council members, and their staffs present and on the teleconference, and the many Federal Government representatives who were present. She also extended a welcome on behalf of the Department to the members of the press and public attending. Ms. Wong reminded the members present and on the teleconference line that the meeting was open to the public and, accordingly, to exercise care when discussing potentially sensitive information. Pursuant to her authority as Designated Federal Official, she called to order the eleventh meeting of the National Infrastructure Advisory Council and the second meeting of the year 2005. Ms. Wong then proceeded to call roll.

II. ROLL CALL

Ms. Wong reminded members and their staffs of conflict of interest regulations and the Federal Advisory Committee Act (FACA) with regard to the conduct of this meeting. All discussion and deliberations in Council meetings are solely the role and responsibility of Council members. However, any member may call upon a staff member for information during a meeting.

She said the NIAC has a well-deserved reputation for its productivity and the quality of its work products. DHS appreciates the commitment, energy, and intellectual contributions of all members and their supporting staffs and extends its deepest thanks.

III. OPENING REMARKS AND INTRODUCTIONS

NIAC Chairman, *Erle A. Nye,* Chairman of the Board, TXU Corp.

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

Michael Chertoff, Secretary, Department of Homeland Security

Thomas G. DiNanno, Acting Assistant Secretary for Infrastructure Protection, DHS

Ken Rapuano, Deputy Assistant to the President for Homeland Security, Homeland Security Council

Cheryl Peace, Director, Cyberspace Security, Office of the Special Assistant to the President for Critical Infrastructure Protection, Homeland Security Council

Chairman Nye thanked Ms. Wong and everyone in attendance. Chairman Nye welcomed the new Secretary of Homeland Security, Michael Chertoff, and thanked him for joining the meeting. He said that he and the Council had followed Secretary Chertoff's rapid ascent to this new role and admired the way in which he had began his term. Secretary Chertoff has many years of experience as a lawyer and served as the US Attorney in New Jersey for a number of years where he had a distinguished record of service. Additionally, he was appointed to the Third Circuit Court of

Appeals where he also developed a great reputation. The Chairman then asked Secretary Chertoff if he had any comments.

Secretary Chertoff thanked Chairman Nye and stated that he had heard wonderful things about the NIAC and its leadership. The Secretary also thanked the members for their outstanding service to the Council. He said that in the short time he had been Secretary, he had witnessed evidence of the Council's highly valuable role and the great job it had done since its inception. He continued, noting how the NIAC had done a tremendous job sharing keen insights and recommendations within the Department and with the government as a whole.

Secretary Chertoff said that like most departments, a large portion of DHS' activities are dictated by the equipment it owns, the people working with the Department, or the operations it undertakes itself. But there is another, perhaps less widely appreciated part of the Department, networking. Much of this networking takes place with state and local partners and with the private sector. DHS has a nationwide reach as it applies to thousands of institutions, physical facilities, and cyber-facilities. These different pieces are all bound together, not by common ownership or workforce, but by a common network. It is important for DHS to focus on that networking function in addition to the more traditional physical attributes of the Department's responsibilities.

The NIAC is a pivotal part of this effort. This Council assists DHS by applying its expert advice and perspective. The Secretary said in addition to the status reports of the Intelligence Coordination and Risk Management Approaches to Protection Working Groups, the NIAC will be launching further initiatives about which he looks forward to hearing.

Secretary Chertoff said the Council's Charter is up for revision to slightly expand and broaden the scope of its work. He asserted this is a tribute to the high quality work the Council has produced and the meaningful impact it has had. He said DHS is considering broadening the Council's perspective and range of operations. He concluded his remarks by reiterating that he looked forward to hearing the Council's discussion. He thanked Chairman Nye for the opportunity to address the Council.

Chairman Nye thanked the Secretary and said he was encouraged by his comments on the pending revision of the NIAC Charter. He said it was important for the Council to lend its expertise to the physical side of infrastructure protection as well as to cyber security. The NIAC looks forward to guidance on this issue. With regard to this meeting of the Council, the Chairman said there were four Working Group status reports as well as Mr. McGuinn's presentation on the Sector Partnership Model Working Group (SPMWG). He then asked if Vice Chairman John Chambers had any further comments.

Vice Chairman Chambers joined Chairman Nye in welcoming Secretary Chertoff to his first NIAC Meeting. He extended an offer to every NIAC member to help the Secretary learn about all of the Council's roles. The Vice Chairman anticipated working with Secretary Chertoff and said he hoped the Council meets and exceeds its goals. Like Secretary Chertoff said in his opening remarks, the NIAC has been very effective, and Vice Chairman Chambers said the key reason is strong CEO and staff participation. He asked the Secretary to provide candid and open feedback on areas the Council might better serve the needs of DHS. He thanked the Council and all those in attendance and returned the floor to Chairman Nye.

Chairman Nye then introduced the Acting Assistant Secretary for Infrastructure Protection, Tom DiNanno.

Acting Assistant Secretary DiNanno thanked Chairman Nye and said he was thrilled to attend the meeting with Secretary Chertoff and the Deputy Assistant to the President for Homeland Security Ken Rapuano to show the administration's commitment to these important issues. Intelligence Coordination is a cornerstone of many DHS programs and also crucial to the success of many of its customers. By coordinating intelligence, DHS can help map threats to owners and operators as well as the consequences of an incident. He thanked Chairman Nye again.

Chairman Nye thanked the Acting Assistant Secretary and introduced Ken Rapuano, Deputy Assistant to the President for Homeland Security. He asked Mr. Rapuano if he had anything to add.

Mr. Rapuano welcomed Secretary Chertoff to the meeting and said the Council was composed of a truly impressive cast of members. He said the President and Homeland Security Advisor Frances Fragos Townsend are confident that the Secretary's leadership will help carry on the Council's exceptional work. He also noted that Chairman Nye and Vice Chairman Chambers' excellent leadership has greatly contributed to the Council's effectiveness. He thanked all the NIAC Members on behalf of the White House as the administration continues its efforts to secure the homeland.

He said that an important statistic to keep in mind is that 85 percent of national infrastructure is operated or owned by the private sector. This fact makes it all the more important to provide a framework for the public-private partnership. The Council is a key part of this partnership. In national strategy and critical infrastructure and key assets, the President has emphasized reducing the terrorist threat through this partnership. Mr. Rapuano said it is important to identify the most critical infrastructure and assets, provide warnings of vulnerabilities and threats, and to develop necessary procedures for critical infrastructure protection nationwide. Mr. Rapuano said the White House was especially interested in the Common Vulnerability Scoring System (CVSS). Ms. Peace said the report was an excellent product and that she will be working very closely with DHS to develop a plan for encouraging other federal agencies to assess the tool for implementation within their own agencies.

Another major issue is the rapid deployment of telecommunications security. This is a significant challenge due to the technological trends of both offensive and defensive capabilities. He said that there is the legitimate concern the pace of growth might exceed security procedures. The White House looks to both the NIAC and the National Security Telecommunications Advisory Council (NSTAC) to analyze and consider these threats and polices for the President. Mr. Rapuano concluded his comments.

Chairman Nye thanked Mr. Rapuano and asked Ms. Cheryl Peace if she had any further comments to add on behalf of the White House.

Ms. Peace said she had no further remarks.

Chairman Nye reminded the Council that during the January meeting, Mr. R. James Caverly discussed the Sector Partnership Model which was later published in the Interim National Infrastructure Protection Plan. He reminded the members that this is an extremely important initiative for the United States Government. It is a mechanism that is intended to allow the government and critical infrastructure sectors to better coordinate critical infrastructure protection activities and to provide the sectors a better means to interact with relevant government agencies. Chairman Nye said he thought the framework in the model was sound. Chairman Nye noted that this model was discussed at the January 11, 2005 meeting and that the discussion is reflected in the minutes. While the Council did not take any action at that time, the NIAC is in the process of organizing actions to work with the Sector Partnership Model.

Chairman Nye stated the next agenda item was the approval of the January 11, 2005 Minutes.

IV. APPROVAL OF JANUARY 11, 2005 MINUTES

NIAC Chairman, *Erle A. Nye*

Chairman Nye opened the meeting up to a discussion of the January 11, 2005 minutes. He recommended the minutes be changed to reflect a correct account of his description of then Secretary-designate, Michael Chertoff. The minutes read that during his tenure at the Department of Justice, Secretary Chertoff supervised 800 people. The draft of these minutes erroneously reads that he supervised 800 as a Judge on the Third Circuit Court of Appeals.

He asked if there was a motion to vote on the approval of these draft minutes with the changes incorporated.

Mr. Berkeley motioned for a vote and the minutes were approved unanimously.

Chairman Nye thanked the Council and called on Vice Chairman Chambers and Mr. John Thompson to present the Report on the placement of the Common Vulnerability Scoring System (CVSS).

V. STATUS REPORT ON CURRENT INITIATIVES

A. REPORT ON COMMON VULNERABILITY SCORING SYSTEM (CVSS) PLACEMENT

NIAC Vice Chairman *John T. Chambers,* Chairman & CEO, Cisco Systems, Inc. and *Mr. John W. Thompson,* Chairman & CEO, Symantec Corporation, NIAC Member

Vice Chairman Chambers thanked Chairman Nye for his introduction and said that he and Mr. Thompson were pleased to lead the discussion on finding a permanent home for the CVSS. He said the Working Group had received proposals from the global Forum of Incident Response and Security Teams (FIRST) Organization, MITRE, and the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie-Mellon University. The Working Group has advanced the idea of replacing a formal recommendation with a strong suggestion.

Vice Chairman Chambers asserted that the US Government should not decide on or officially recommend a permanent location for the CVSS because the system is open and global.
In order to achieve the goal of a single worldwide common scoring system, all three organizations need to cooperate with a single vision and under a single umbrella. All three entities are necessary to the process. MITRE and CERT/CC both bring distinct but important value. Based on those proposals, the Working Group strongly suggests that these organizations work under the umbrella provided by Global FIRST for the CVSS. Vice Chairman Chambers asked Mr. Thompson for any additional comments.

Mr. Thompson thanked Vice Chairman Chambers and said that the Vice Chairman had covered it all. He continued that it is clear that Global FIRST's cyber incident coordination scope positions them well to be a key interaction point. It is also clear both MITRE and CERT/CC have incredible competencies that may be leveraged for the betterment of CVSS.

Vice Chairman Chambers said the Working Group wanted to thank FIRST, MITRE and CERT/CC for their interest in CVSS and look forward to seeing the methodologies being broadly used and improved worldwide by the combined efforts of those organizations as they work under the coordination provided by the FIRST Organization.

Chairman Nye reminded the Council that this report has in fact been submitted to the White House, but because it is a living document, the methodology still needs a home. Vice Chairman Chambers made a strong point that it is not appropriate for the Council or for the government to select a host but to work with any entity who has expressed a willingness to step forward. His hope was that the companies providing input to this system would help make it become a reality by user choice as opposed to a NIAC or government designation.

Vice Chairman Chambers said the Chairman articulated this point very well.

Chairman Nye asked if there were any questions for Vice Chairman Chambers or Mr. Thompson. There were none and the Chairman thanked Vice Chairman Chambers and Mr. Thompson for their presentation.

Chairman Nye said the Council had an active agenda and has another presentation from Vice Chairman Chambers, who co-chairs the Intelligence Process and Work Products Working Group with Chief Gallegos. He turned the floor to Chief Gallegos and Vice Chairman Chambers.

B. INTELLIGENCE PROCESS AND WORK PRODUCTS REGARDING CRITICAL INFRASTRUCTURES	NIAC Vice Chairman *John T. Chambers,* Chairman & CEO, Cisco Systems, Inc. and *Chief Gilbert Gallegos (retired),* NIAC Member

Vice Chairman Chambers thanked Chairman Nye and the Intelligence Coordination Working Group. He said that the Council recognizes the need to develop efforts to establish a closer connection between critical infrastructure industries and Intelligence Communities. He said it is important to educate one another. It is especially important for the Intelligence Community to understand critical infrastructure protection needs articulated by the private sector and to help prioritize these issues. The Vice Chairman said that another key goal is to use industry connections to assist in the constructive dissemination of intelligence products. Vice Chairman Chambers then invited two Study Group members, Mr. Ken Watson and Mr. John MacGaffin, to add their perspectives to the status report.

Mr. Watson thanked the Vice Chairman and said he was going to provide the Council with a short status report to review the Study Group's progress. This status report will cover the Study Group's accomplishments over the last quarter, its plans for the next quarter, and to provide some information on the overall timeline.

Mr. Watson said over the last quarter the Study Group refined its purpose and clarified its focus. Mr. MacGaffin has been meeting with senior intelligence community officials and initial reports suggest enthusiastic responses from the intelligence community. He said that they are excited about the prospect of cooperating with the NIAC to develop this required architecture. Mr. Watson added that the timing is appropriate with the introduction of intelligence reform law and the push to integrate intelligence efforts. He then turned the floor to Mr. MacGaffin.

Mr. MacGaffin thanked Mr. Watson and said he wanted to make some quick observations on the refinements the Study Group has made thus far. The first step the Study Group made was to analyze both the intelligence and law enforcement communities. For purposes of this study, the Study Group has decided to consider law enforcement within intelligence for the initial stages, realizing eventually these two types of organizations will likely need to be considered separately again later. As the Study Group moves forward it is essential to remember that when the group speaks about the intelligence community, it is understood that they are including law enforcement partners.

