NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING AGENDA

Tuesday, January 11, 2005
1:00-4:00 p.m.
Hamilton Crowne Plaza
Washington, DC

I.	**OPENING OF MEETING**	*Ms. Nancy J. Wong,* U.S. Department of Homeland Security (DHS) / Designated Federal Official (DFO), NIAC
II.	**ROLL CALL OF MEMBERS**	*Ms. 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. *The Honorable Tom Ridge,* Secretary, DHS (Invited) *Lt. Gen. Frank Libutti,* Under Secretary for Information Analysis and Infrastructure Protection (IAIP), DHS *The Honorable Robert P. Liscouski*, Assistant Secretary for Infrastructure Protection, DHS *Ms. Cheryl Peace,* Director, Cyberspace Security, Office of the Special Assistant to the President for Critical Infrastructure Protection Homeland Security Council
IV.	**INTRODUCTION AND WELCOME OF NEW NIAC MEMBERS**	NIAC Chairman *Erle A. Nye*
V.	**APPROVAL OF OCTOBER 12, 2004 MINUTES**	NIAC Chairman *Erle A. Nye*
VI.	**BRIEFING OF THE NEW DHS SECTOR PARTNERSHIP MODEL**	*Mr. R. James Caverly,* Director, Infrastructure Coordination Division, DHS

VII.	**STATUS REPORTS ON CURRENT INITIATIVES**		NIAC Chairman, *Erle A. Nye*, Presiding
	A.	**INTELLIGENCE PROCESS AND WORK PRODUCTS REGARDING CRITICAL INFRASTRUCTURES**	NIAC Vice Chairman, *John T. Chambers,* Chairman & CEO, Cisco Systems, Inc. and *Chief Gilbert Gallegos,* Police Chief, City of Albuquerque, New Mexico, NIAC Member
	B.	**RISK MANAGEMENT APPROACHES TO PROTECTION**	*Mr. Thomas E. Noonan*, Chairman, President & CEO, Internet Security Systems, Inc., NIAC Member; and *Ms. Martha Marsh*, President & CEO, Stanford Hospital and Clinics, NIAC Member
	C.	**ASSURING ADEQUATE NATIONAL INTELLECTUAL CAPITAL TO SECURE CYBER-BASED CRITICAL INFRASTRUCTURES**	*Mr. Alfred R. Berkeley III,* e-Xchange Advantage Corp., NIAC Member; and *Dr. Linwood Rose*, President, James Madison University, NIAC Member
VIII.	**REPORTS RELATED TO PAST NIAC RECOMMENDATIONS**		NIAC Chairman, *Erle A. Nye,* Presiding
	A.	**SUMMARY OF NIAC RECOMMENDATIONS BY SUBJECT AREA**	*Ms. Nancy J. Wong*
IX.	**PRESENTATION/DISCUSSION OF: CYBERCRIME AGAINST BUSINESSES – DEPARTMENT OF JUSTICE (DOJ)/DHS COMPUTER SECURITY SURVEY**		Introduction by *Mr. Patrick J. Morrissey,* Deputy Director, Law Enforcement and Intelligence, National Cyber Security Division (NCSD), Department of Homeland Security Presentation by *Ms. Ramona R. Rantala,* Department of Justice, Bureau of Labor Statistics
X.	**NEW BUSINESS**		NIAC Chairman, *Erle A. Nye, NIAC Members*
XI.	**ADJOURNMENT**		NIAC Chairman, *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Chairman Nye, Mr. Berkeley, Chief Denlinger, Ms. Grayson, Mr. Peters, and Mr. Rohde.

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

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

STAFF DESIGNEES PRESENT MONITORING PROCEEDINGS:
Mr. Muston (for Chairman Nye), Mr. Watson (for Vice Chairman Chambers), Mr. Schrader (for Governor Ehrlich), Mr. Allor (for Mr. Noonan), and Mr. Clyde (for Mr. Thompson)

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

OTHER DIGNITARIES PRESENT:
U.S. Government: The Honorable Tom Ridge, Secretary of the Department of Homeland Security (present via teleconference), Under Secretary Frank Libutti, Assistant Secretary Robert Liscouski, 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, Mr. Patrick J. Morrissey, Deputy Director, Law Enforcement and Intelligence, National Cyber Security Division, Department of Homeland Security, Ms. Ramona R. Rantala, Department of Justice, Bureau of Labor Statistics, and Ms. Nancy J. Wong, Information Analysis and Infrastructure Protection (IAIP) Directorate of the Department of Homeland Security and Designated Federal Official 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 Tom Ridge and other officials from DHS, Chairman Erle A. Nye, Vice Chairman John T. Chambers, all Council members and their staffs present and on 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, care should be exercised when discussing potentially sensitive information. Pursuant to her authority as Designated Federal Official, she called to order the tenth meeting of the National Infrastructure Advisory Council and the first meeting of the year 2005. Ms. Wong then proceeded to call roll.

II. ROLL CALL

Ms. Wong called the roll.

She 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 as the NIAC begins another year with a challenging agenda. The Council approved three sets of recommendations at the October 12th meeting. Those reports are pending transmission to the President. All reports previously transmitted to the President are currently availably for viewing on the NIAC website—www.dhs.gov/niac. Ms. Wong then turned the meeting over to Council Chairman Erle A. Nye.

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.

Lt. Gen. Frank Libutti, Under Secretary for Information Analysis and Infrastructure Protection

Robert P. Liscouski, Assistant Secretary for Infrastructure Protection, DHS

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

R. James Caverly, Director, Infrastructure Coordination Division, DHS

Chairman Nye thanked Ms. Wong and everyone in attendance. He stated the NIAC had a busy agenda. The Chairman reiterated the fact the Council reports directly and through the White House to the President, but maintains a close affiliation with Secretary Tom Ridge and the Department of Homeland Security—something the NIAC has greatly enjoyed. The President recently announced his appointment of Judge Michael Chertoff as Secretary-Designate of the Department of Homeland Security. Secretary Ridge will continue to have authority until the Senate approves Judge Chertoff. Judge Chertoff is currently a judge on the US Third Circuit Court of Appeals and has a background at the Department of Justice where he led a division of 800. He also served as US Attorney in New Jersey. Chairman Nye said Judge Chertoff certainly has a very distinguished record and is a very distinguished person.

Chairman Nye continued, saying the Council will acknowledge the loss of Secretary Tom Ridge and will express its appreciation to him when he joins the teleconference later in the meeting. Chairman Nye said he thought the Secretary had done a remarkable job under very difficult circumstances. In addition to Secretary Ridge's resignation, there are two other changes that will affect the Council directly. Both Lt. Gen. Frank Libutti, Under Secretary for Information Analysis and Infrastructure Protection, and Assistant Secretary Bob Liscouski have announced their resignations. He pointed out that this is the time in the cycle of presidential administrations when changes like these occur. Both Under Secretary Libutti and Assistant Secretary Liscouski have been stalwarts in this effort and the Council holds them in high regard. They have both served in various public service capacities, and the Council wishes them the very best. At this point, Chairman Nye turned the floor to Under Secretary Libutti for comments.

Under Secretary Libutti thanked Chairman Nye and said it had been a great honor to serve. The Under Secretary said the experience had been exciting, exhilarating, and frustrating. When he looked at the Department's leadership team—General Patrick Hughes, Assistant Secretary for Information Analysis, General Matthew Broderick, Director of the Homeland Security Operations Center, and Assistant Secretary Liscouski—he felt very positive about each of their contributions as well as the future of the Department and IAIP. Under Secretary Libutti again thanked the Council and extended his wishes for a happy new year.

Chairman Nye asked Assistant Secretary Liscouski if he had anything to add.

The Assistant Secretary thanked Chairman Nye, former Chairman Richard Davidson and Vice Chairman Chambers for their collective leadership. He stated that their accomplishments over a short period of time have been unparalleled. The DHS partnership with the private sector is thoroughly exemplified by the NIAC's achievements. He said the Council's progress over the past few years had been remarkable; something that is a testament to private sector leadership in the mission of Homeland Security. Assistant Secretary Liscouski congratulated the members for their ability to help DHS become a success. Like the Under Secretary, he said he was honored to have played a part. Under Secretary Libutti's leadership and wisdom has provided IAIP the opportunity to operate freely. At this point, Assistant Secretary Liscouski publicly thanked Under Secretary Libutti for his support and for a job well done. The Assistant Secretary thanked Chairman Nye as well and returned the floor to him.