The second clarification is around terminology regarding the private sector. Early on, the Study Group defined the private-sector participants as the "critical infrastructure protection" community. This could be confusing to the intelligence community, since that community is well-defined and has prescribed members and architectures. Since there is no parallel construct in the private sector, the Study Group has elected to simply call that group of participants "the private sector".

He continued, noting the fact the Study Group has emphasized the point that it is working toward reciprocal understanding, bringing the intelligence community to the point where it understands the domain expertise and other attributes of the private sector, and vice versa.

Mr. Watson noted that the efforts of the Study Group can be folded down back to the original two questions the Council asked:

- In what ways can the intelligence community help the private sector?
- In what ways can the private sector help the intelligence community?

Each side of this partnership has core competencies that are valuable to the other if the overall mission is protecting the country. Mr. Watson turned the presentation back to Mr. MacGaffin.

Mr. MacGaffin said that it was important to remember that the intelligence community and private sector must complete separate yet parallel operations before the Council can bring the two together to move ahead further. The next task is to establish how the Study Group will pursue using the National Infrastructure Protection Plan (NIPP) and the National Response Plan (NRP) together to provide the framework for moving forward. This will address the seven elements of infrastructure risk management:

- Detection
- Deterrence
- Prevention
- Protection
- Preparedness
- Crisis Management and Response
- Recovery
- Restoration

Mr. MacGaffin said that these seven pillars provide the framework within which the Study Group will analyze information flows and gaps between the private sector and the intelligence community. He described a scenario that uses a complex matrix to address an issue within the transportation sector. Within this matrix, he stressed that the key data gathering points hinged around the information requirements of the private sector applicable to deterrence, prevention, protection, etc.

Using the transportation sector as an example, he stated that the intelligence community could use this approach to fulfill its critical infrastructure protection responsibilities as well as the characteristics of the information they require. By pulling together these different pieces, the Study Group can better understand the current battlefield and what needs to be done to maximize critical infrastructure protection. Mr. MacGaffin said that the final objective is to evaluate where critical infrastructure protection can be optimized across both the Private Sector and the Intelligence Community.

Chairman Nye asked Mr. MacGaffin if he could interrupt to ask a question.

The Chairman said that as one analyzes the nature of information flows it seems almost apparent that the flows as they currently exist are probably not optimal. He asked if this was a fair assessment.

Mr. MacGaffin said that the flows are not currently optimal but the definition of what exactly is optimal needs to be determined. This is something the Study Group will have to assess.

Chairman Nye thanked Mr. MacGaffin for his clarification.

Mr. MacGaffin then addressed the Study Group's completed actions. He said that the Council has received some of the research and analysis also provided to the Study Group as well as information on work done in the intelligence community. The Study Group owes an analysis of the Weapons of Mass Destruction Commission and will provide this shortly. The Commission sets an environment conducive to the things the Council is trying to do. It discusses information sharing in great detail, refers to new approaches, and highlights the problems of stovepipes.

He continued by saying that as the administration incorporates previous legislation and the 9/11 Commission Report, it also becomes more relevant to the Study Group's work. The next completed action deals with contacts the Study Group has made thus far. The Study Group has been in contact with the Central Intelligence Agency (CIA) in some extended detail. Current contact with the CIA has been on an individual basis, with the expectation evolving to a larger setting. In addition to the problems of time, the connectivity between the classified and unclassified worlds can be problematic. The Study Group is working to ensure that these discussions remain unclassified. It has also prepared a briefing to address senior staff members from both the private sector and the intelligence community. Mr. MacGaffin then returned the briefing to Mr. Watson.

Mr. Watson thanked Mr. MacGaffin and said that in addition to briefings and participation by the intelligence community, law enforcement and private sector, the Study Group will conduct detailed analysis of the information requirements and flows using the NIPP framework. The Study Group expects to conclude this analysis around July.

Over the subsequent quarter, the Study Group plans meetings with intelligence community and private sector staffs to begin comparing requirements and analyzing information architectures. The group hopes to finish within the original timeframe of finishing the report by the October 2005 NIAC Meeting. Mr. Watson concluded the presentation and returned the floor to Vice Chairman Chambers.

Vice Chairman Chambers thanked Mr. Watson and Mr. MacGaffin and asked Chief Gallegos if he had any further comments.

Chief Gallegos also thanked Mr. Watson and Mr. MacGaffin for an outstanding job of presenting the progress thus far. Chief Gallegos said that he had contacted the Los Angeles Police Department (LAPD) which is redeveloping written protocols on intelligence and how it processes information in cooperation with the private sector. He said he had talked to Captain Williams about this and he said that he would provide this information to the Working Group as soon as it is developed.

Vice Chairman Chambers thanked Chief Gallegos and asked if there were any questions from the Council or from any government representatives.

Chairman Nye said that he had monitored this Working Group and had been very impressed with its dialogue and activity. He stated that the Working Group is certainly headed in the right direction. He asserted that he did not want his question to imply any dissatisfaction because there is none, but asked if it would be helpful to have additional Council members.

Vice Chairman Chambers said this would certainly help.

Chairman Nye said he was very pleased with the direction and quality of the Working Group. He encouraged members to join in as there is still much that needs to be done.

Vice Chairman Chambers agreed and said he would very much like to see a talented new Council member, Mr. Greg Peters, become a member of the Working Group. He also said the Working Group would welcome any other volunteers.

Mr. Peters thanked Vice Chairman Chambers and said he would be pleased to join.

Chairman Nye thanked Mr. Peters and said this Working Group is a very active one. He again thanked Vice Chairman Chambers and Chief Gallegos and said if there were no further questions he would turn the floor to Mr. Tom Noonan and Ms. Martha Marsh for their presentation on the Risk Management Approaches to Protection Working Group.

C. RISK MANAGEMENT APPROACHES TO PROTECTION

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

Ms. Marsh thanked Chairman Nye for the opportunity to provide an update on the efforts of the Risk Management Working Group and said that Mr. Noonan was unfortunately not able to attend. She said that this Working Group had been active for six months and enjoys broad representation across the NIAC, as well as private sector critical infrastructure players. She said that her assistant, Mr. Scott Blanchette, Director of Information Technology and Chief Information Security Officer at the Stanford Hospital and Clinics would walk the Council through the presentation.

Mr. Blanchette thanked Chairman Nye, the Council, and Ms. Marsh. He also said that he wanted to thank Mr. Peter Allor for his efforts with the Study Group. He began by saying that the identification of the private sector risk management experience is key to strengthening federal efforts to protect national critical infrastructure. He said although private and public sectors seek similar outcomes, the manner in which each entity assesses, manages, and accepts risk is different.

Accordingly, the Council created a Working Group and Study Group to explore the varying risk management philosophies, methodologies, and outcomes used by the private sector to gauge the potential for their inclusion in government infrastructure protection programs. The Study Group continues to believe that the Council's broad representation of industries relying upon formalized, scientific, and time-tested risk management methodologies will yield a successful outcome.

Mr. Blanchette stated that the Study Group will provide an update on the progress of the Working Group, will spend some time discussing attributes of mature risk management, and will update the Council on the Study Group's current status in terms of outcomes and objectives.

Mr. Blanchette said that the Study Group spent a considerable amount of time defining risk management attributes, ultimately establishing three fundamental risk management drivers:

- Probability: the likelihood of an adverse event
- Impact: the potential outcome of an adverse event
- Efficiency: the cost-effective allocation of risk management resources to avoid an adverse event

In many industries, the manner in which the private sector balances these three components often defines a firm's competitive advantage.

Mr. Blanchette asserted that considering industry's focus on cost efficiency and effectiveness, failure to manage this balance can mean a critical and even fatal outcome for private sector management. For example, failing to manage risks in a just-in-time supply chain might cripple business operations. On the other hand, expending excessive resources on supply chain risk management may squander profits and reduce corporate value. These two outcomes are both undesirable and either scenario may prove to be fatal for a growing concern.

Mr. Blanchette said that effective risk management is not solely a fiscal exercise. The Study Group is engaged in the study of risk across many industries. There are both mature and immature risk management models. Specific attributes that define mature risk management models include:

- Free markets and competitiveness
- Legal precedents
- Significant actuarial data
- A mature understanding of failure mechanisms; and
- Proximity between risk assessors and management

While mature risk management models tend to incorporate many, if not all, of the previously identified attributes, immature models tend to possess few, or none, of these.

Mr. Blanchette continued by saying the Study Group covers a significant spectrum of critical infrastructure and continues to identify industry-specific examples of both mature and immature risk management practices.

He said that the insurance industry possesses many attributes of risk management maturity. Risk decisions are based upon substantial actuarial data and there are legal precedents to guide risk management decisions. For example, free markets will guide consumer decisions away from companies that over-subscribe to risk management; this means they over-allocate capital damaging their competitive advantage. Free markets also guide consumers away from firms failing to adequately manage their risk, potentially leaving customers uncovered or dissatisfied. There is a generally recognized understanding of failure mechanisms and a high degree of proximity between those who assess risk and senior management. Across all industries, the Study Group continues to identify areas of maturity and immaturity.

Mr. Blanchette said that the field of maturing or emerging risk management is an area of interest for the Study Group is the field of maturing or emerging risk management. Some risk management activities that have historically been poorly predictive are maturing more with time. An example of this is information technologies. Historically, this area has been difficult for the average company to effectively manage risk and has been somewhat prone to failure. However, as technologies continue to mature, data points become more available, and information technology managers play greater roles within the company, and have a greater understanding of failure mechanisms are developed. With this, IT risk management continues to migrate from an immature model to a mature model.

Mr. Blanchette said that the Study Group is optimistic it can provide value as the public sector continues to undergo a risk management transformation.

For nearly half a century, the Federal Government focused its resources on defending the nation from risks inherent in a bilateral world. This historical risk management model focused on the low-probability, high-impact clash between the United States and the Soviet Union. Today, the Federal Government continues to make the risk management transition to a world that presents higher probability threats. This transition brings into very specific relief the challenges the Federal Government will continue to face as it tries to reduce this distributed risk.

Although the challenges the private sector faces pale in comparison to the magnitude of the national security challenge, the dispersion of threats in an ever-changing environment is one in which the private sector can identify and hopefully contribute value to federal risk management efforts. Effective risk management, efficient allocation of resources, and a focus on value, all tenets of the private sector risk management model, will become core components of federal practice over time.

In the near term, the Study Group will complete the identification of risk management attributes, methods, and outcomes used by the private sector and make helpful recommendations to strengthen public sector risk management efforts. With the recent addition of Chief Denlinger to the Working Group, there is now a vetting resource within the Working Group to ensure recommendations would have a high probability of adoption by the Federal Government. In addition, the Study Group has recently been approached by DHS to receive a brief on the DHS Federal Risk Management Study. Allowing the Study Group to review and understand this study will significantly strengthen the quality of the deliverable and ensures the Study Group has a complete understanding of the current state of federal risk management efforts.

Mr. Blanchette said the Working Group and its Study Group look forward to socializing its findings and recommendations prior to the next meeting as well as soliciting feedback from NIAC members on the appropriateness, completeness, and value of the groups' efforts.

Mr. Blanchette thanked Chairman Nye for the opportunity to provide this update and asked if there were any questions before he returned the presentation to Ms. Marsh.

Ms. Marsh asked if Mr. Allor had anything further to add.

Mr. Allor said that the Study Group is also looking at risk management methodologies from the Department of Defense in addition to DHS.

Ms. Marsh thanked him and asked if there were any questions from the Council.

Chairman Nye asked if the Working Group needed any additional members.

Ms. Marsh said that additional members are always appreciated but the broader spectrum for input from people makes for a better product. She said she thought the Working Group was strong as it was currently composed. She said she and Mr. Noonan would always welcome new members but is fine as it is.

Chairman Nye thanked Ms. Marsh and moved the meeting to the Working Group working on Assuring Adequate National Intellectual Capital to Secure Cyber-Based Critical Infrastructures.

D. ASSURING ADEQUATE NATIONAL INTELLECTUAL CAPITAL TO SECURE CYBER- BASED CRITICAL INFRASTRUCTURES

Alfred R. Berkeley III, Pipeline Trading LLC, NIAC Member and *Dr. Linwood Rose,* President, James Madison University, NIAC Member

Mr. Berkeley thanked Chairman Nye and noted that this Working Group has divided its work into an Education Study Group and a Research Study Group. He said that he would begin by discussing the Education Study Group and turn the floor to Dr. Rose for the Research Study Group. The first task addresses issues specific to cyber security. The second addresses the broader issue of math and science competency in K-12 students as well as the competitiveness of the American education system. While this task might initially appear broad and consisting of amorphous topics, the Study Group is actually developing very specific and actionable recommendations. The third task relates to the timeliness of security clearances; there are many other groups working on this and the Study Group intends to build on the work done before.

The Study Group holds a weekly conference call that includes anyone who wishes to join. During these conference calls, an expert addresses the Study Group on a particular topic area.

Mr. Berkeley provided the Council with a couple of examples of how the United Kingdom is finding success in adding a national curriculum for mathematics. Initially, the UK and the US shared many of the same problems. The UK's curriculum is relatively new but is still generating good results. The Study Group had Mr. Don Hirsh, an American educator, discuss his strategies on core knowledge as well as the advantages and disadvantages of standardized curricula in various fields.