Chairman Nye thanked both Assistant Secretary Liscouski and Under Secretary Libutti. He then introduced 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 Advisor. Ms. Peace serves very ably in the White House and as a liaison to the NIAC and had some brief comments for the Council.

Ms. Peace thanked Chairman Nye and the members for attending and participating in these Council meetings. She welcomed the members to the first meeting of 2005 and said the White House looks forward to a highly productive year. Ms. Peace also welcomed our newest members and stated that there will be an opportunity to talk further with them at a later date.

Chairman Nye said he appreciated Ms. Peace's comments as well as the assistance she provides the Council. He thought it notable the NIAC continues to get comments from DHS, the White House, and from the public about the strength, quality, and quantity of work performed. Chairman Nye said he wanted to take an opportunity to voice his appreciation for the Council's work ethic. He said it had been quite a remarkable success and he hoped it will continue.

Chairman Nye stated four of the Council's previous final reports and recommendations had been transmitted to the White House and that three more reports and recommendations were approved by the Council at the last business meeting in October. These three reports are in the process of being transmitted to the White House. More information on this will be provided later in the meeting. Chairman Nye said these reports were receiving much attention and were beginning to be implemented. Ms. Wong will report on this implementation, and it is certainly something the Council can take pride in. Chairman Nye said this work is often referenced, with both the White House and Secretary Ridge taking notice.

At this point, Chairman Nye introduced Mr. R. James Caverly, Director of the Infrastructure Coordination Division (ICD) to provide the Council with information on an important development—a new Conceptual Framework for a DHS Sector Partnership Model. Chairman Nye said this was the first public description and announcement of this model. He also stated the Council will hear from Ms. Wong later on in the meeting on the status of the NIAC's previous recommendations. She has categorized these for us. The Council will also hear a report on the Department of Justice-Department of Homeland Security computer security survey. With regards to the regular business, Chairman Nye turned the floor to Vice Chairman John T. Chambers for further opening remarks.

Vice Chairman Chambers thanked Chairman Nye and said he wanted to echo some of the previous comments. He stated the Council's counterparts and working partners from the government, Secretary Ridge, Under Secretary Libutti, and Assistant Secretary Liscouski have all been very effective by being great team players. Their direction will be sorely missed. The Vice Chairman challenged the members to maintain their quality involvement, and to leverage their staffs to enhance the end products even further. He said he anticipated working with the new officials from DHS as well as new members of the Council. He thanked Chairman Nye again and strongly encouraged DHS, the White House, and other groups to ensure the NIAC continues its steady stream of reports and recommendations to the President. It is critical these reports are relevant, and this can be assured by the government's continued candor relating to where the Council can add value and where it cannot. He concluded his comments.

Chairman Nye thanked the Vice Chairman and asked Under Secretary Libutti if he had any further comments for the group.

The Under Secretary thanked the Chairman and reiterated Assistant Secretary Liscouski's praise of the Council's leadership. He said one of the key elements he took from participation with DHS and the Council is the manner in which the word "partnership" has been successfully redefined. In the future, this new definition will be conveyed across this nation. In addition to the important work underway at DHS, he was pleased to announce that the National Response Plan (NRP) had been finalized, approved and posted to the DHS website. Hard copies of the NRP have been distributed to each NIAC member via mail and are available at this meeting. He thanked the NIAC members for their review and input—a key contribution to this effort. Under Secretary Libutti again thanked Assistant Secretary Liscouski for his leadership in coordinating the NRP. His insights and expertise were critical in ensuring a comprehensive and effective plan. The NRP established a comprehensive all-hazards approach to enhancing national domestic incident management ability. The plan incorporates best practices and procedures from incident management disciplines including:

- Homeland security
- Emergency management
- Law enforcement
- Firefighting
- Public works
- Public health
- Responder recovery
- Worker health and safety
- Emergency medical services, and
- The private sector.

The plan takes these disciplines and integrates them into a unified structure. It forms the basis for how the federal government coordinates with state, local, and tribal governments as well as the private sector in managing incidents. Additionally, the NRP establishes protocols to help save lives and protect the health and safety of the public, emergency responders and disaster recovery workers. These protocols also ensure homeland security, prevent imminent incidents including acts of terrorism, protect and restore critical infrastructures and other key resources and aid in conducting law enforcement investigations to resolve incidents.

Furthermore, the NRP assists in apprehending responsible parties, collecting and preserving evidence for prosecution, protecting property, mitigating damages and impacts to individuals, communities, and the environment as well as facilitating the recovery of individuals, families, businesses, governments and the environment. Recognizing the importance of communication and coordination with the private sector, the plan also includes a private sector annex to provide an interaction framework.

Under Secretary Libutti again thanked the members for their participation and noted it had been an honor and a pleasure to work with such a distinguished group and such distinguished leaders.

Chairman Nye thanked the Under Secretary and said the Council appreciated him very much. He asked if the Assistant Secretary had any comments.

Assistant Secretary Liscouski said the Under Secretary's discussion of the National Response Plan clearly highlights it as a key deliverable to both the White House and the nation. The Infrastructure Protection Office has submitted the interim National Infrastructure Protection Plan (NIPP) for review through the secretary to the White House for comments. These plans as well as the others have benefited from the involvement of the NIAC. This again exemplifies the tremendous public-private sector partnership DHS enjoys. The Assistant Secretary said Mr. Caverly would discuss the new model later in the afternoon. The model has a new conceptual framework for the sector partnership model, Mr. Caverly will also cover this.

Assistant Secretary Liscouski said he had reviewed the work of the three NIAC Working Groups currently in progress:

- Intelligence Process and Work Products Regarding Critical Infrastructures
- Risk Management Approaches to Protection
- Assuring Adequate National Intellectual Capital to Secure Cyber-Based Critical Infrastructures

After looking at materials developed by these working groups, he said he was extremely encouraged by the progress made to date. The issues confronted by these three Working Groups are precisely the kinds of topics the NIAC needs to address. The Assistant Secretary again thanked the members for their attendance and said he looked forward to answering any questions that might arise over the course of the meeting.

IV. INTRODUCTION AND WELCOME OF NEW NIAC MEMBERS — NIAC Chairman, *Erle A. Nye*

Chairman Nye thanked both the Under Secretary and the Assistant Secretary. He said he wanted to offer a warm welcome to three newest NIAC members. These three have been approved by the President. Chairman Nye first introduced Chief Rebecca Denlinger, Chief of the Cobb County, Georgia Fire and Emergency Services Department. Chief Denlinger comes to the Council with a very celebrated career. She began her career as a firefighter and worked her way to Chief in one of the country's larger systems. Chief Denlinger has participated in numerous fire safety, firefighting, and emergency preparedness activities and has received numerous awards both in Georgia and elsewhere. Chief Denlinger also has a history of being very active in Georgia's homeland security efforts.

The Chairman then introduced Mr. Gregory Peters, President and Chief Executive Officer of Internap Network Services Corporation. Mr. Peters has served as Internap's President and CEO since April 2002. Prior to this appointment, he held a series of positions in the communications industry including part of his career at AT&T.

Finally, Chairman Nye introduced Mr. Bruce Rohde, Chairman and Chief Executive Officer of ConAgra Foods. As the Council certainly knows, ConAgra is literally an agricultural giant. He has served as the Chief Executive and Chairman of ConAgra Foods for many years. Mr. Rohde attended Creighton University as an undergraduate and also received his Juris Doctor Cum Laude from Creighton. He is also a Certified Public Accountant. He brings a particular expertise that will be very useful to the Council.

Chairman Nye asked the three newest members of the NIAC if they had any comments.

Chief Denlinger thanked the Chairman for his warm introduction and said it was a pleasure to join the Council. She added she felt she had a great deal to offer.

Chairman Nye said the Council was grateful to count her a member.

Mr. Peters also said it was an honor to participate with this esteemed Council and he looked forward to continuing its success by contributing in any way he could. He thanked the Chairman again for the opportunity to serve.

Mr. Rohde thanked the Council and said he was pleased to join.

Chairman Nye thanked all three of the new members. He then moved on to the direct business of the meeting and asked the Council to consider the approval of the October minutes. Each member received these minutes in advance and he said he would now entertain any corrections, comments, deletions, or improvements in the minutes.

V. APPROVAL OF OCTOBER 12, 2004 MINUTES — NIAC Chairman, *Erle A. Nye*

Mr. George Conrades recommended a change to the minutes as they refer to the Working Group on Hardening the Internet. In the fourth sentence of the fourth paragraph on page 17 the draft of the minutes read "Mr. Ellis said that as a security professional he was unfamiliar with 90% of those practices," it should actually read "Mr. Ellis said that as a security professional he was unfamiliar with 90% of the publications of those practices."

Chairman Nye said this correction will be made unless there are any exceptions. Hearing no more recommended changes, Chairman Nye asked if there was a motion to approve the minutes with Mr. Conrades' change.

Mr. Alfred Berkeley moved for approval and was seconded by Mr. Donald Carty. The minutes were put to a vote and passed unanimously.

Chairman Nye then moved the meeting to Mr. Caverly's briefing on the new Conceptual Framework for the DHS Sector Partnership Model. Chairman Nye said this was the first public announcement of the new Sector Partnership Model and he was pleased it could occur at a NIAC meeting. He turned the floor to Mr. Caverly.

VI. BRIEFING OF THE NEW DHS SECTOR PARTNERSHIP MODEL

Mr. R. James Caverly, Director, Infrastructure Coordination Division, DHS

Mr. Caverly thanked the Chairman and said he wanted to discuss the evolving nature of the public sector-private sector partnership. One the purposes of this briefing is to report back to the Council how recommendations made by the Council in the Cross Sector Interdependencies and Risk Assessment Guidance Report in January 2004 have been of value and utilized by DHS. DHS believes that this model provides the framework and venue to put into practice a significant number of the Council's recommendations through a structure for sector coordination, information sharing, and enhancement of the public sector-private sector partnership. Mr. Caverly reviewed how an understanding of the Presidential Defense Directive 63 (PDD-63), President Clinton's guidance to executive agencies on organizing for Critical Infrastructure Protection, was important to understand where DHS is today on that issue. PDD-63 introduced two new mechanisms: 1) Sector Coordinators and 2) Information Sharing and Analysis Centers (ISACs). PDD-63 called for the government to appoint a sector coordinator for each critical infrastructure sector.

As PDD-63 was implemented, it became increasingly evident the government could not fully accomplish all of the goals envisioned for the sector coordinator role. The government appointing the sector coordinator stunted internal sector leadership in some sectors. Individual agencies were inconsistent in the guidance, roles, and expectations for these individuals. In effect, there was not a consistent strategy and approach across all the sectors. Additionally, the government failed to provide resources to sector coordinators who were already somewhat constrained by full-time careers on top of their own full-time, professional responsibilities to lead a sector's development of agendas for protection programs, legislation, and research and development agendas as called for in PDD-63.

Mr. Caverly said another issue emerged over time in that the agencies were not able to reach down consistently to the sector's execution levels, the owners and operators of individual facilities. Because of individual efforts by individual agencies, the sector coordinating role did not materialize as it was originally envisioned by the PDD. The position lacked the necessary cross-sector coordination across interconnected and interdependent sectors.

PDD-63 also introduced ISACs. These centers were envisioned to be the principal information sharing mechanisms between the public and private sectors and the chief distribution channel for alerts and warnings. The ISACs are also the bodies intended to develop sector-specific analysis on threats and vulnerabilities. In order to achieve these objectives, each sector was encouraged to voluntarily create an entity with adequate resources to accomplish these tasks. Several business models emerged. One of these models was a fee-for-service model and established dues for participation by subscribers. The other model was principally dependent upon individual agencies providing grants.

Both of these models presented several problems. The fee-for-service model represented an inherent barrier to entry for many individual institutions. With one notable exception, the government was unable to reach all of the participants in an individual sector. The grant model also created challenges because it was not coordinated across government agencies. Different agencies were funding different activities at different levels of effort, and the resource commitment was unequal with very different implementations and core capabilities and reach.

Given this landscape, the government is not able to connect to every participant in a sector to disseminate alerts and warnings as is its obligation. Each model was developed in relative isolation within each sector and did not provide the capability easily to share information across the public and private sectors, and many times, across sectors as well.

Mr. Caverly pointed out that President Bush's direction to his executive agencies, as contained in Homeland Security Presidential Directive 7 (HSPD-7), adopted a slightly different framework. He stated that the Directive called for the creation of a new organization to address the absence of a national organization representative of all the critical infrastructure sectors. This new group would come together in a way that made sense to each individual sector. The structure of these organizations was not to be federally directed, but rather pulled together in a manner innately sensible to each sector.

DHS has identified a Sector Coordinating Council concept, stemming from direct development of several "best practice" sectors. This concept gives government the flexibility to build a broadly inclusive framework that touches the entire spectrum of critical infrastructure and key resource (CI/KR) sectors.

Mr. Caverly noted the self-organizing process and structure of the food and agricultural sectors as an example—he said it is an extremely complex sector that begins at the farm and ends on a consumer's table. Obviously, there are numerous components that make up that sizable supply chain. He suggested that almost all other sectors also have similarly complicated components. The sector coordinating concept includes a framework that allows both DHS and the sector-specific agency to work directly with a single entity. Thus far, DHS has not been instructive in shaping these sectors and this provides for private sector initiative to build the sector coordinating councils. The core criterion is very basic, it must be representative of the sector, focused on owners and operators, and have a homeland security focus. For the sake of consistency, the senior representative of that group should be an owner-operator of the CI/KR sector, not a representative or associate of a group.

DHS recognizes that organizing a sector requires a delicate balance between system owners and operators as well as the associations representing them. The second component of the sector coordinating council involves providing a framework to support its administration and logistics so there is no barrier to participation. DHS will provide administrative resources and the executive secretariat functions necessary to support the sector, as requested. Sector participants are expected to attend the meetings and to provide the sweat equity for their products.

In conjunction with the sector coordinating council, DHS in cooperation with the sector specific agencies have also begun creating government coordinating councils, consisting of federal agencies and at times, state and local and tribal representatives, relevant to the security issues of the sector to provide interagency coordination in working with the sector coordinating council. These coordinating councils are effective forums to meet jointly and address issues. In fact, the sector coordinating council framework stems from work with the food and agricultural sector in particular.

In 2003, the White House tasked DHS, the Department of Agriculture (USDA), and the Food and Drug Administration (FDA) to cooperate in facilitating the organizing the food and agriculture sector in order to effectively engage the owners and operators of those infrastructures.

The three departments jointly convened a wide representation of the entire food supply chain, a very diverse group of institutions with wide ranging interests. Encouraged by the three departments, over the course of six months, the concept of a sector coordinating council emerged from the work of the members of the sector, reflecting the food and agriculture sector’s diversity. In the process, the sectors asked that government also put a structure in place to coordinate across government to parallel the owner and operator’s efforts. In response, the three departments led the forming of an interagency Government Coordinating Council. At the final session, the three agencies reported on the usefulness of this proposal, and DHS noted that it also replicated how the financial services sector had organized itself about a year prior. In 2002, the financial services sector established a sector coordinating council that was broadly representative of the participants in the sector. The Federal Lead Agency, the Department of the Treasury, established a similar Government Coordinating Council to encompass many agencies with equities in homeland security as well as in financial services.

DHS has examined this “best practice” model and it is the model the Department will move forward with. Mr. Caverly said that there are currently about ten other sectors that have either completed or are in the final stages of completing their sector coordinating organization. He said DHS believes this provides an effective framework to develop the kind of partnership necessary for interactions and a true partnership on to address issues involving homeland security. He asserted his belief that this is a true partnership of equals and that the two councils provide a venue for true cooperation. Both the Sector Coordinating and the Government Coordinating Councils meet independently as well as jointly for their quarterly meetings. These councils also create working groups and subgroups to carry out any specific tasks.

Mr. Caverly reminded the Council of the inherent complexity of the food and agriculture sector. To address this, the sector created sub-sector councils that allow them to group themselves in the natural groupings of the sector. This kind of flexibility is appropriate and will serve as a sound model to develop other sector coordinating councils. These councils provide mechanisms allowing a more specialized focus on specific components that differentiate these sub-groupings and yet coordinate across the entire sector as required. For this venue to be effective, it is understood that it is a venue in which to address common homeland security issues only. There are other venues for other legitimate issues that separate these groups in the normal course of their activities.

Another issue that arose in the food and agriculture model hinged on state commissioners' and local organizations' significant emphasis on first line detection, defense and response for the sector. Consequently, appropriate for the Food and Agriculture Sector, appropriate state commissioners were enlisted to participate in the Government Coordinating Council.

Mr. Caverly said as Assistant Secretary Liscouski indicated, DHS is moving forward with the NIPP. A key component of rolling out the NIPP is the creation of a National Infrastructure Protection Plan Senior Leadership Council. This council will link public-sector, private-sector, and state organizations that are comprised of state homeland security authorities. This framework not only allows DHS to operate at the execution level for homeland security on a sector by sector and program by program basis, but it also gives the department the opportunity to provide an overarching strategic framework that is necessary for the NIPP.