Mr. John Yokleson, President of Building Engineering Science Talent, also talked to the Study Group to identify what has proven successful in keeping students in math and sciences in the US. Currently, there is very little in the core curriculum that promotes math and science. Most of the successful programs boast things such as after school programs or charismatic teachers. The Study Group will continue its discussions with the Department of Education to understand what has already been done.

At this point, Mr. Berkeley turned the discussion toward education on cyber security. While this was a small part of the total issue, the Study Group found that there are not many students who are interested in cyber security courses. Additionally computer science enrollment has generally declined, particularly in universities. This is a limiting factor as there are not many places actually teaching cyber security. Most cyber security education is vendor-specific and less broad based. The Study Group has talked to SUNY-Buffalo, one of the more active cyber security learning centers, about the student involvement life cycle. One of the main deterrents to a cyber security program is that students often have problems finding jobs once they finish a cyber curriculum.

Mr. Berkeley stated that the Study Group will have to make some recommendations about defining what kinds of jobs are acceptable. The Study Group illustrates this through what they refer to as the billet issue. Currently, some of the programs require students to get jobs in the Federal Government. This is a problem because the Federal Government actually outsources most positions to contractors. A specific recommendation will most likely involve the concept of allowing students to complete these courses on scholarship to take a job with a contractor working for the Federal Government.

Mr. Berkeley said that there is also a clear need for more Ph.D.s in the university community, especially those with a theoretical basis of cyber security knowledge. One limitation is that there are a number of different efforts by different federal agencies that are somewhat uncoordinated. The Study Group will probably return a recommendation about having information available on all of these programs.

He continued by saying that the Study Group has discovered that a very small number of people have received scholarships in cyber security, just 540 students over the last four years. Mr. Berkeley noted that the certification program issue is also very interesting to the Study Group. The individual or individuals that certify cyber education must obviously have a certain degree of qualification. The key question to consider who in the Federal Government or in business honors these certifications. He added that the Study Group will pursue this but the fact remains the government does not want to be, nor should be, in the certification business. Despite this barrier, there is the need for buy-in from various federal agencies to give momentum to the certification processes currently underway.

Mr. Berkeley moved on to discuss security clearances. He stated it was a complicated issue and the Study Group had done some work in identifying potential advisers but had yet to begin any actual work on this piece. He asked the Council if there were any questions on his presentation. There were none and he turned the floor over to Dr. Linwood Rose.

Dr. Rose thanked Mr. Berkeley and began to address four key areas as they pertain to research:

- The Study Group recognizes the need for a national cyber security research agenda
- Whether the funding dedicated to research is sufficient
- The possibility for recommendations to speed up the transfer of new technologies and products from the research phase through production
- Whether the US has a sufficient research talent pool

Upon initial investigation of these topics, the Working Group discovered that several groups have also undertaken similar inquiries. Rather than conduct another study and again request expert consultants be called, the Working Group will take advantage of some of the previous work. The Working Group will track the work that is underway, seeking to understand the findings and recommendations of those bodies. The Working Group ultimately wants to test the findings with appropriate audiences and determine if its Study Group and ultimately the Council might support and encourage the implementation of those recommendations.

Dr. Rose said there are two such studies apparently paralleling the Working Group's own interests. The first of these is the President's Information Technology Advisory Committee (PITAC), which published its report in February. The second is the Computer Science and Telecommunications Board of the National Academies (CSTB), is currently conducting its study entitled Improving Cyber Security Research in the United States. To date, interviews, discussion and correspondence had been conducted with Drs. Freeman and Landwer of the National Science Foundation (NSF), Dr. Richard McConaughey of the National Security Agency (NSA), Dr. Simon Zeichman of the DHS Science and Technology, Dr. Charles Bronstein of the National Academies, and several representatives of the Centers of Excellence Higher Education Institution.

Dr. Rose began by reviewing some of the critical findings of the PITAC:

- Increase funding for basic research in ten priority areas
- Promote recruitment and retention of researchers and students
- Increase repaid transfer of federally developed technologies to the private sector
- Strengthen coordination of federal cyber security research and development activities.

In their review of funding, the PITAC recommended increasing annual basic research funding and cyber security by approximately $90 million. NSF only funded eight percent of cyber security as opposed to the nearly 25-30% of proposals it typically funds. The research topics identified by the PITAC are:

- Authentication technologies
- Secure fundamental protocols
- Secure software engineering and software assurance

- Holistic system security
- Monitoring and detection
- Mitigation and recovery methodologies
- Cyber forensics: catching criminals and deterring criminal activities
- Modeling and test-beds for new technologies
- Metrics, benchmarks, and best practices
- Non-technology issues that can compromise cyber security.

The PITAC also recommended that the interagency work group on critical infrastructure protection co-chaired by Dr. Zeichman of DHS be officially designated as the focal point for coordination of federal research and development efforts.

The Working Group also references the CSTB study: Improving Cyber Security Research in the United States. This study considers the four topics the Working Group previously identified, as well as others. The director, Dr. Brownstein, anticipates a report by the end of the year. Dr. Rose said the CSTB report will take a somewhat longer view of the cyber security research issue.

Dr. Rose mentioned that the Working Group intended to continue reviewing existing cyber security research for pertinent assessments that might prove useful in developing NIAC observations and recommendations. The group will continue soliciting insights from Defense Advanced Research Projects Agency (DARPA) and anticipates further discussions with the interagency work group on critical infrastructure protection.

Dr. Rose concluded his remarks by saying the Working Group administered a survey to select higher education and critical infrastructure sector coordinators to validate study findings and solicit private sector perspectives on the cyber security research topic. In reviewing the findings and recommendations of the two bodies, he said he did not mean to imply at this point that the Working Group intends to propose these recommendations to the Council. Dr. Rose reiterated that these are items the Working Group does want to consider, and for which the Working Group will ultimately reach its own conclusions. These conclusions will be brought back to the Council for review at a later date.

Vice Chairman Chambers thanked Mr. Berkeley and Dr. Rose and commended their first steps in this area. He added that the main challenge in this case will be to generate three or four unique recommendations without overlap with the work of previous similar studies. He congratulated the group again and strongly encouraged the team to pare it down to just a few recommendations.

Dr. Rose agreed.

Mr. Berkeley added that the Working Group is looking to come up with unique, actionable and actually scalable recommendations to meet these criteria.

Chairman Nye thanked Mr. Berkeley and Dr. Rose and asked for questions or comments. There were none, so he asked Nancy Wong for her comments.

Ms. Wong thanked Chairman Nye. She noted that this report concluded the vulnerability disclosure initiative that the Council had taken on. It also led to a series of policy recommendations.

Ms. Wong added that she wanted to recognize the success of this particular initiative. This initiative also led to the CVSS methodology, which as Vice Chairman Chambers reported, now has a group of institutions within private industry stepping forward to take responsibility for it. This also helped make these recommendations operational by the private sector. She wanted to recognize how unique this outcome and deliverable is for an advisory council. Both represented taking responsibility for, accepting accountability for, and providing leadership within the private sector in relationship to these recommendations and policy recommendations. This represents a true public private partnership. Ms. Wong congratulated the Council for a job well done and reinforced what a real contribution each of the NIAC Members has made to this particular issue.

Chairman Nye thanked Ms. Wong and expressed the Council's appreciation for her comments. He said there was nothing quite as gratifying as working on something, bringing forward recommendations and actually having an outcome as a result of those recommendations. When this happens, the Council is very pleased. He said he continued to be thankful and impressed with how hard this Council works and how well the work is received.

VI. NEW BUSINESS — *Chairman Erle A. Nye*, NIAC Members

A. IMPLEMENTATION OF DHS SECTOR PARTNERSHIP MODEL — *Martin G. McGuinn,* Chairman and CEO, Mellon Financial Corporation, Working Group Chair, NIAC Member

Chairman Nye stated he wanted to turn the Council to the issue of new business. He said he earlier had alluded to the formation of the Sector Partnership Model Working Group (SPMWG). He said it seems most of the Council's work can have a tendency to be overshadowed by a bit of nuisance in the recognition that there is a lot of ongoing activity in various industry sectors or with the NIPP. Most industry sectors have organized in some fashion to respond on an industry basis, through either Information Sharing and Analysis Centers (ISACs) or sector coordinating councils. He added there is work going on within industry as well as within various government agencies. Because of FACA and a variety of other circumstances, there does not seem to be the free and effective flow of information between industry and government agencies, a problem that has been discussed in meetings. Chairman Nye said he did not want to take away from any of the ISACs and did not intend to imply criticism of any industry or government agency, but DHS has recognized the need to better integrate these activities, better exchange information, and still conform to FACA's legal requirements. At the January NIAC meeting, Mr. Caverly presented a report on a partnership model that had already been developed. DHS has now requested the NIAC put together a Working Group to give recommendations on the implementation of the model. In response to this request, he and Vice Chairman Chambers agreed this to be a worthy project to undertake and committed to Ms. Wong to establish the Working Group. Thankfully, one of the Council's capable members, Mr.

Martin McGuinn, has agreed to chair this group. At this point, the Chairman asked Mr. McGuinn to present some materials on this undertaking.

Chairman Nye introduced Mr. McGuinn's briefing on the Implementation of the Sector Partnership Model. He said that most sectors are organized to some extent and are cooperating with other sectors and the government on critical infrastructure protection. However, because of FACA guidelines, there is not effective information flow across sectors and the government. He stressed that he did not intend to take anything away from Information Sharing and Analysis Centers (ISACs), but that DHS has recognized the need to better integrate these critical infrastructure protection activities and to conform to the legal requirements of FACA. Chairman Nye reminded the Council members that Mr. Caverly gave a briefing at the January meeting on the new Sector Partnership Model. DHS has since requested that the NIAC create a Working Group to make recommendations on the implementation process of this model. Chairman Nye and Vice Chairman Chambers then sent a letter to Ms. Wong recognizing their agreement with DHS' request and established the Sector Partnership Model Working Group (SPMWG), chaired by Mr. McGuinn. Chairman Nye called this Working Group a valuable undertaking.

Mr. McGuinn thanked Chairman Nye for his introduction and indicated that he intended to go into a little more detail about the proposed structure of the Working Group, as well as the timeline and core deliverables.

After the January 11 NIAC meeting, DHS requested that the NIAC form a Working Group to develop advice and recommendations for the structure, function, and implementation of the Sector Partnership Model. This model builds on past work of the NIAC Cross Sector Interdependencies Working Group, which looked at the best practices of how various sectors collaborated both within and across the sectors. Mr. Caverly presented the conceptual framework for the Sector Partnership Model at the January meeting and this model has been published in the Interim National Infrastructure Protection Plan (I-NIPP).

The model is a framework at this stage and is not a detailed operational plan. Mr. McGuinn said he would review the proposed Working Group deliverables to help to begin further development of this framework.

Before doing this, it is helpful to review the role of the sector coordinating councils as they were envisioned in the Interim NIPP. Mr. McGuinn directed the NIAC to focus on several key points:

- The councils are self-organizing; they are not organized or approved by DHS
- The scope of the councils is two-fold:
    - To provide sector-wide policy development, infrastructure protection planning, and plan implementation
    - To identify and support the information-sharing mechanisms and capabilities (for example, ISACs) deemed most appropriate for the sector

It is anticipated that this project will include deliverables such as:

- Validate that the conceptual structure will work, and to identify and validate the composition and representation in the Sector Partnership Model
- Help define the roles and responsibilities of the coordinating groups

Mr. McGuinn said that the Working Group will also work to define elements of a charter for the overall Sector Partnership Structure as well as the sub-elements, but not the sector councils themselves. This process includes defining the purpose and rules of engagement for how the sector councils, as private organizations, will function within this sector partnership framework.

With respect to the legal framework, the Working Group will identify and review options around whether a workable framework can be established under FACA guidelines. If this is not feasible, the Working Group will work to determine an alternative.

Finally, the Working Group will consider the key processes required to support a true partnership and work to develop overarching principals to guiding the partnership's mode of operations.

Mr. McGuinn illustrated the proposed structure the new Working Group will use to further develop this framework.

Looking at this effort from a top-down approach, it is anticipated that each member of the NIAC would want to be involved in this process. The Working Group believes it will provide an excellent opportunity for NIAC members to become more familiar with their specific sector's coordinating council, and that it will help facilitate communication between the councils and the NIAC representatives.

In addition to the NIAC members participating in the Working Group, members of the sector coordinating councils will also be invited to be a part of Study Groups under the Working Group. In addition to a study group for each sector, there will also be an Integrated Study Group representing cross-sector issues.

As Chairman Nye indicated, the Working Group is working under a very stringent time frame.

The proposed timeline of the Working Group is:

- Through the end of April, it will work to identify, engage, and conduct orientation for those participating in the Working Group
- From April to June, the Working Group will address identified issues and develop recommendations
- The Working Group's goal is to present the Working Group's final recommendations to the Council at the July meeting

Chairman Nye thanked Mr. McGuinn for his presentation, said he recognized there might be some sensitivity among sectors, and wanted to reiterate that the Council is not attempting to direct sectors in how they are organized. As long as the sector coordinating council is broadly representational, the NIAC will defer to the specific sector itself in that regard. In this regard, however, each sector needs to be broad enough so that all elements of the industry can effectively participate. He added that it is important that each critical infrastructure industry have an active group and they be involved in this partnership as Mr. Caverly discussed in January. Chairman Nye asked Vice Chairman Chambers if he had any thoughts.