Mr. Caverly closed by addressing the issue of information sharing, common to both the PDD-63 and HSPD-7. The government has a responsibility to share alerts, warnings, threats, and other information with all sector participants. In March 2004, Secretary Ridge announced the Homeland Security Information Network (HSIN) as the common network by which DHS would communicate with state and local government and law enforcement. The HSIN represents a large suite of capabilities as well as a set of tools DHS has already implemented. These tools are connected to all police departments, counties, and increasingly to the emergency management community and fire departments throughout the United States.

HSIN provides a very robust communication capability and has been offered to the sectors as a way to share threat warning information. Mr. Caverly said that the Department plans to work with each sector to tailor the capabilities suite to meet each sector's unique needs and requirements. He said by providing communications resources, DHS believes it has eliminated participation barriers and helped facilitate the public-private partnership and information sharing. In doing this, DHS feels it has met substantially recommendations made by the Council last year on enhancing information sharing and analysis for all the sectors. By tailoring the HSIN capabilities to each sector's needs, DHS provides the capability to share information within a specific sector or across the various sectors, and ultimately with both the local and federal agencies.

Another issue raised in both PDD-63 and HSPD-7 is analysis capability. The government lacks the specific expertise and knowledge of exactly how all sectors operate. This knowledge is centrally located with system owners and operators. In PDD-63, the original framework centered on the government's intelligence and threat analysis. This intelligence and threat data would be analyzed by a private sector group before distribution to owners and operators.

As DHS matures and its information analysis capabilities continue to grow, a much more robust intelligence and information sharing capability will emerge. Mr. Caverly said DHS is looking to bring sector expertise into the analytical framework at the beginning of its analytical process. As a cadre of private sector subject matter experts is developed and cleared, DHS feels that it can bring in people with specific and current day-to-day operating knowledge of the system to help evaluate threat warnings and utility of information received.

Mr. Caverly stated that DHS is trying to leverage these new frameworks to satisfy the basic requirements set forth in both PDD-63 and HSPD-7. These frameworks also address one of the Council's recommendations: the ability to robustly share information with the sector and a way to apply private sector expertise to the analytical framework so that information provided to the sectors is meaningful and useful. Mr. Caverly concluded his presentation and opened the floor to questions.

Chairman Nye thanked Mr. Caverly and said it was a very thoughtful and thorough report. He asked the Council if there were any questions or comments.

Vice Chairman Chambers thanked Mr. Caverly for his report and said the guiding principles of the Sector Partnership Model reach across sectors to decision makers and also aid to put owners and operators in charge. He also congratulated the government for doing its part in the much needed Government Coordination Council. The Vice Chairman also thanked DHS for implementing the concept of an analytic fusion center with the capacity for on-call industry representatives. He again thanked Mr. Caverly for a very thorough job and anticipated continued progress. He then challenged each sector representative on the NIAC to do their part to support the implementation of this Model.

Mr. Berkeley asked if Mr. Caverly could identify each sector's sector coordinating council or key representatives for the NIAC.

Mr. Caverly said each NIAC Member will be informed on the exact structure of the sector coordinating council as it ties to their specific sector. Additionally, some connectivity between the sector coordinating council and its representation on the Council will be formed. The interaction between the members of the NIAC and the sector councils is very valuable.

Mr. Noonan echoed Vice Chairman Chambers' comments regarding the progress the Infrastructure Coordinating Division (ICD) has made in this area. He asked Mr. Caverly how this work will interact with cross sector ISAC discussions. He asked if the Council was tied into this effort and how DHS would build upon independent ISAC work.

Mr. Caverly replied that as each sector coordinating council stands up over time, each one will decide how to engage in information sharing with the government. He thought in most cases, a sector would likely do so in the form of the existing ISACs. In some cases, sectors that did not previously have ISACs showed interest in using a slightly different mechanism. The chief concern for DHS is that whatever form is chosen by the sector coordinating councils should have the sufficient breadth and depth to reach all sector members. He said that DHS does want to build upon previous successful engagement and partnership and will continue to support whatever the sector decides.

Mr. Noonan asked if DHS will support cross-sector communication efforts using secure channels.

Mr. Caverly replied that the first step is to introduce of the HSIN, both to reach all segments of the sector and also to provide cross sector reach. He stated that this will be in a protected environment. The classified environment, typically referred to as secure, will be much more difficult because of security regulations. Information sharing does need to be in a protected environment and HSIN provides this capability.

Mr. Noonan asked if there will be some kind of policy dictating how alert and vulnerability information will be disseminated.

Mr. Caverly stated that each of the sector coordinating councils has established rules of engagement relevant to each sector. Obviously, the interest and concern at the federal level is information sharing. How it is shared is dependent upon how individual sectors want to receive it as well as the general complexity of their sector. DHS will work with each sector coordinating council to build this framework. Additionally, HSIN's individual capabilities implementation will vary from sector to sector due to each sector's unique characteristics.

Mr. Noonan thanked Mr. Caverly for his response and efforts and expressed his support for the new Sector Partnership Model.

Chairman Nye thanked Mr. Caverly and said the presentation was effective and that the Council appreciated the efforts of Mr. Caverly and his colleagues and anticipated its implementation.

Chairman Nye moved to the next item on the agenda, the status reports on current initiatives. At the October meeting, the Council approved the Final Report and Recommendations of the Common Vulnerability Scoring System (CVSS) Working Group. This report is being prepared for transmission to the White House. In the best interests of ongoing maintenance, the Council needs a place to house the actual system. Vice Chairman Chambers will address this and other issues related to the CVSS.

Vice Chairman Chambers thanked the Chairman and said Carnegie Mellon University, MITRE, and the FIRST Organization have all promised proposals to house the CVSS. With the Council's agreement, Vice Chairman Chambers volunteered to participate on a Working Group with Mr. Thompson of Symantec Corporation and himself as co-chairs to recommend a housing site for the Common Vulnerability Scoring System. Vice Chairman Chambers asked Chairman Nye if this was acceptable.

Chairman Nye said that the Council strongly encourages volunteerism and he did not see any disagreement.

Vice Chairman Chambers said that the Working Group will explore the options related to providing a permanent home for tool development updates as well as helping with the integration of the Common Vulnerability Scoring System. The Vice Chairman said the Council needs a group to house the system and that groups like CERT, FIRST, and MITRE are all promising candidates. The Working Group needs to evaluate which of these potential sites is most effective in maintaining tool development, updates, and any other help on integration issues.

Mr. Carty asked Vice Chairman Chambers if any work been done to assess who would be most willing to take this on.

The Vice Chairman said Carnegie Mellon, FIRST Organization, and MITRE have all expressed interest and indicated that they are preparing proposals. If the Council approves the co-chairing of Mr. Thompson and himself, the Working Group will examine the proposals, incorporate input from DHS and make a recommendation to the Council.

Chairman Nye asked if there were any other comments.

Vice Chairman Chambers said he was unclear on the specifics of these proposals but would be willing to address this issue at the next Council meeting in April 2005.

Chairman Nye said the Council hopes an organization would find it in their best interest to be involved.

Vice Chairman Chambers said the Working Group would find the answer to this question and distribute it to each participant.

Chairman Nye thanked the Vice Chairman and said the report was solid but the CVSS needed follow up and maintenance. The location of this system will be very important, and the Council looks forward to hearing the recommendations from the Working Group. Chairman Nye thanked the Vice Chairman Chambers and turned the floor over to the Intelligence Process and Work Products Regarding Critical Infrastructures Working Group for a status update.

VII. STATUS REPORT ON CURRENT INITIATIVES

A. INTELLIGENCE PROCESS AND WORK PRODUCTS REGARDING CRITICAL INFRASTRUCTURES

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

Vice Chairman Chambers thanked Chairman Nye and introduced the Working Group's Co-Chair, Chief Gilbert Gallegos from the Albuquerque Police Department. Vice Chairman Chambers said that the Working Group represents an effort to develop a closer connection between the critical infrastructure industries and the intelligence community. He introduced Mr. Ken Watson, Senior

Manager of the Critical Infrastructure Assurance Group at Cisco Systems, Inc., to review the project and its status.