Vice Chairman Chambers added that the Sector Partnership Model Working Group is one of the most important practical initiatives the NIAC has taken on thus far. He echoed the Chairman's comments that these sector stakeholders are independently reorganizing and should shape the effort of this. He also recognized that the timeframe is ambitious, but he trusted the Council's judgment.

Chairman Nye thanked Vice Chairman Chambers and announced that the position of Vice Chairman of the SPMWG is currently open.

Mr. McGuinn confirmed the Working Group could use any assistance the NIAC was willing to provide.

Chairman Nye also acknowledged the work of the SPMWG is very important and it is critical the NIAC get active participation from industry. He committed to Mr. McGuinn that the members of the NIAC will help him in anyway they could on this endeavor.

Mr. McGuinn thanked him.

Chairman Nye asked if there were any further comments or suggestions. He reiterated that he could not overemphasize how critical it is that the Council gets the active participation of various critical infrastructure industries and interacts with the relevant government agencies in a fashion complying with FACA regulations with respect to receiving and delivering information.

He asked if there were further comments or questions about the projects that are pending. There were none.

Chairman Nye noted that the Council's charter is up for renewal and that the White House is very enthusiastic about the work the Council has done. He said he anticipated the renewal will come fairly soon, and as the Secretary said, he expected the charter to be extended to include more physical considerations as well as cyber considerations. He also anticipated that additional members would be brought forward. He understood that there were several prospects going through the nominating process and there are some critical infrastructure areas and industries that are not represented. Hopefully, new appointments will remedy this. The Chairman also said he was pleased that a majority of the members now have their secret level clearances. These clearances will allow the Council to have briefings that are more complete. A few clearances are still in process and a few members have not completely submitted their data. He encouraged everyone to complete this.

Chairman Nye stated that the NIAC is scheduled to meet in person in Washington on July 12th at the National Press Club. The meeting will begin at 1:30 p.m. He said the Secretary is at least presently planning to attend. The Council has several projects that should be coming to a critical stage at this time and he said he hoped everyone would plan to attend. There is also an in-person meeting scheduled for October 11th in Washington. The White House has been notified for both of these meetings. It would be helpful if the President could brief the Council on one of those dates. Obviously, his schedule comes first and the Council certainly understands this. Chairman Nye said he did anticipate that the Council would have an opportunity to brief the President on its progress later this year. Chairman Nye said he had nothing further to add and asked if anyone had any further comments.

Ms. Wong again congratulated the Council for a job well done.

Vice Chairman Chambers said that the meeting had been a very efficient one.

VII. ADJOURNMENT *Chairman Erle A. Nye*

Chairman Nye thanked everyone for coming and said he looked forward to the meeting in July. With this, Chairman Nye adjourned the meeting.

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

By: ______________________ Dated: 7/12/05
Erle A. Nye, Chairman

ATTACHMENT A:
Status Report on the Intelligence Coordination Working Group

NIAC Intelligence Coordination Working Group

Status Report
April 2005

John Chambers
President & CEO,
Cisco Systems, Inc.

Gilbert Gallegos
Chief of Police (ret.)
Albuquerque, NM

To Review……

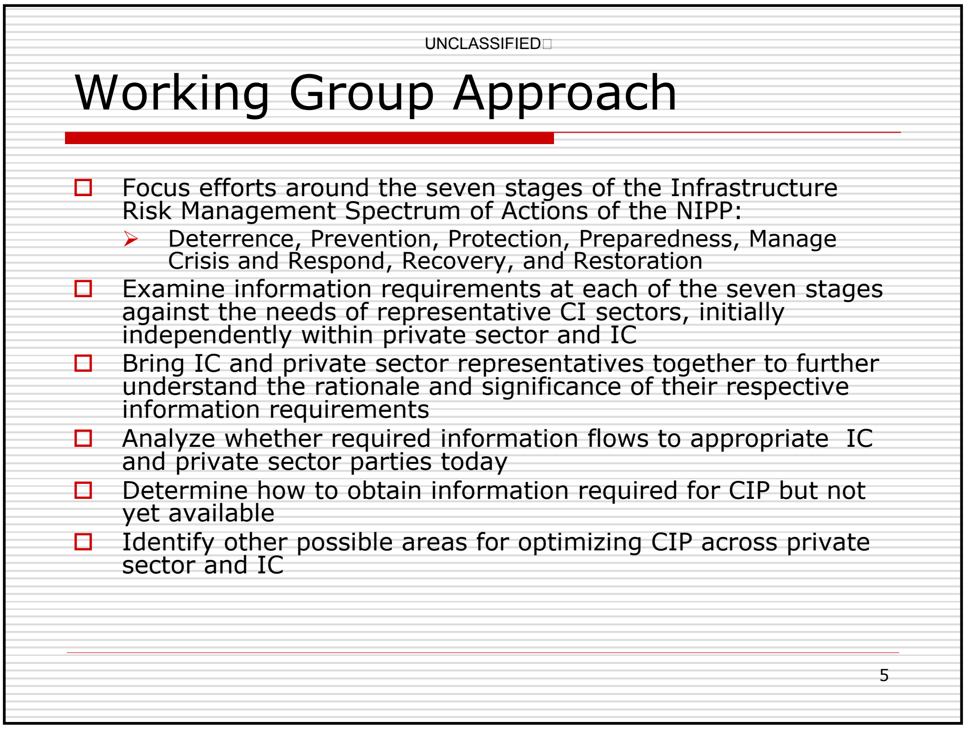
- Purpose
- Working Group Focus
- Pending Actions

Purpose

- □ Develop policy recommendations that ensure:
  - Intelligence Community (IC) (including Law Enforcement) understands private sector’s Critical Infrastructure Protection (CIP) domain expertise, intelligence requirements, and dissemination capabilities
  - Private sector understands IC responsibilities, objectives and processes in CIP, especially regarding threat assessments
  - Improvements in IC and private sector community interaction and optimum contribution to CIP are understood and considered by policymakers

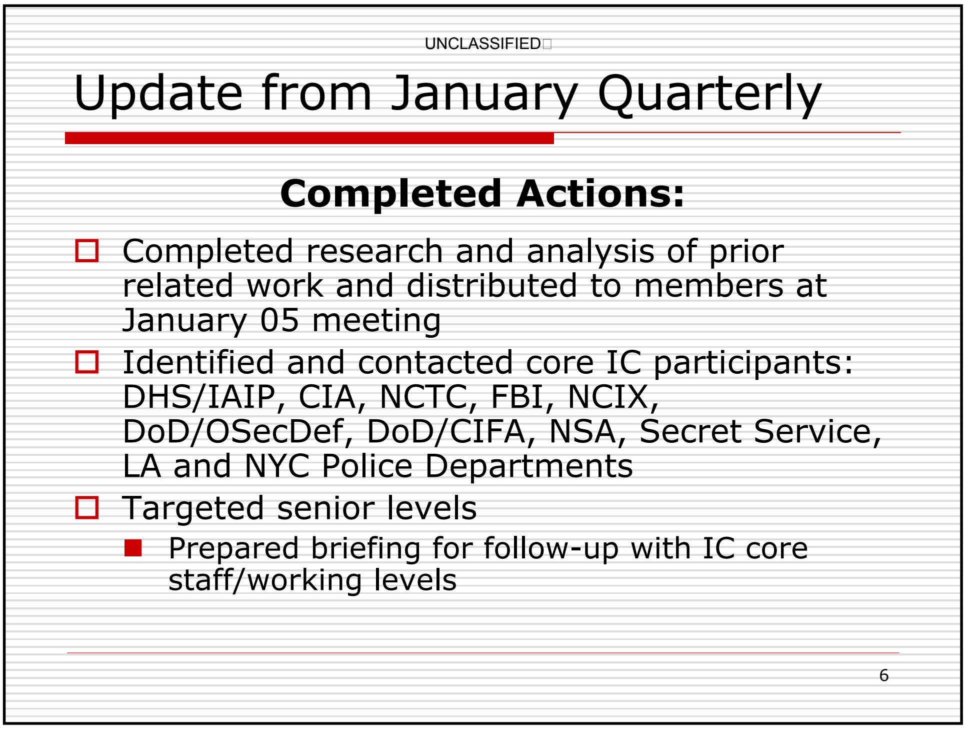
NIAC IC Working Group Focus

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



Working Group Approach

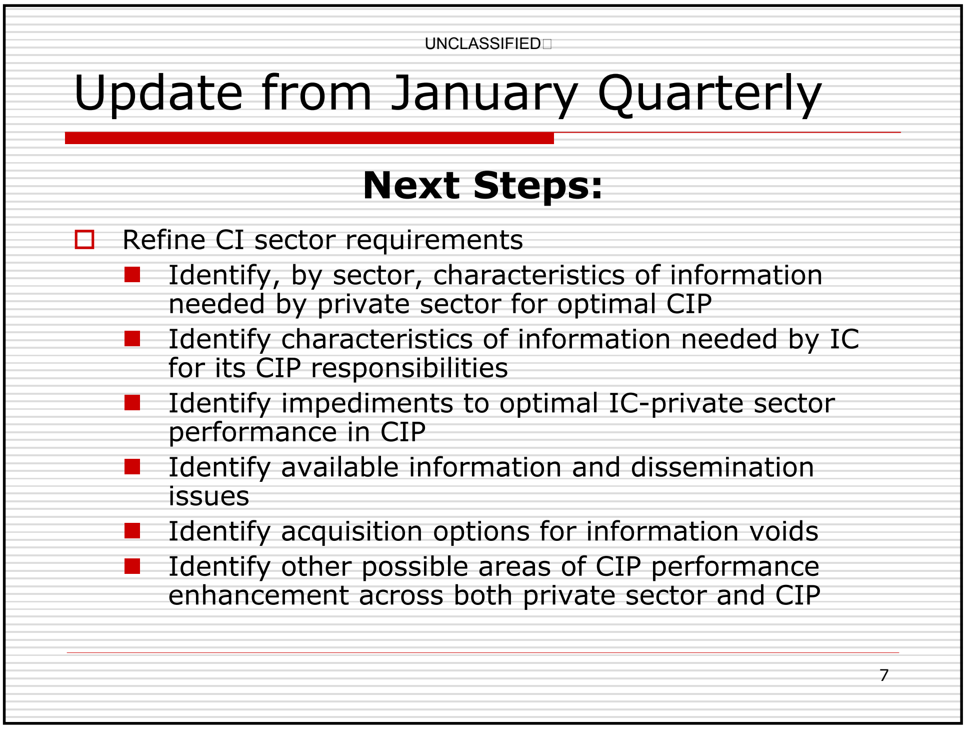
- □ Focus efforts around the seven stages of the Infrastructure Risk Management Spectrum of Actions of the NIPP:
  - ➢ Deterrence, Prevention, Protection, Preparedness, Manage Crisis and Respond, Recovery, and Restoration
- □ Examine information requirements at each of the seven stages against the needs of representative CI sectors, initially independently within private sector and IC
- □ Bring IC and private sector representatives together to further understand the rationale and significance of their respective information requirements
- □ Analyze whether required information flows to appropriate IC and private sector parties today
- □ Determine how to obtain information required for CIP but not yet available
- □ Identify other possible areas for optimizing CIP across private sector and IC



Update from January Quarterly

Completed Actions:

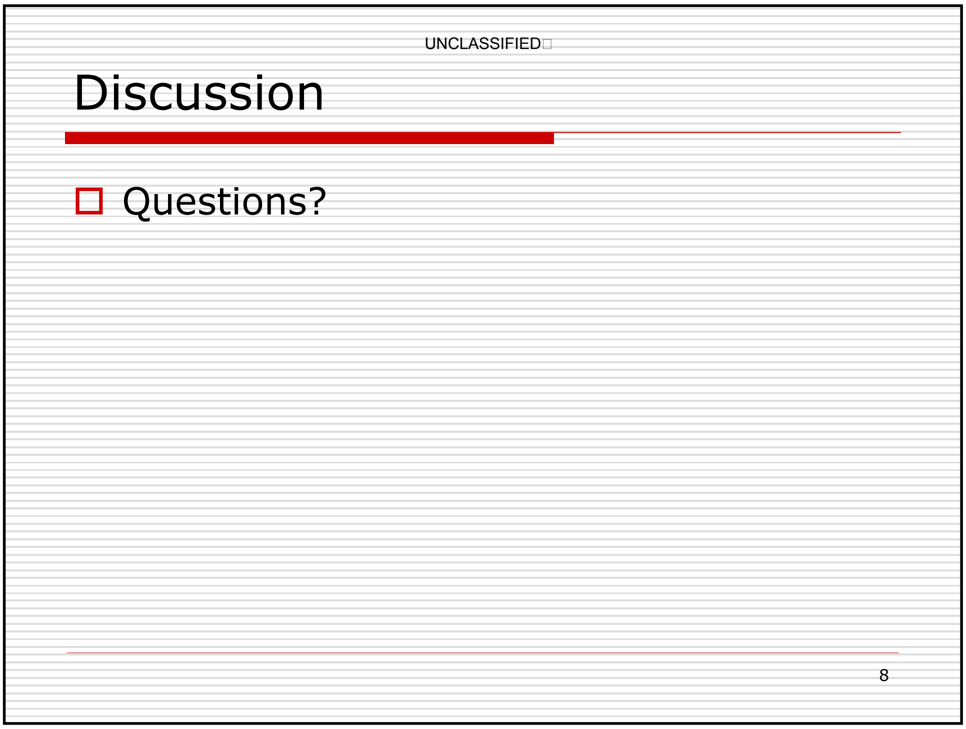
- □ Completed research and analysis of prior related work and distributed to members at January 05 meeting
- □ Identified and contacted core IC participants: DHS/IAIP, CIA, NCTC, FBI, NCIX, DoD/OSecDef, DoD/CIFA, NSA, Secret Service, LA and NYC Police Departments
- □ Targeted senior levels
  - ■ Prepared briefing for follow-up with IC core staff/working levels



Update from January Quarterly

Next Steps:

- Refine CI sector requirements
  - Identify, by sector, characteristics of information needed by private sector for optimal CIP
  - Identify characteristics of information needed by IC for its CIP responsibilities
  - Identify impediments to optimal IC-private sector performance in CIP
  - Identify available information and dissemination issues
  - Identify acquisition options for information voids
  - Identify other possible areas of CIP performance enhancement across both private sector and CIP



Discussion

- Questions?