Mr. Watson thanked the Vice Chairman and began by outlining the purpose of the Working Group and its Study Group. The Working Group and Study Group wanted to ensure substantial and cohesive coordination between the intelligence community, law enforcement community, and the critical infrastructure protection community. It is imperative to have domain expertise and to address intelligence information gaps extending across all three of these communities. The Study Group believes that critical infrastructure owners and operators can provide real and substantive input to the intelligence community processes.

Mr. Watson continued by pointing out the key questions the Study Group faces:

- What can the critical infrastructure provide to the intelligence community?
- What can the intelligence community provide to critical infrastructure and is there a law enforcement aspect to both of these questions?
- How do these communities interact?
- What approaches and measures have been successful thus far?
- What are the gaps and how are recommendations made to close these gaps while ensuring information flow in all directions?

The Study Group has begun both a research study and a literature search. Additionally, the Study Group is examining current analysis, the 9/11 Commission Report, and current intelligence reform legislation and has also identified the core participants from the intelligence community, law enforcement community, and critical infrastructure protection community. The Study Group will continue to broker meetings and briefings and perform analysis.

The Study Group has already examined the Aspin-Brown Commission reports as well as other studies and will distribute a summary to the Council members very soon. With Mr. John MacGaffin's help, the Study Group must identify not only key intelligence agencies, but also key offices within these agencies that are most relevant to the critical infrastructure community to improve information exchange

In addition to NIAC principals, as members of the Critical Infrastructure community, the Study Group has also reached out to the existing Partnership for Critical Infrastructure Security (PCIS). The PCIS houses most of the current sector coordination mechanisms and also uses George Mason University as a conduit to reach other sectors. The overall goal is to reach all CI/KR sector leadership when the Study Group briefs the intelligence community or sectors so that all key players will be included. Mr. Watson said the Study Group will use Chief Gallegos and other law enforcement connections across the nation.

The Study Group will follow the steps in the National Infrastructure Protection Plan in examining what actions information enables–these seven steps include actions for both the public and private sectors. These actions include:

- Deterrence

- Prevention
- Protection
- Preparedness
- Crisis management and response
- Recovery
- Restoration.

Each of these steps requires an information flow between the public and private sectors. The Study Group will analyze this flow to determine what the gaps in both content and process are. This analysis will tie into the working group recommendations to develop processes to fill these gaps in information as required by both the intelligence community and the critical infrastructure community.

Mr. Watson continued by discussing the Study Group's timeline. The first task was to brief the NIAC on the intelligence community and was accomplished in October. During this quarter the Study Group will perform a counterpart brief for intelligence community leaders and will also read and analyze existing studies.

After this analysis, the study group will convene a core group from these communities to analyze research results and develop a draft report over the coming quarter. Developing this report is expected to take three months. Beginning in July, the Study Group plans to use two months to author the final report and to provide it for a member review. The member-vetted final report should be ready by the October, 2005 business meeting of the NIAC.

Vice Chairman Chambers asked Chief Gallegos if there was anything he wanted to add or if the Council had any questions.

Chief Gallegos said that the Homeland Security Science and Technology Directorate put together some ideas and programs originating in several cities across the country that might serve as a model for the Study Group's efforts. Chief Gallegos was not entirely sure about timelines, but that someone may know when those networks are expected to be operational so that the Study Group can begin evaluating these models' feasibility.

Vice Chairman Chambers commended Chief Gallegos on his work.

Chief Gallegos thanked him and noted that his experience suggests that with disparate treatment of information within the intelligence community, joining different information streams can sometimes be the biggest hurdle in a project.

Vice Chairman Chambers asked if there were any further questions. There were none and he returned the floor to Chairman Nye.

Chairman Nye thanked Vice Chairman Chambers and Chief Gallegos for their work and said that producing a result by the October meeting will be am outstanding result.

Chairman Nye then turned the floor to Mr. Thomas Noonan and Ms. Martha Marsh for their status report on Risk Management Approaches to Infrastructure Protection.

B. 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 the Chairman and began by saying that the Working Group has been very active and the status report would discuss the Working Group's materials, timeline, and next steps. Mr. Scott Blanchette, Director of Information Technology and Chief Information Security Officer at the Stanford Hospital and Clinics, walked through the presentation.

Mr. Blanchette thanked Ms. Marsh and Mr. Noonan for the opportunity to provide an update on the Study Group's progress. The first part of the presentation will revisit the original NIAC question to clarify what the Study Group is tasked to accomplish. In discussing the timeline, he wanted to highlight the focus areas on which the study group has been spending its time. Additionally, he asserted that he would briefly discuss initial findings and would outline next steps.

Mr. Blanchette said that at the October meeting, the NIAC tasked the Working Group to provide answers to the following questions:

- Can private sector experience with risk management and prioritization provide meaningful guidance to the President for risk management?
- Can this experience be applied to the government's national critical infrastructure planning and programs?

Current thinking suggested that the private sector had significant experience in this area based on its familiarity with volatile variables. These variables are tied into risk management and are often addressed daily. For instance, financial volatility or supply chain disruptions are cited as risks requiring mitigation.

As he said earlier, the October 2004 meeting marked the beginning of the Working Group and identified specific stakeholders. Mr. Blanchette said there have been extraordinary participation levels to date with input from sector stakeholders from finance, healthcare, technology, water, academia, construction, energy, and manufacturing as well as a significant number of ex-officio officials from DHS and other government agencies.

He said that the Study Group is still in its data aggregation phase and is in the process of continuing to collect methodologies across sectors to produce a deliverable by the July 2005 NIAC meeting. A final product should be ready for the October 2005 business meeting.

The Study Group's focus has primarily been on building a document repository that contains risk assessment methodologies on which to base analysis to formulate recommendations. The Study Group has focused on aggregating government risk management methodologies, practices, and decision models. In addition to these models, the government has also examined philosophies, albeit to a lesser degree. The Study Group has engaged in the same activities with the private sector. A key area for the Study Group over the last 30 to 60 days has been identifying commonalities and differences at a strategic level, particularly how strategic risk data is managed.

Mr. Blanchette said that the Study Group has experienced success in building out the document repository. In building this repository, the Study Group has been aware of being sensitive to proprietary information and intellectual property protection while still building a usable methodology baseline from which to work. The Study Group will continue to confront this challenge but has been successful in managing Information Technology protection while creating this repository. Additionally, a good deal of time has been spent desensitizing private sector documents so the Study Group does not risk infringing upon proprietary information protection concerns.

At an operation level, the Study Group has noticed defined commonalities, especially within sectors using similar operational risk management methodologies. Continued analysis over the next few months will identify some of the less obvious reasons for these commonalities and discrepancies. Ex-officio input from DHS has prodded the Study Group to reach out to non-traditional information sources such as academia, where researchers have conducted extensive risk management. Outreach to industry associations has also been invaluable.

Mr. Blanchette moved on to discuss the Study Group's next steps. By the April 2005 NIAC meeting, the Study Group hopes to complete baseline inventory of risk management methods and philosophies. This activity will also be completed with DHS in order to form a comparison with private sector risk management activities. The Study Group hopes to identify common trends as well as differences. At the April NIAC meeting, the Study Group will begin to release initial findings in a more formal manner. It will also identify projected deliverables. At the October 2004 meeting, the Study Group wanted to discuss a feasibility decision at the mid-point of its timeline to ensure it was staying on task. At the April meeting, the Study Group will identify a manageable scope and timeline.

At this point, Mr. Blanchette turned the floor back to Ms. Marsh and Mr. Noonan for closing comments and questions.

Ms. Marsh thanked and recognized Mr. Peter Allor from Internet Security Systems. Mr. Allor has collaborated with Mr. Blanchette.

Vice Chairman Chambers echoed Ms. Marsh's comments and said Mr. Allor and Mr. Blanchette have brought the Study Group along quickly.

Chairman Nye thanked Ms. Marsh and Mr. Noonan and asked if there were any comments or questions. When there were none, he commended the Working Group and moved to Mr. Berkeley and Dr. Rose for a status report on Assuring Adequate National Intellectual Capital to Secure Cyber-Based Critical Infrastructures.

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

Alfred R. Berkeley III, e-Xchange Advantage Corp., NIAC Member and *Dr. Linwood Rose*, President, James Madison University, NIAC Member

Dr. Rose thanked Chairman Nye. He said that after a number of organizational meetings held by the Working Group, the participants have determined it would be best to sub-divide its efforts. Mr. Berkeley has taken responsibility for chairing the Workforce Preparation Sub Group. Dr. Rose said he would comment on the Research Sub Group and Mr. Berkeley will follow with comments on Workforce Preparation.