ATTACHMENT B:
Status Report on the
Risk Management Approaches to Protection
Working Group

Risk Management Working Group Update

Martha Marsh
President and CEO
Stanford Hospital and Clinics

Tom Noonan
CEO and Chairman
Internet Security Systems

March 28, 2005

Agenda

- Attributes of maturity
- Risk management across industries
- Government intervention
- Next Steps
  - Complete cross-industry risk management analysis
  - Public-private sector benchmarking study
  - Socialize findings

Attributes of Maturity

- □ Predictive risk management is enhanced when predicated upon past performance
- □ Mature risk management
  - Free market impacts competitiveness
  - Legal precedent provides foundation for qualitative nature of risk management
  - Highly actuarialized data; mature understanding of failure mechanisms and failure indicators
  - Proximity between actuaries, indicators, and decision-makers
- □ Immature risk management includes inverse attributes of maturity

Risk Management Across Industries

- □ Across all industries, there exist examples of mature and immature risk management; some areas are becoming more mature over time
- □ Areas that lend themselves well to predictive analysis include:
  - Airline safety
  - Automobile insurance
- □ Areas that ***do not*** lend themselves well to predictive analysis include:
  - Natural events (e.g. weather, earthquakes, etc.)
  - Commodities
- □ Areas that are emerging from poorly predictive to more mature analysis include:
  - Network or infrastructure disruptions

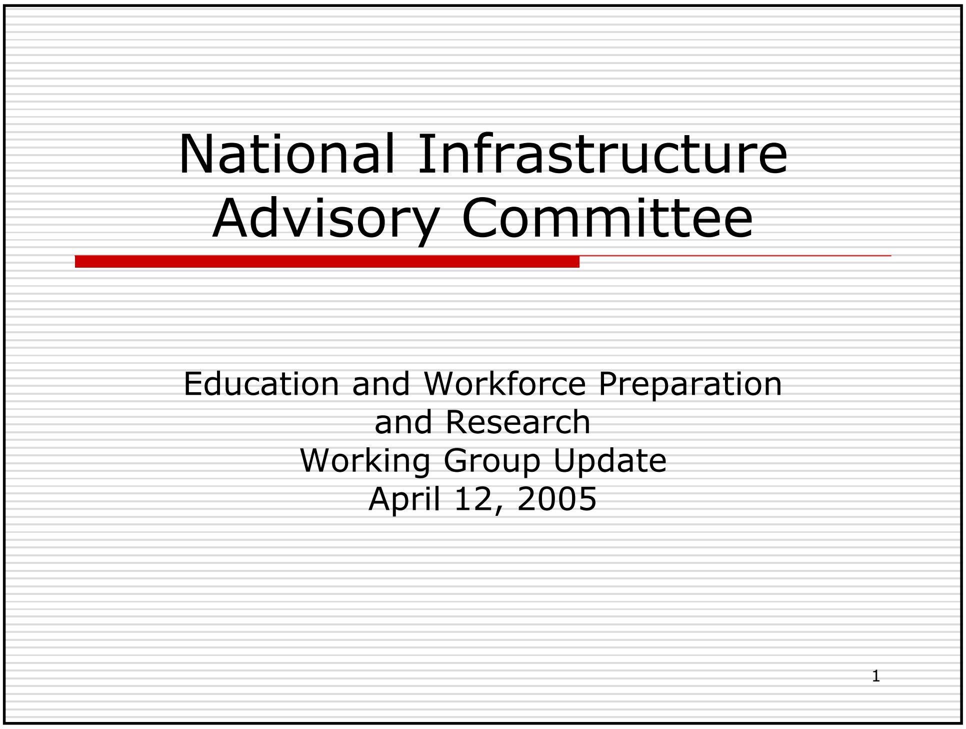
Next Steps

- □ Complete analysis of industry risk management
  - ■ Maturity models; risk management methodologies
  - ■ Spectrum of acceptable/unacceptable risk
  - ■ Cross-sector risk management commonalities
  - ■ Examples of government intervention in RM
- □ Complete benchmark against DHS risk management study
- □ Develop and socialize specific findings and recommendations within next 60 days

Discussion

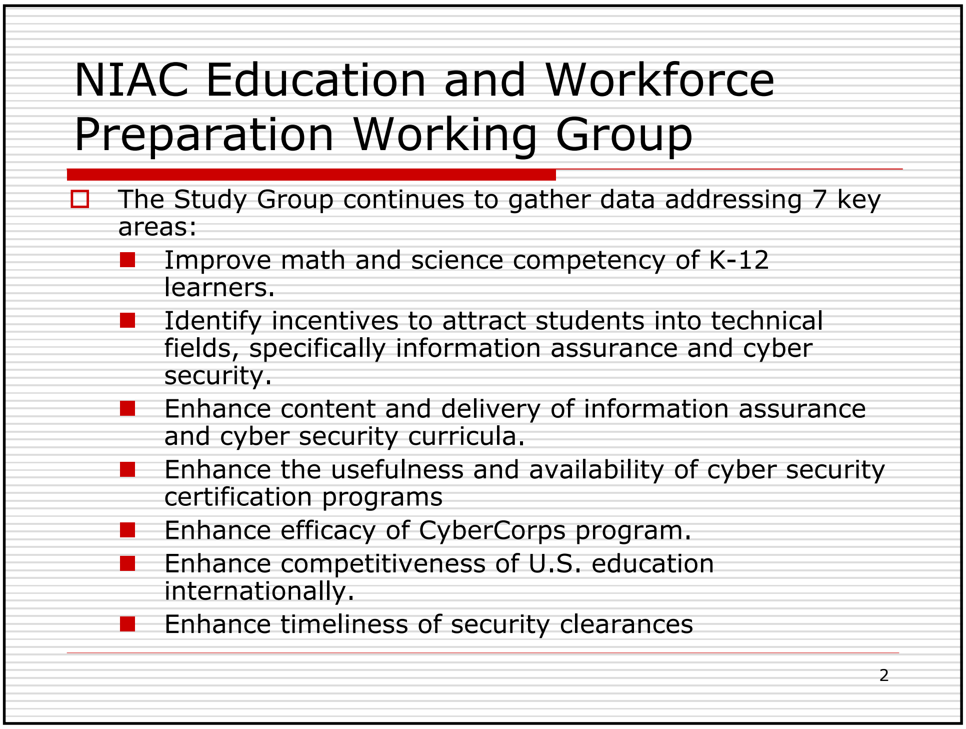
- □ Questions?

ATTACHMENT C:
Status Report on the Education and Workforce Preparation Working Group



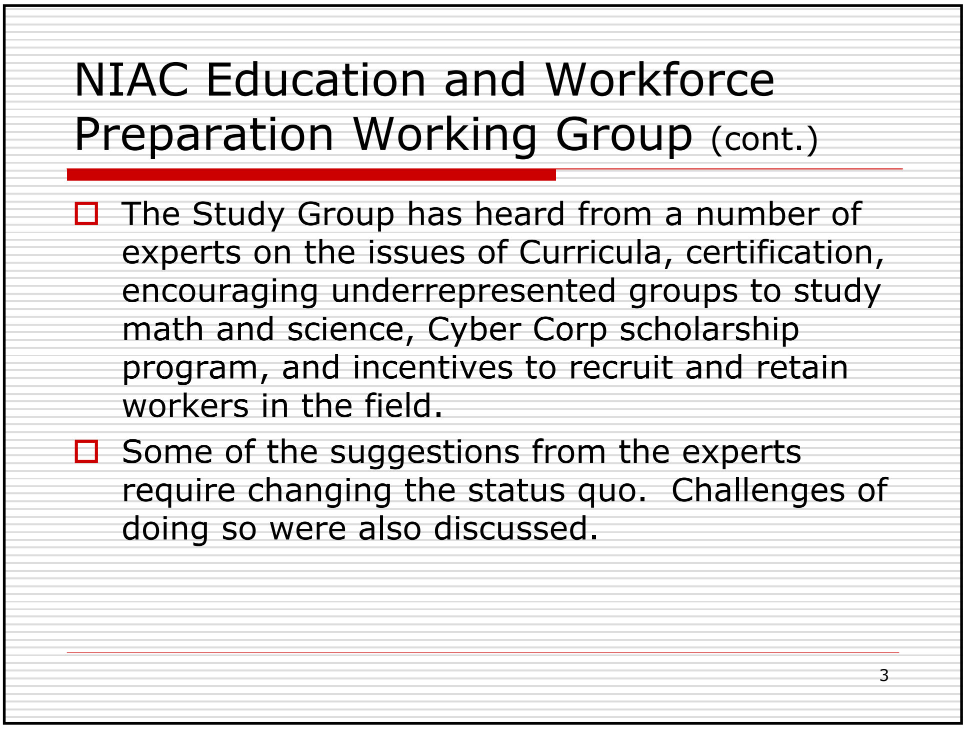
National Infrastructure Advisory Committee

Education and Workforce Preparation
and Research
Working Group Update
April 12, 2005



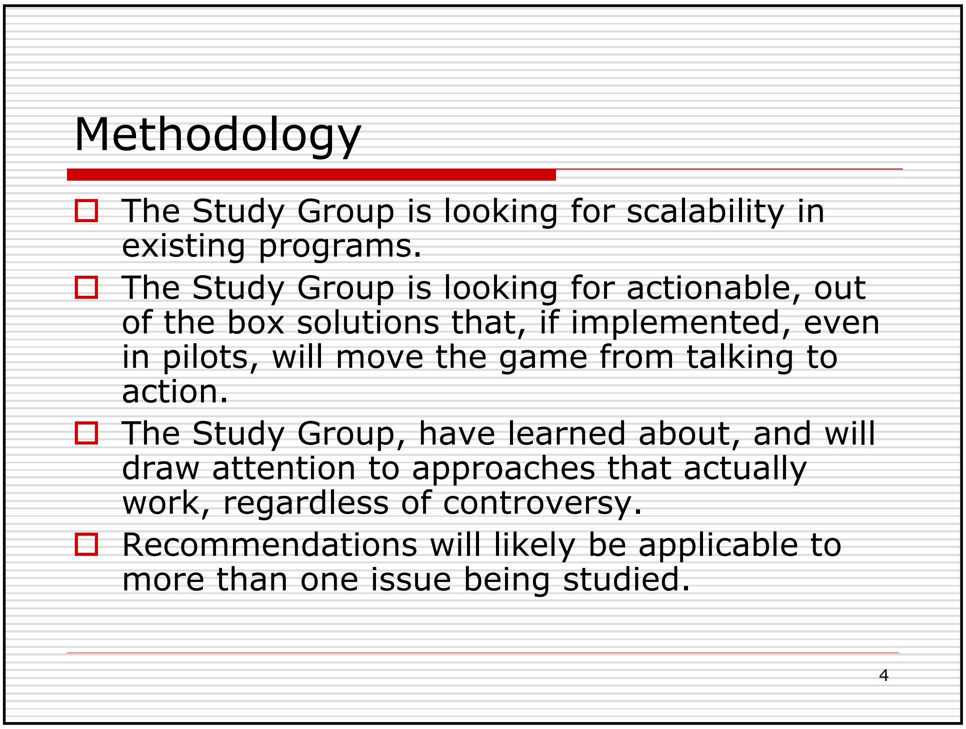
NIAC Education and Workforce Preparation Working Group

- The Study Group continues to gather data addressing 7 key areas:
  - Improve math and science competency of K-12 learners.
  - Identify incentives to attract students into technical fields, specifically information assurance and cyber security.
  - Enhance content and delivery of information assurance and cyber security curricula.
  - Enhance the usefulness and availability of cyber security certification programs
  - Enhance efficacy of CyberCorps program.
  - Enhance competitiveness of U.S. education internationally.
  - Enhance timeliness of security clearances



NIAC Education and Workforce Preparation Working Group (cont.)

- □ The Study Group has heard from a number of experts on the issues of Curricula, certification, encouraging underrepresented groups to study math and science, Cyber Corp scholarship program, and incentives to recruit and retain workers in the field.
- □ Some of the suggestions from the experts require changing the status quo. Challenges of doing so were also discussed.



Methodology

- □ The Study Group is looking for scalability in existing programs.
- □ The Study Group is looking for actionable, out of the box solutions that, if implemented, even in pilots, will move the game from talking to action.
- □ The Study Group, have learned about, and will draw attention to approaches that actually work, regardless of controversy.
- □ Recommendations will likely be applicable to more than one issue being studied.

Math and Science Competency for K-12

- Spoke with E. D. Hirsch, retired Education professor from University of Virginia and author about “process oriented” vs. “knowledge based” education.
- No consistency in education between localities or state.
- Discussed benefits & difficulties of developing Core Curriculum.

Math and Science Competency for K-12 (cont.)

- Spoke with John Yochalson, President of Best Engineering and Science Talent (BEST) on how to encourage underrepresented groups to enter field of math and science.
- Challenge in education, in general, no connectivity between K-12, and higher education.
- Found pockets of excellence within school programs, but nothing that was system wide.

Math and Science Competency for K-12 (cont.)

- □ Outreach to Department of Education.
- □ Department of Education representatives to present to the Study Group in April. Interested in available metrics and related studies.

Incentives to Attract Students

- □ Attracting students to technical fields
  - ■ The Study Group continues to examine this issue.
  - ■ Scholarships, such as those from the National Science Foundation.
  - ■ Mentorship programs.
  - ■ To encourage more PH.D, one expert suggests 5 year loans to students. When done with PH.D, for each year they work at a University, forgive a year of the loan.

Incentives to Attract Students (cont.)

- The Study Group is using contacts at SUNY Buffalo, which has an NSF grant to research this issue.
- Looking to speak to a Cyber Corp graduate(s) and get feedback on their experience as well as suggestions.

Cyber Security Curricula Development

- □ Dr. Blaine Burnham, a Senior Research Fellow, at the University of Nebraska Consortium on Information Assurance discussed how College Education needs to be less vocational, or training oriented, and more core theory.
- □ Educators in the field need more real world experience. Compared to ROTC, how officers rotate into ROTC teaching positions after having been in the field.
- □ Need to encourage those with the most knowledge to get in-front of a class. But pay in private industry is better than teaching.
- □ Need more PH.Ds.

Cyber Security Curricula Development (cont.)

- □ National Science Foundation’s Federal Cyber Program Scholarship for Service Program (Cyber Corp) has a Capacity building track. Have provided $150,000 a year for two years, for curriculum and faculty development to qualifying educational institutions.

Efficacy of CyberCorps

- □ Dr. Diana Gant of the Federal Scholarship for Service Program in Information Assurance (Cyber Corp) discussed the program.
- □ Scholarship money goes to Universities that are Centers for Academic Excellence in Information Assurance Education (CAE/IAE). About $2.5 million, which funds 30 students for two years (tuition, room board, fees and stipends).
- □ 540 students have received scholarships.
- □ Challenges: lag in hiring process and security clearances for graduates.

International Competitiveness of US Education

- This is closely related to the K-12 question.
- Recommendations for K-12 will likely overlap.
- Study group scheduled to hear from a technology trade association regarding an industry view of this issue.

Certification programs

- Spoke with Hun Kim, Department of Homeland security. Government is looking to establish a consistent Information Security Certification Programs based on Common Body of Knowledge.
- Government does not want to be in business of certification, but would like to see nationally recognized, privately administrated certification programs.
- The Institute for Defense Analyses (IDA) also presented. Wrote a white paper for Dept of Defense (DOD) compared existing certification programs to DOD requirements.

Certification programs (cont’d)

- □ Found many existing programs fit DOD requirements.

Timeliness of Security Clearance Process

- □ The group is still collecting data on this issue. This is an issue for many.

Next Steps

- □ The Study Group continues to collect information.
- □ Is currently forming draft recommendations to address the 7 key areas.

National Infrastructure Advisory Committee

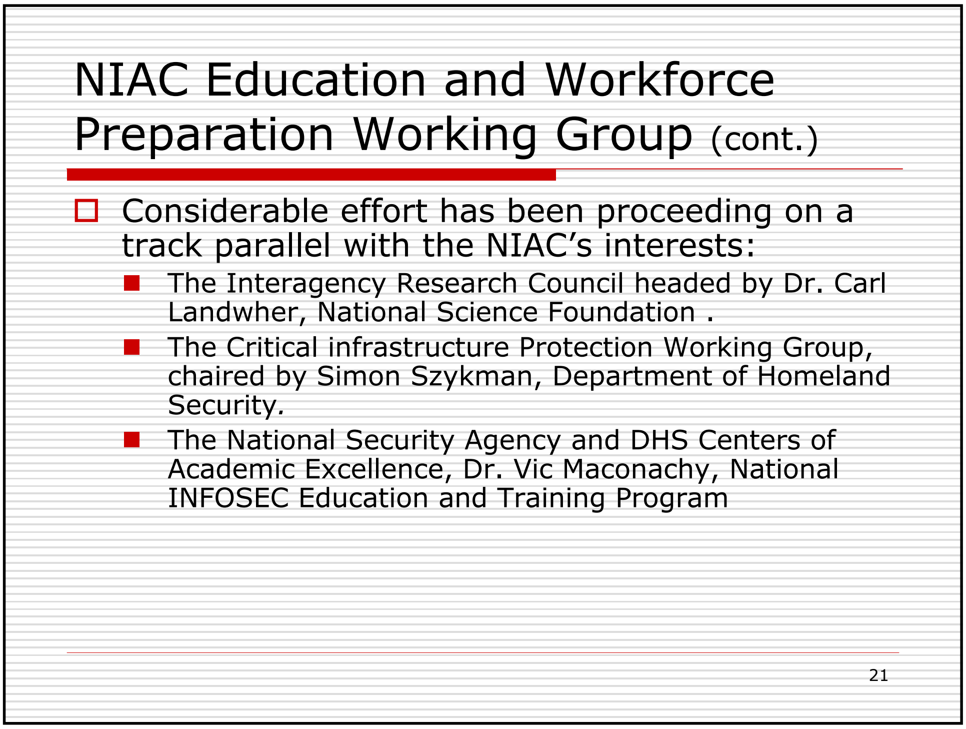
Workforce Preparation & Education -
Research Working Group Update
April 12, 2005

NIAC Education and Workforce Preparation Working Group

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

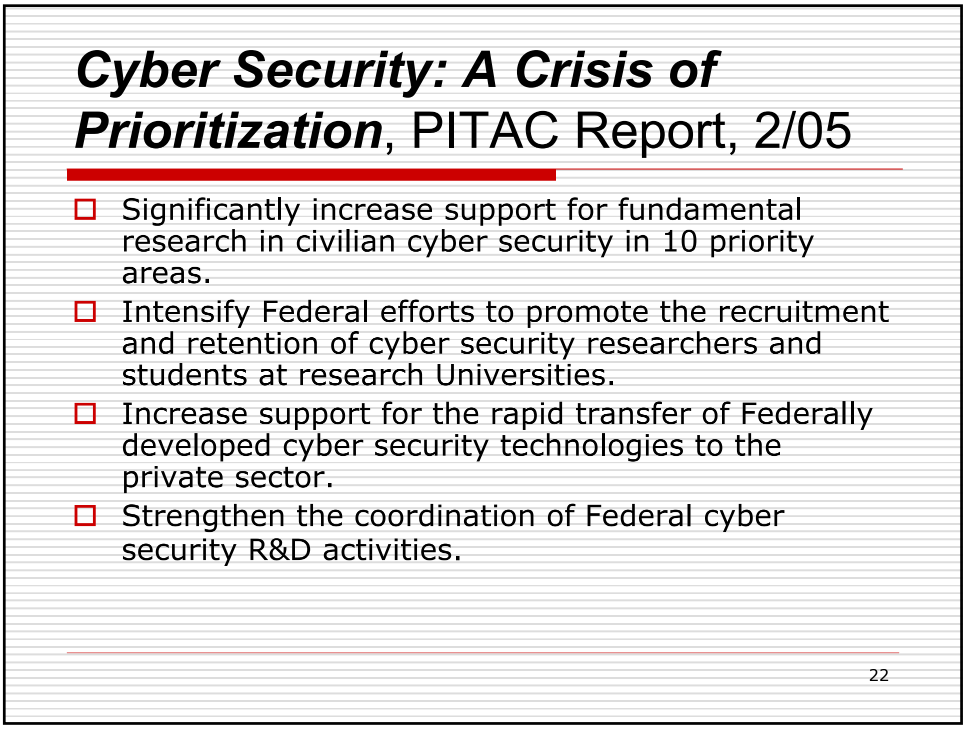
NIAC Education and Workforce Preparation Working Group (cont.)

- Considerable effort has been proceeding on a track parallel with the NIAC’s interests:
  - The February 2005 report of the President’s Information Technology Advisory Committee published by the National Coordination Office for Information Technology Research and Development.
  - The Computer Science and Telecommunications Board current study, *Improving Cyber Security Research in the United States.*



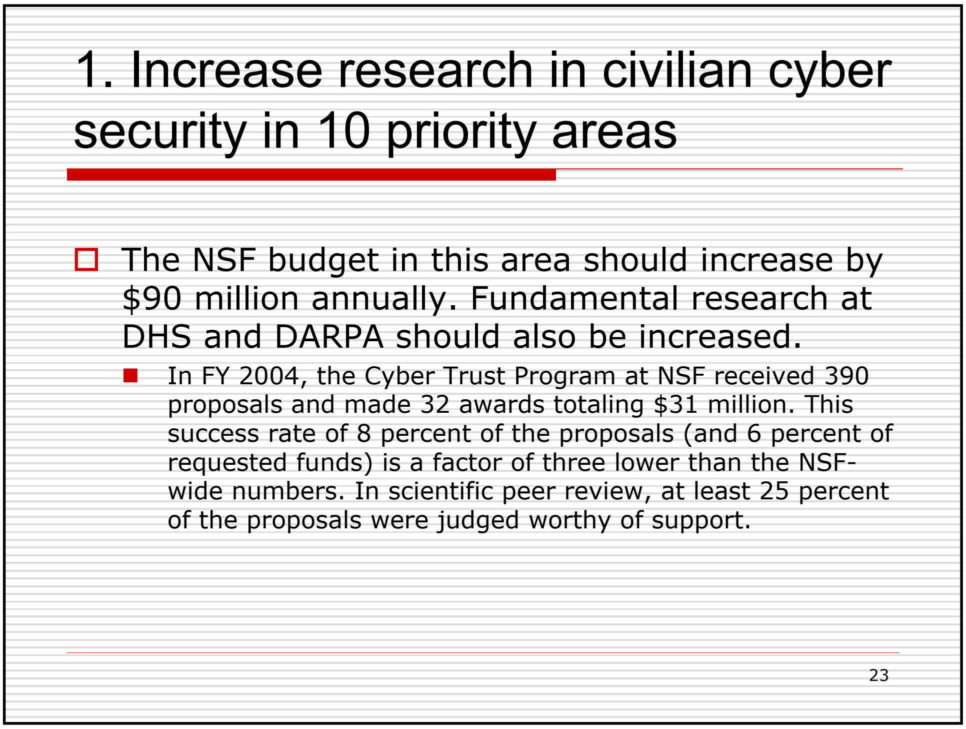
NIAC Education and Workforce Preparation Working Group (cont.)

- □ Considerable effort has been proceeding on a track parallel with the NIAC’s interests:
  - The Interagency Research Council headed by Dr. Carl Landwher, National Science Foundation .
  - The Critical infrastructure Protection Working Group, chaired by Simon Szykman, Department of Homeland Security.
  - The National Security Agency and DHS Centers of Academic Excellence, Dr. Vic Maconachy, National INFOSEC Education and Training Program



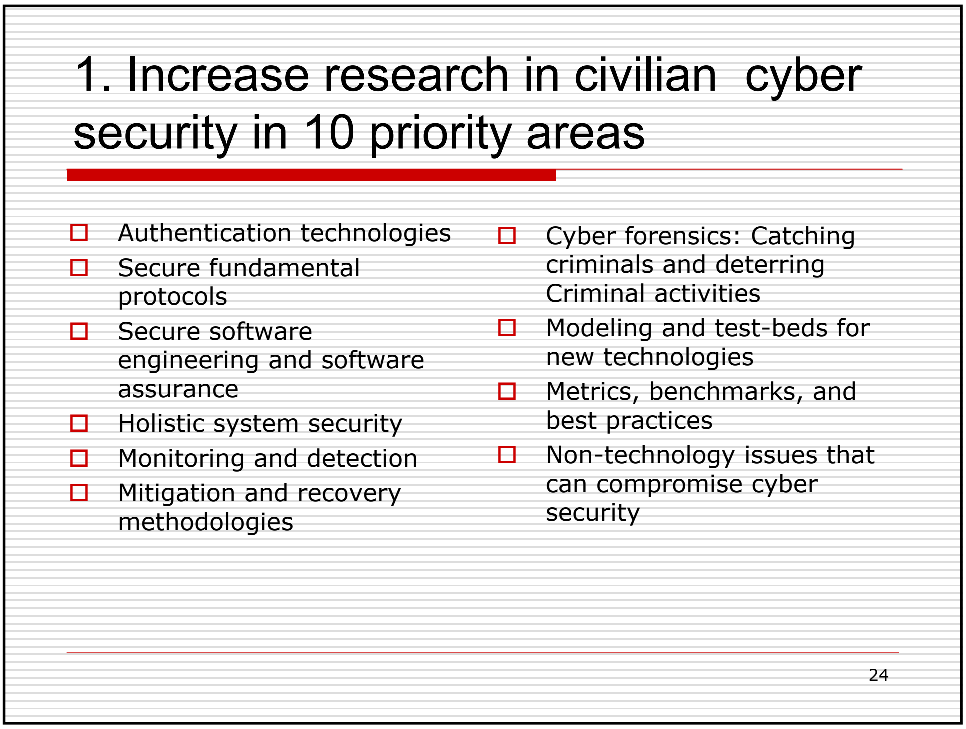
Cyber Security: A Crisis of Prioritization, PITAC Report, 2/05

- □ Significantly increase support for fundamental research in civilian cyber security in 10 priority areas.
- □ Intensify Federal efforts to promote the recruitment and retention of cyber security researchers and students at research Universities.
- □ Increase support for the rapid transfer of Federally developed cyber security technologies to the private sector.
- □ Strengthen the coordination of Federal cyber security R&D activities.