Dr. Rose asserted that the Research Working Group has identified four goals upon which to focus its immediate attention:

- Determine whether there is a need to develop a national research agenda for cyber and critical infrastructure protection
- Determine an adequate base for this research activity
- Evaluate research products with potential time-to-market issues—these products may be affected by the unintended consequences of internet protocol policies and laws preventing rapid deployment of new technologies to market
- Examining the national research talent pool to gauge where the workforce is in comparison to the research agenda.

The Working Group is employing two methods to currently look at these topics. The first method relies upon consultation with experts in academia and industry. The Working Group has also considered whether to develop a survey to examine research issues and needs. The survey would be administered to NIAC members, but the main goal would be to identify an appropriate person in each sector and to catalogue identified research needs. Once these requirements have been identified, the Working Group can hopefully prioritize those needs.

Dr. Rose said that some groups have already been invited to provide input into the Working Group. The Working Group's agenda is to analyze survey results and summarize its work with these consultants. From these efforts, the Working Group will ultimately make recommendations to the Council. The time-to-market issues and talent pool issues have not been addressed thus far, but will be shortly. Dr. Rose turned the meeting to Mr. Berkeley for the second phase of the presentation.

Mr. Berkeley said he first wanted to address the talent pool issue. In addressing this issue, there are seven specific areas and the clear reality that the problem is on many different fronts. These seven areas are:

- Math and science competency of K-12 students ;

- Incentives specifically geared towards attracting students into technical fields
- The manner in which content related to information assurance and cyber security is delivered. Usefulness and availability of cyber security certification programs
- Timeliness of security clearances
- US educational competitiveness
- Usefulness and availability of cyber security certification programs
- Identifying other government projects to build upon.

Mr. Berkeley said that one of the main issues confronting the country is the math and science competency of K-12 students. Initially, this looks like a problem for the Department of Education. It is a huge issue, but one the Working Group should find some very specific and actionable recommendations that can make a difference.

The second area specifically explores incentives for attracting students into technical fields—particularly information assurance and cyber security. After the Soviet Union launched the Sputnik satellite in 1958, Congress passed the Defense Education Act. Currently there is a similar initiative in the Department of Defense, and the Working Group will incorporate some of these activities into its results.

The Working Group also wants to examine the way educational content, specifically information assurance and cyber security, is delivered in curricula. Is the curricula studied worth the time and energy students put into it and does it adequately reflect the needs of the security community now, the information assurance and cyber communities?

Additionally, the Working Group is studying the usefulness and availability of cyber security certification programs as well as the efficacy of an existing program called Cyber Corps—now called Federal Cyber Service Scholarship for Service. Mr. Berkeley said the Working Group finds itself repeatedly returning to the question of US educational competitiveness and has procured some interesting statistics and testimony in order to generate actionable recommendations from these observations.

Finally, the Working Group is looking at the issue of the timeliness of security clearances and will add on to work being done in other parts of the government.

Mr. Berkeley said that this Working Group's methodology is similar to some of the other Working Groups' methodologies. It has identified the topics and coordinated the assistance of a series of experts in these areas to discuss their observations. The Working Group is trying to come up with actionable and innovative solutions without becoming caught in an endless policy discussion. It is concentrating on identifying successful programs—mostly small pilot programs. These programs will be successful as well as scalable.

Mr. Berkeley proceeded to provide the Council with examples of the programs. Mr. Bill Schmidt is a professor at Michigan State University and represented the United States in the Third International Math and Science (TIMS) Survey. This survey indicated American children are in the 75th percentile in fourth grade, the 50th percentile in eighth grade, and the 5th percentile in 12th grade. Mr. Schmidt has spent a tremendous amount of time examining the reasons behind this performance, comparing American curricula to the curricula of the countries and schools whose students were far more advanced. He believes American educators are focusing on the breadth of subject as opposed to exploring them in more complete detail while their foreign counterparts are teaching real depth in academic subjects. This observation will form the basis for a recommendation and we are going to build on that in our recommendation.

The Working Group has also brought in Nobel Laureate Mr. Leon Lederman, former Director of the Fermi Lab. He has discussed his efforts to transform the 100-year old American model of teaching biology first, chemistry second, and physics in the third year. He has been successful in reversing this curriculum in over 100 schools. The new program places Physics first, as a prerequisite to understanding Chemistry, which itself is a prerequisite for comprehending Biology in a modern world. He has encouraged the Working Group to consider how a fairly simple shift of sequence can produce fairly profound results.

The third example comes from input provided by the National Association of Manufacturers. Former Michigan Governor John Engler is the Association's new CEO. Ms. Phyllis Eisen also works at the Association and has developed and implemented a series of low-risk, self-testing modules. Any child can take this test, it is on the web at www.getsmarter.org and there have been over one million children who have participated just to see where they stand. There are no names or scores kept and the test tells the student what they know or do not know in comparison to other children in their age group in forty countries around the world.

These are three specific and powerful examples of witnesses and programs leading to actionable results. He said the Working Group has had good conversations with the Department of Education and it is crucial to build practical solutions based on what is possible. The Working Group's next round of discussions will include Mr. Chris Dougherty and Dr. Diana Gant. Dr. Gant is responsible for the Cyber Corps Program and Mr. Dougherty is responsible for the Reading First initiative in the No Child Left Behind Act.

Additionally, it is important to attract and keep students in technical fields, particularly as they relate to cyber security and information assurance. The Working Group will build on some National Science Foundation grants and previous work. It will explore initiatives like the National Defense Education Act. The Working Group is also fortunate to have Mr. Ken Watson and Cisco Systems involved. Mr. Watson has been terrific and he and his colleagues have provided valuable insights on just-in-time education over the web and on the role of scholarships.

Mr. Berkeley said that the Working Group will also work with a National Science Foundation grant team at SUNY-Buffalo to examine what it takes to keep women and minorities in math and science. There has been a 40% drop in the last two years of the number of women participating in some of the cyber security courses. This is something that does not make sense and requires investigation as well as a subsequent recommendation.

Mr. Berkeley went on to address the role of the Cyber Corps program—there is a question as to whether or not participants are actually able to get jobs. The Working Group will look into this issue. It will also build on Mr. Schmidt's insights. There are many certification programs in Infrastructure Protection and they serve an extremely useful and important role. These programs again allow the opportunity to build on something that is already working.

The last item on the list addresses the timeliness of security clearances. The Working Group will build on the National Academy's program administered by the Center for Secure Information Systems (CSIS). Mr. John Hamray will help digest some of these study results. The ability to get security clearances in a timely fashion is an overarching workforce issue. The Working Group will probably return with a finished work product at the October 2005 meeting although it cannot firmly commit to that deadline quite yet. Mr. Berkeley turned the floor back to the Chairman.

Chairman Nye said he appreciated the Working Group's application of risk management to the expected completion date. He stated that Dr. Rose and Mr. Berkeley had put forth a strong presentation and asked the Council if there were any questions or comments.

Dr. Rose requested a moment to make an appeal to the Council to expand the membership of the Working Group that is addressing the research topic. There is already a solid representation of educators in the Working Group but it would benefit from the addition of members from the business community. He said he hoped that some of the members would consider placing someone from their organizations on the research topic.

Chairman Nye said Dr. Rose had made a strong point, as there are a number of members with capabilities in this area and whose assistance would be greatly appreciated. He asked Mr. Berkeley if he had anything further to add.

Mr. Berkeley said the Working Group does need more help and specifically needs people from industry to help.

Mr. Noonan said he thought this presentation was a terrific step forward and that the Council appreciates the Working Group's hard work. He said that he has previously worked with former astronaut and long-time NASA member Sally Ride to support her science club that specifically focuses on middle school science and math skills for young women. He said he would assist the Working Group if they were interested in contacting her. She has had tremendous success through her work and might be a great resource to this effort.

Mr. Berkeley thanked Mr. Noonan and said he would follow up with him after the meeting.

Mr. Craig Barrett said that many Council members have been deeply involved in this effort. He reiterated Mr. Noonan's endorsement of Ms. Ride. The science talent search and science and engineering fair are also happy to participate. He cautioned that there are many people working in this space already and there is the possibility for an immense amount of effort duplication.

Chairman Nye recognized the potential for effort duplication but said the White House had raised this as a possibility at the beginning of the Working Group and it is something the Council will keep in mind. He asked if there were any other questions or comments.

Chairman Nye said that the Council will have an opportunity to undertake some more projects this year and the White House is vetting other potential ideas. He encouraged the new members to bring forward ideas worthy of consideration.

Chairman Nye said the Council now would listen to a few reports on the reception of its work. He turned the floor to Ms. Wong.