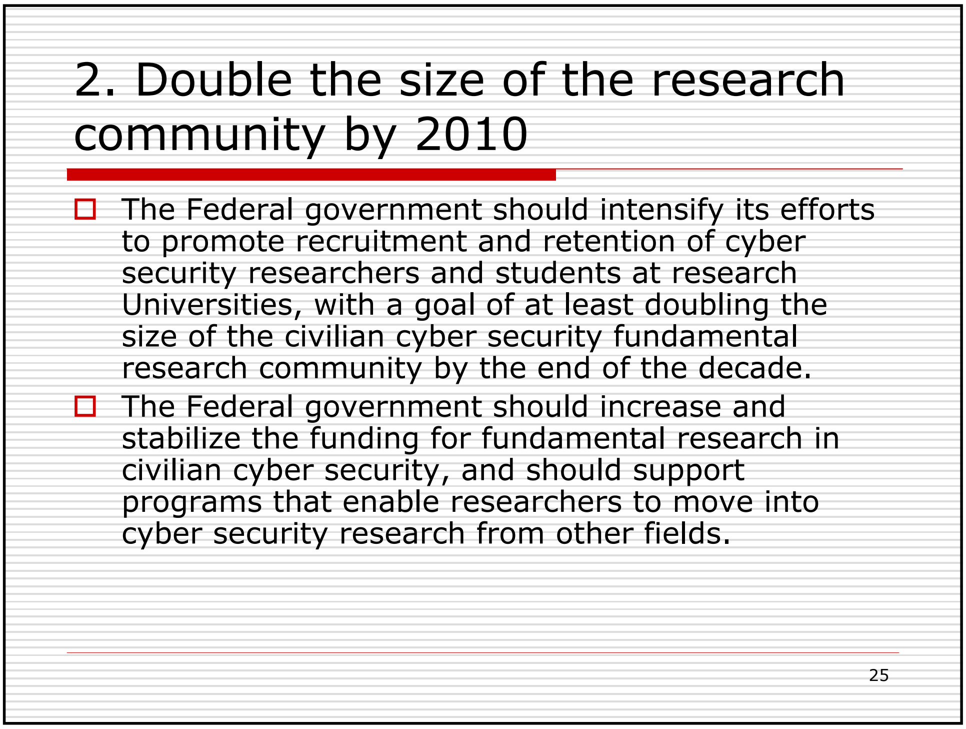
1. Increase research in civilian cyber security in 10 priority areas

- □ The NSF budget in this area should increase by $90 million annually. Fundamental research at DHS and DARPA should also be increased.
  - ■ In FY 2004, the Cyber Trust Program at NSF received 390 proposals and made 32 awards totaling $31 million. This success rate of 8 percent of the proposals (and 6 percent of requested funds) is a factor of three lower than the NSF-wide numbers. In scientific peer review, at least 25 percent of the proposals were judged worthy of support.



1. Increase research in civilian cyber security in 10 priority areas

- □ Authentication technologies
- □ Secure fundamental protocols
- □ Secure software engineering and software assurance
- □ Holistic system security
- □ Monitoring and detection
- □ Mitigation and recovery methodologies
- □ Cyber forensics: Catching criminals and deterring Criminal activities
- □ Modeling and test-beds for new technologies
- □ Metrics, benchmarks, and best practices
- □ Non-technology issues that can compromise cyber security



2. Double the size of the research community by 2010

- □ The Federal government should intensify its efforts to promote recruitment and retention of cyber security researchers and students at research Universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade.
- □ The Federal government should increase and stabilize the funding for fundamental research in civilian cyber security, and should support programs that enable researchers to move into cyber security research from other fields.

3. Strengthen the cyber security technology transfer partnership

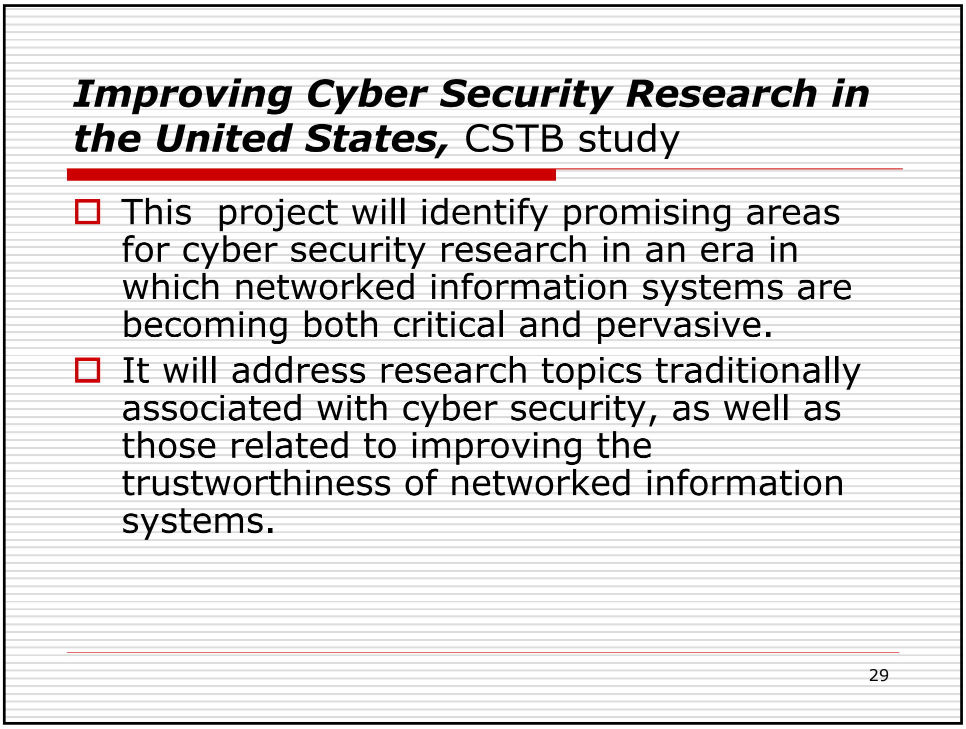
- □ Specifically, the Federal Government should place greater emphasis on the development of metrics, models, datasets, and test-beds so that new products and best practices can be evaluated.
- □ Jointly sponsor with the private sector an annual interagency conference to showcase new cyber security R&D.
- □ Fund technology transfer efforts (in cooperation with industry) by researchers who have developed promising ideas or technologies.
- □ Encourage Federally supported graduate students and post doctoral researchers to gain experience in industry as researchers, interns, or consultants.

4. Focal point for coordinating Federal cyber security R&D efforts

- □ The Interagency Working Group on Critical Information Infrastructure Protection (IWG/CIIP) should become the focal point for coordinating Federal cyber security R&D efforts. This working group should be strengthened and integrated under the Networking and Information Technology Research and Development (NITRD) Program.

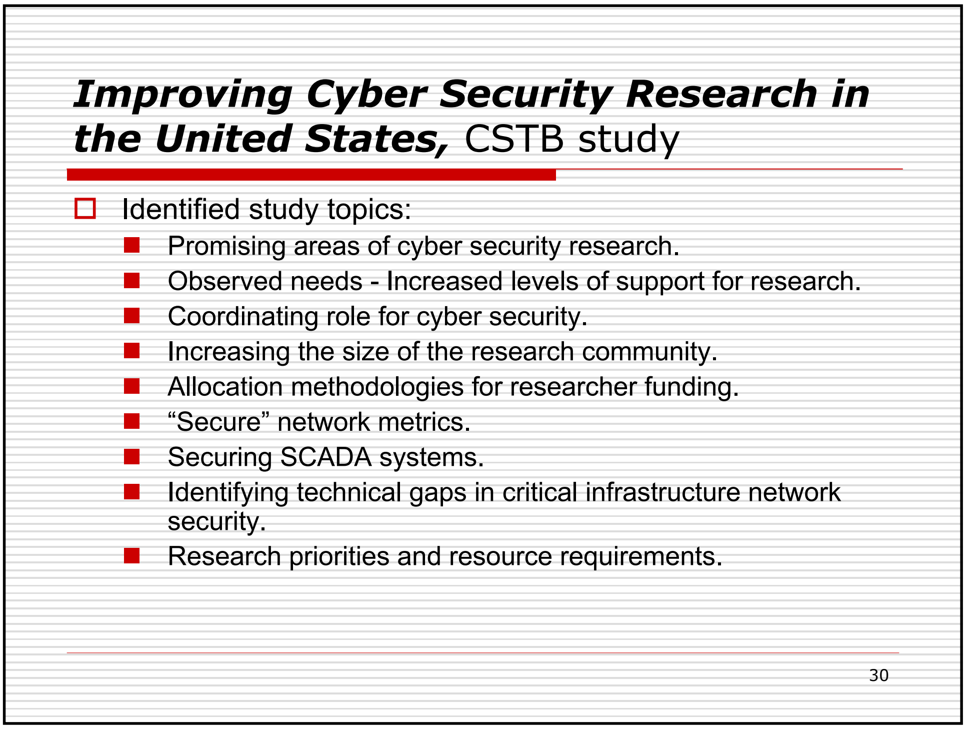
4. Focal point for coordinating Federal cyber security R&D efforts

- □ Current Federal Government cyber security R&D coordinating bodies:
  - ■ Interagency Working Group on Critical Information Infrastructure Protection (IWG/CIIP), which is part of the National Science and Technology Council (NSTC)
  - ■ Subcommittee on Networking and Information Technology Research and Development, which coordinates the NITRD Program and which is also part of the NSTC, and the Subcommitee's Coordinating Groups, especially the :
    - □ High Confidence Software and Systems Coordinating Group
    - □ Large Scale Networking Coordinating Group
  - ■ Infosec Research Council



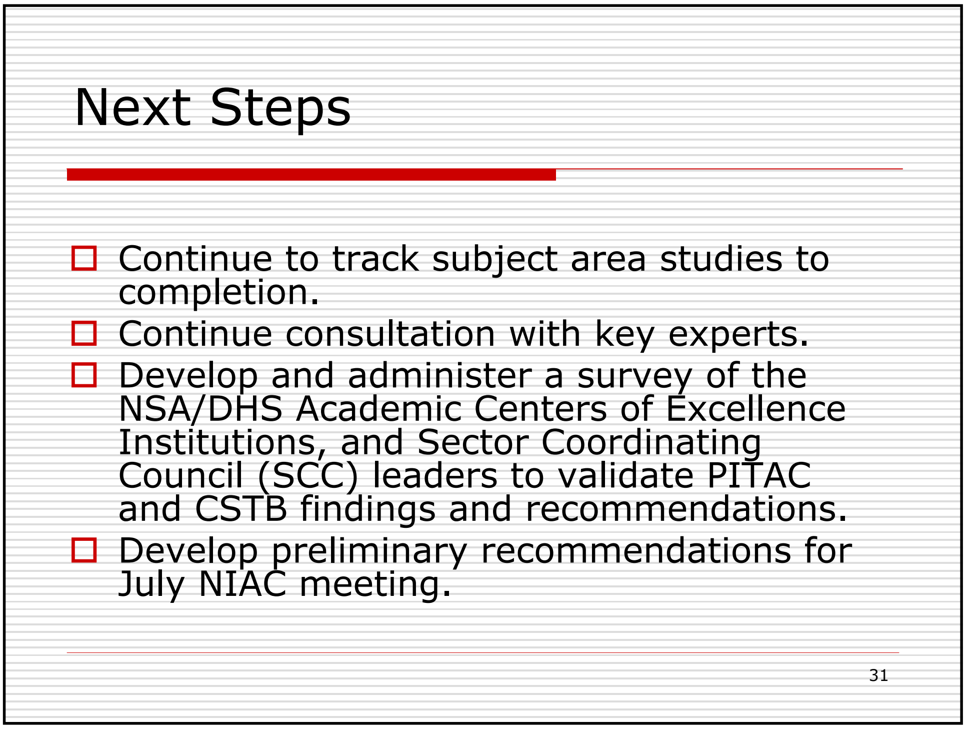
Improving Cyber Security Research in the United States, CSTB study

- □ This project will identify promising areas for cyber security research in an era in which networked information systems are becoming both critical and pervasive.
- □ It will address research topics traditionally associated with cyber security, as well as those related to improving the trustworthiness of networked information systems.