VIII. REPORTS RELATED TO PAST NIAC RECOMMENDATIONS

NIAC Chairman *Erle A. Nye*
Presiding

A. SUMMARY OF NIAC RECOMMENDATIONS BY SUBJECT AREA

Nancy J. Wong, U.S. Department of Homeland Security (DHS) / Designated Federal Officer, NIAC

Ms. Wong thanked the Chairman. At the last meeting, the Council requested that the NIAC Secretariat summarize the Council's recommendations by subject area. This was not an easy task because the Council is incredibly productive and has delivered a large number of highly regarded studies over a very short period of time. These reports and recommendations are now used as references by other studies that are being done by other very prestigious groups.

This Council has submitted four reports and three independent recommendations. One of these was a recommendation around Internet Protocol Version 6 (IPv6), which was delivered before many members joined. This particular study, as recommended by the Council, is now being completed in draft form by Department of Commerce and will be made available to this Council for review in the future.

In addition to the four reports already delivered to the White House, the Council has approved three reports soon to be delivered to the President—Final Report and Recommendations on Hardening the Internet, Final Report and Recommendations on the Common Vulnerability Scoring System, and the Final Report and Recommendations on the Prioritization of Cyber Vulnerabilities.

Ms. Wong indicated that these recommendations' general themes include.

- Education
- Awareness and outreach
- Identifying and encouraging the use of best practices
- Interdependency analysis
- Internet dependencies
- Information sharing
- Promoting consistency and commonality of technology management procedures, analysis, and tools

- Empowering law enforcement and security policy enforcement, emergency situation planning and management, and policy and regulatory framework reviews.

This is a very wide-ranging set of themes, but the recommendations are adding to the bodies of knowledge and understanding for issues the NIAC has chosen to take on. As a result, the Secretariat is working with the White House to organize the Council's recommendations into themes and put a process in place to regularly review their disposition, progress and report back to the Council. Today's report by Mr. Caverly represents an example of that periodic review and report to the Council, reflecting the utility of the Council's recommendations.

The very first report on Cross Sector Interdependencies Risk laid out the landscape of the sector coordination responsibility. The conceptual framework for the Sector Partnership Model reflects much of what was recommended in that report. In future meetings, she said that continuing progress reports will be provided. She then asked if there were any questions or comments.

Vice Chairman Chambers thanked Ms. Wong and asked if there was a way to formalize a regular implementation.

Ms. Wong said the Secretariat had initiated the systematic process but needs to formulate a standard operating procedure in addition to the conceptual process agreed upon with the White House. The Secretariat will proceed with this implementation over the next few weeks to provide the Council with a periodic snapshot.

Chairman Nye thanked Ms. Wong and asked if there were any further questions or comments for Ms. Wong. He said he was pleased that the White House is so excited about the Council and is committed to reviewing the implementation of these reports and providing quarterly feedback.

Chairman Nye then introduced Mr. Patrick Morrissey, Deputy Director for Law Enforcement and Intelligence of the National Cyber Security Division (NCSD) for DHS to present relevant and helpful material.

IX. PRESENTATION/DISCUSSION OF CYBERCRIME AGAINST BUSINESSES – DOJ/DHS COMPUTER SECURITY SURVEY

Introduction by Mr. *Patrick J. Morrissey,* Deputy Director, Law Enforcement and Intelligence, National Cyber Security Division (NCSD), Department of Homeland Security

Presentation by Ms. *Ramona R. Rantala,* Department of Justice, Bureau of Labor Statistics

Mr. Morrissey thanked Chairman Nye, Vice Chairman Chambers, Assistant Secretary Liscouski, and the Council members for providing the time to present this initiative. He said there are many cyber surveys but there still is confusion around being able to definitively determine whether a problem is being remediated or worsening. The government is awash with anecdotal evidence but little scientific or verifiable evidence. Among other things, this initiative is targeted at 36,000 businesses across all sectors of the United States. It is designed to identify security trends, estimate incidence, prevalence, and consequences of computer crime in the private sector, including critical infrastructure. It is designed to be the first statistically relevant survey of this topic in the world. NCSD hopes it will become an annual survey and replace the numerous current surveys. The results will be of great benefit both to private industry and the government. At this point, Mr. Morrissey introduced Ms. Ramona Rantala from the Department Justice's Bureau of Statistics.

Chairman Nye welcomed Ms. Rantala.

Ms. Rantala thanked the Council and said survey development began in the summer of 2001. Before explaining the pilot, she wanted to present the Council with the array of current surveys being distributed throughout the nation. There are a few data sets at a national level providing concrete numbers, all of which are conducted by the Bureau of Justice Statistics with some assistance from the Federal Bureau of Investigation (FBI). Other data sets such the Computer Security Institute have an annual survey with their members but the data is not nationally-representative.

The data sets the Bureau of Justice Statistics has conducted in the past have had very little to do with cyber security or cyber crime: The National Prosecutors Survey, last collected in 2001 had only one relevant question to each of the 2,300 nationwide prosecutors' offices. A question was posed asking if they had prosecuted any cases of cyber crime, which types, and what the results were. The largest offices have a million or more constituents within their jurisdiction and consequently have handled the largest share of these prosecutions. There are approximately 200 medium-sized prosecutors' offices and the remainder of these offices are either small scale or part-time. Ninety-eight percent of all large prosecutors' offices prosecuted at least one case of some type of cyber crime.

Ms. Rantala asserted that the Federal Justice Statistics Program examines different areas. For instance, the bureau has tracked civil cases over the past few years with respect to intellectual property theft. Since 1999 there have been over 8,000 cases of intellectual property theft in each of those years. This survey does not discern whether the victim is an individual or a business. It also criminally prosecutes intellectual property cases, though they are not as common—there were 400 in 2002, half being copyright infringement cases.

Ms. Rantala said that the National Incident Based Reporting System, part of the FBI's uniform crime reports, and is voluntarily submitted by individual police agencies. There are currently about 17,000 police agencies, sheriffs' offices, and police departments nationwide. In 2002, about 4,200 of those submitted detailed incident-based data to the FBI. In 2001 there were nearly 7,000 victims of computer crime that were reported to a police department participating in this program. Thirty-three percent of all victims are private businesses, government agencies, and the bulk of them are private industry or financial institutions. There were about 19,000 crimes committed using a computer. The most common types of crime reported to the police in this data were forgery, 26% of the businesses reporting were victims of forgery, 20% were victims of fraud, 4% were victims of embezzlement, and the others were different kinds of theft and vandalism.

The Computer Security Survey is trying to fill this gap. Beginning in 2001, the bureau devised a questionnaire and sent it to 500 businesses. This questionnaire was a feasibility test to see if data was available and if companies would be willing to provide information. Of the 500 businesses sampled for the pilot test, 208 responded— a 42% response rate. The bureau categorized the responders by size: companies with less than 1,000 employees had a 59% response rate. Larger companies with 1,000 or more employees were less able or willing to provide this information, only 28% filled out the questionnaire. Unfortunately, these firms have the most impact on statistics as larger companies are more likely to be victimized and, thus, impact the economy.

Chairman Nye asked Ms. Rantala why larger organizations were less responsive.

Ms. Rantala said the bureau performed a post-survey evaluation and 82% of the larger companies said they would not take voluntary surveys. They added that if the survey had been mandatory, they would complete them and provide the results.

Chairman Nye asked if the bureau had the capability to do anything other than voluntary surveys.

Ms. Rantala said this would take an act of Congress to make the survey mandatory. DHS and DOJ would prefer to keep it voluntary. If after the first year or two of the full-scale survey, there are not enough responses to obtain meaningful results it is possible other options would be explored.

Chairman Nye said the bureau might be able to leverage the Sector Coordinating Councils to encourage these organizations to participate.

Ms. Rantala responded that this was a wonderful idea. The bureau had considered contacting the ISACs and trade associations, but the more sector leaders on board in the beginning will boost the chances for a successful survey.

She continued, saying of the 208 responding companies, 95% used computers. The only ones not using computers were very small companies with fewer than 10 employees. Of those using computers, nearly 75% were victimized by some type of computer crime or computer security incident. Computer viruses were the most common. Of the 147 companies with at least one incident in 2001, there were 8 victims of embezzlement, 17 of fraud, and 12 of proprietary information theft. Of those same 147 victims, 89% had more than one attack. These attackers have been able to strike fast enough to beat any new or upgraded defenses.