Improving Cyber Security Research in the United States, CSTB study

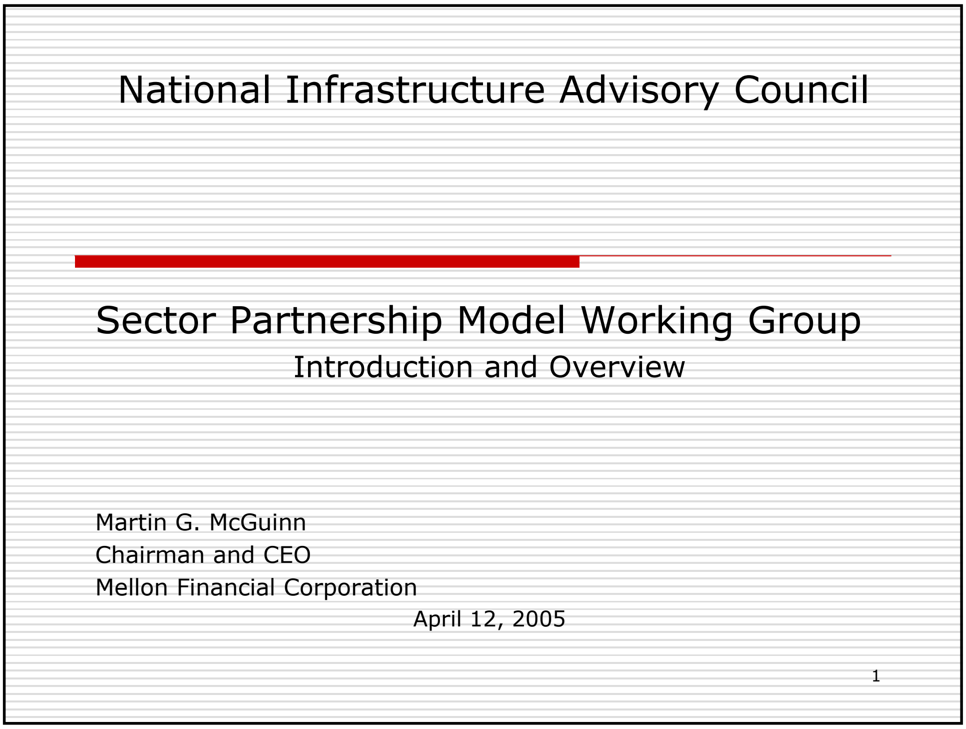
- □ Identified study topics:
  - Promising areas of cyber security research.
  - Observed needs - Increased levels of support for research.
  - Coordinating role for cyber security.
  - Increasing the size of the research community.
  - Allocation methodologies for researcher funding.
  - “Secure” network metrics.
  - Securing SCADA systems.
  - Identifying technical gaps in critical infrastructure network security.
  - Research priorities and resource requirements.



Next Steps

- □ Continue to track subject area studies to completion.
- □ Continue consultation with key experts.
- □ Develop and administer a survey of the NSA/DHS Academic Centers of Excellence Institutions, and Sector Coordinating Council (SCC) leaders to validate PITAC and CSTB findings and recommendations.
- □ Develop preliminary recommendations for July NIAC meeting.

ATTACHMENT D:
Status Report on the Sector Partnership Model Working Group



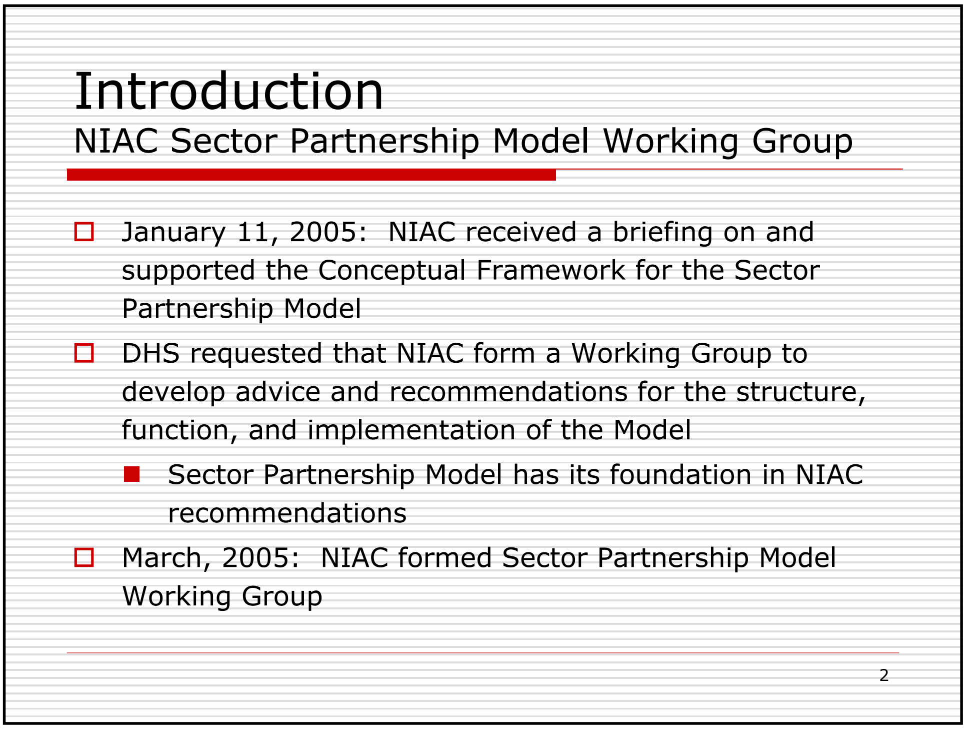
National Infrastructure Advisory Council

Sector Partnership Model Working Group

Introduction and Overview

Martin G. McGuinn
Chairman and CEO
Mellon Financial Corporation

April 12, 2005

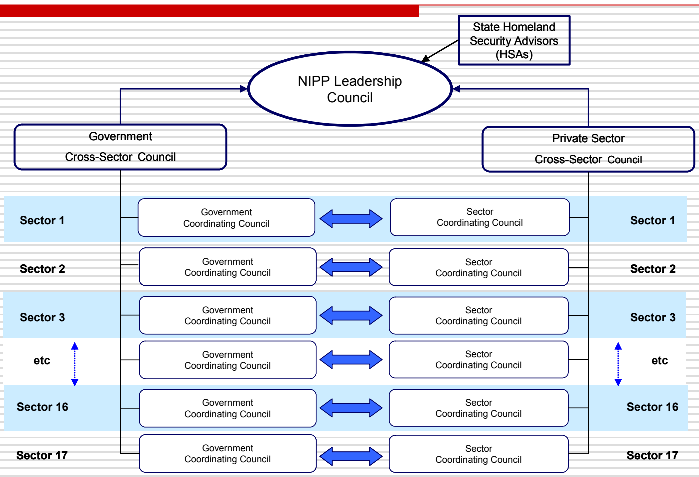


Introduction

NIAC Sector Partnership Model Working Group

- January 11, 2005: NIAC received a briefing on and supported the Conceptual Framework for the Sector Partnership Model
- DHS requested that NIAC form a Working Group to develop advice and recommendations for the structure, function, and implementation of the Model
  - Sector Partnership Model has its foundation in NIAC recommendations
- March, 2005: NIAC formed Sector Partnership Model Working Group

Conceptual Framework for Sector Partnership Model



State Homeland Security Advisors (HSAs)

NIPP Leadership Council

Government Cross-Sector Council

Private Sector Cross-Sector Council

Sector 1	Government Coordinating Council	Sector Coordinating Council	Sector 1
Sector 2	Government Coordinating Council	Sector Coordinating Council	Sector 2
Sector 3	Government Coordinating Council	Sector Coordinating Council	Sector 3
etc	Government Coordinating Council	Sector Coordinating Council	etc
Sector 16	Government Coordinating Council	Sector Coordinating Council	Sector 16
Sector 17	Government Coordinating Council	Sector Coordinating Council	Sector 17

Role of Sector Coordinating Councils

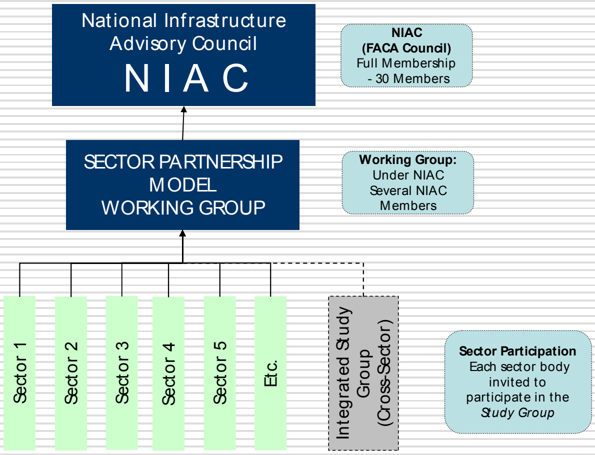
As described in the Interim National Infrastructure Protection Plan:

- Sector coordinating councils are being established by the private sector
- Purpose of these councils is to provide the framework for private-sector owners and operators to engage DHS and Sector Specific Agencies, and to collaborate with them to:
  - Identify, prioritize, and coordinate the protection of Critical Infrastructures/Key Resources, and
  - Facilitate sharing of information about threats, vulnerabilities, incidents, potential protective measures, and best practices.
- The primary function of a sector coordinating council is to:
  - Facilitate inclusive organization and coordination of the policy development, infrastructure-protection planning, and plan implementation activities within the sector.
  - Identify and support the information-sharing mechanisms and capabilities deemed most appropriate for the sector.

Scope –
Elements of Proposed Core Deliverables

- **Structure**
  - □ Validate conceptual structure, and
  - □ Identify and validate composition and representation in the sector partnership
- **Roles and Responsibilities**
  - □ Define the roles and responsibilities of coordinating groups
  - □ Elements of a charter (for overall structure and sub-elements)
    - Purpose / Rules of engagement
- **Legal Framework**
  - □ Identify and review options: FACA/non FACA
  - □ Review authorities and core requirements to implement
- **Processes**
  - □ Key processes to support true "partnership"
  - □ Principles of operations

Proposed Structure



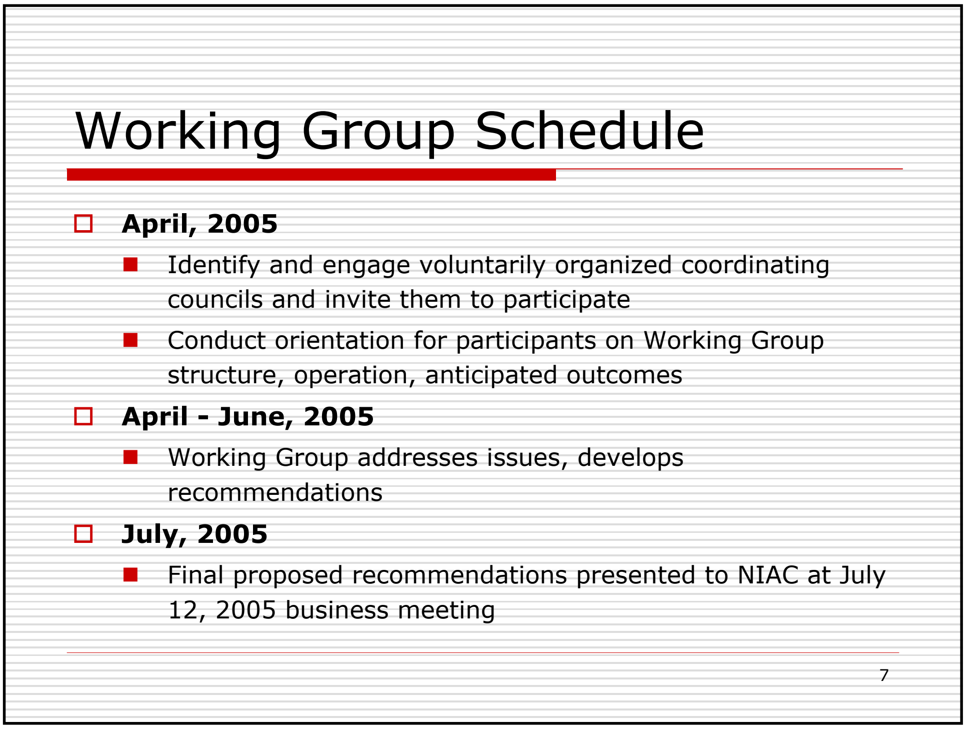
National Infrastructure Advisory Council
N I A C

NIAC
(FACA Council)
Full Membership
- 30 Members

SECTOR PARTNERSHIP
MODEL
WORKING GROUP

Working Group:
Under NIAC
Several NIAC
Members

Sector Participation
Each sector body invited to participate in the *Study Group*



Working Group Schedule

- □ **April, 2005**
  - Identify and engage voluntarily organized coordinating councils and invite them to participate
  - Conduct orientation for participants on Working Group structure, operation, anticipated outcomes
- □ **April - June, 2005**
  - Working Group addresses issues, develops recommendations
- □ **July, 2005**
  - Final proposed recommendations presented to NIAC at July 12, 2005 business meeting