Ms. Rantala said the survey expects to find a pattern in these attacks and to estimate losses from cyber crime. Right now, no national data exists with these kinds of statistics. There should be more data on what kinds of losses occur. Of the 147 companies with some kind of computer security incident, 100 of them provided data on their estimated losses, $61 million in one year:

- Fraud accounted for $18 million

- Viruses cost companies $10 million to recover and another $12 million in other losses,
- Denial of service counted $7 million in recovery costs and another $7 million in losses.

These figures are large, especially when one considers the fact that this is from only 100 companies. The numbers will probably be far higher if there was an exhaustive nationwide survey.

Ms. Rantala outlined responses to additional questions:

- 83% of companies subject to a computer attack reported down time
- Two percent reported no down time whatsoever
- 15% did not respond either way.

The survey also asked if companies reported their most significant incident to authorities. Theft was most reported to the police, Computer Emergency Response Team (CERT), or an ISAC. However, very few companies reported computer attacks to external authorities. The FBI is only informed on a very small percentage of what really is occurring. Many companies consider this as a cost of doing business.

She said there were also a number of questions on safeguards against intrusions. The bureau sought to know the kinds of infrastructure, networks, and modes of access companies have. In addition, the survey asked what kinds of computer security technology each company has and what kinds of security practices they incorporate. The bureau is hoping to use this data to look at points of vulnerability. The theory is if you contract computer security out to another company than that may be just one more avenue of vulnerability than if it was in-house.

Ms. Rantala said the bureau anticipates a full scale survey incorporating all the types of infrastructure and security practices. Many Chief Information Officers said it would be helpful to take this kind of information to their President and highlight vulnerable, weak areas.

The 2004 Computer Security Survey joins DHS and DOJ and is the first the first nationally-representative study among US businesses. It has been revised based on the 2001 pilot results and has been reviewed and vetted by the participating businesses as well as the FBI, the Economic Security Working Group, the Electric Power ISAC, and the President's Information Technology Advisory Committee. She asked the Council to review the survey and provide feedback if there are additional data points needed, other products, or any other type of analysis that it would like to see when the final results are returned.

Ms. Rantala said that the bureau is currently testing and finalizing the changes so it is not too late to make suggestions. The survey will be fielded live this spring and will hopefully generate preliminary results by the end of the year. There must be enough responses to have meaningful answers before any kind of preliminary data analysis is done. After 12 to 15 months, the absolute final results should be ready, including:

- National estimates
- Standard errors are associated with those
- Computations that need to be done.

Results will include the prevalence and types of computer security incidents, points of vulnerability, monetary losses, identity of the offenders, and a classification of the attack.

Mr. Berkeley said this survey may really assist the Common Vulnerability Scoring System Working Group and Internet Hardening Working Group.

Chairman Nye agreed and told Ms. Rantala she would be put in touch with these Working Groups following the meeting. He asked Ms. Rantala if she wished to conclude her presentation.

Ms. Rantala closed by saying any insights and recommendations the Council are most welcome and the bureau would keep the Council informed on the progress of this survey.

Chairman Nye thanked Ms. Rantala and asked if there were any questions or comments.

Mr. Conrades said he would be interested in having them include questions that had to do with the effectiveness of the implementations on security and technology. He added another important piece of information would be to know the financial cost of these implementations.

Mr. Peters asked Ms. Rantala if she knew the percentage of attacks that were internally generated versus externally generated attacks.

Ms. Rantala replied that embezzlement was almost all internally generated.   Computer attacks tended to be external. Fraud and theft were both internal and external.

Mr. Peters said he was curious to know whether the Sarbanes-Oxley legislation is helping to address any of these internally generated issues. This is a very extensive requirement.

Chairman Nye said he thought this was a good starting point on the discussion of security and it relates to Dr. Rose and Mr. Berkeley's presentation earlier. One of the most basic elements is training people to write secure code at the university level as opposed to trying to fix issues after the fact. Secondly, the Council itself struggles with the same problem just presented, that people do not give up data very easily. He encouraged the members to find a way to maintain focus and add value to the Council. He asked if there were any further questions or comments.

Chairman Nye said he appreciated Ms. Rantala's work. He said the survey will hopefully be of service to the Council and the private and public sectors in general.

Chairman Nye said the NRP had been distributed and the NIPP is in the approval process.

X. REMARKS FROM THE SECRETARY *The Honorable Tom Ridge,* Secretary, DHS

At this point in the meeting, Chairman Nye introduced Secretary Tom Ridge, who was participating in the meeting by teleconference.

Chairman Nye thanked the Secretary for joining the meeting and said the Council appreciated his leadership. It has enjoyed the opportunity to follow and work with the Secretary. He turned the floor to Secretary Ridge.

Secretary Ridge thanked Chairman Nye and welcomed Chief Denlinger, Mr. Peters, and Mr. Rohde to the Council. The National Infrastructure Advisory Council does substantive, relevant work. The Secretary said that one of the notions he will reaffirm with his successor, Judge Michael Chertoff, is the value of this organization and how closely it works with DHS. Secretary Ridge said he was confident that the relationship between Secretary Chertoff's leadership team and the NIAC will be strong.

Secretary Ridge said that many extraordinary things have been accomplished over the past few years, but the work will never end. It is still the Department's responsibility to integrate its efforts with the rest of the country as well. He added that the Council's role over the next few years will be to work with the NIPP to identify critical pieces of infrastructure, assess vulnerabilities, develop protection plans, and assess the risk management environment. This is where the private sector and the NIAC have such an incredibly important role.

Secretary Ridge said there had been an article in the *USA Today* suggesting DHS had lost its way when it produced a list of more than 80,000 infrastructure pieces that must be reinforced. Under the leadership of Assistant Secretary Liscouski and Under Secretary Libutti, DHS went into individual states and urban areas to determine what was deemed critical infrastructure. As the Council might imagine, it proved to be a formidable task to determine what are considered legitimate targets, hard targets, soft targets, or items not warranting inclusion on the critical infrastructure protection list. There was an internal decision to include what these sources considered critical. DHS is very mindful the list is very large but still must collect data points to begin a working list. Secretary Ridge said work to protect critical assets is ongoing, and the Council will have a critical role to play. He said he would reiterate the need to involve DHS' internal organization down to the regional level with Secretary Chertoff. This evolution to a regional structure will enhance the interaction between the department and private sector. There are many benefits to the country as well as to DHS if a regional structure is in place.

Secretary Ridge said one of the pilot projects with a bright future is the extension of the Homeland Security Information Network (HSIN) down to the counties, local governments, organizations, and corporations with critical infrastructures. DHS will continue to push forward for regional organizations to more closely work with organizations at those levels. He said he was confident he would be able to build intelligence and information sharing responsibilities with the assistance of the Council.

One of the current challenges now is the Interim National Infrastructure Protection Plan (I-NIPP). HSPD-7 gave DHS subject matter responsibility and accountability for Critical Infrastructure Protection but designated specific responsibilities in this realm to the Departments of Agriculture, Health and Human Services, Energy, Defense, Interior, Treasury, and agencies like the Environmental Protection Agency (EPA). Some of these departments' contributions to the broader package were not as complete or comprehensive as DHS would like. DHS is working with those agencies to produce a final document where the presentations are at the same level of specificity and quality.

The Secretary reiterated his personal gratitude to the Council. He thanked them for their service to the country and their work with the department through the NIAC. He stated it had been a pleasure getting to know and working with them to deal with a very complex and difficult post-9/11 world. It is important to remember the notion that security, homeland security and economic security are inter-related. One cannot stand without the other. He said the Council helps to maintain this balance, and he thanked them again for their contributions.

Chairman Nye thanked Secretary Ridge and said he spoke for everyone on the Council by stating he appreciates the Secretary's great public service. He set DHS on a noble course and had clearly helped enhance the security of this nation. He extended the Council's respect, admiration, and appreciation.

Chairman Nye then concluded the meeting and asked if any members had any comments regarding new business.

XI. NEW BUSINESS *Chairman Erle A. Nye*; NIAC Members

Chief Gallegos asked if there would be any updates on clearance statuses.

Ms. Wong described the process is in place and agreed to inform each member as to the status of each of their clearances.

XII. ADJOURNMENT *Chairman Erle A. Nye*

Chairman Nye thanked all those participating via teleconference and said the next meeting will be at 1:30p.m on April 12th, 2005 at the National Press Club in Washington. He noted that those who could not physically attend could join in via telephone. He encouraged the working groups to continue their work. He said that this work was essential to the Council's progress. He again thanked the members and adjourned the meeting.

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

By: ______________________ Dated: 4/12/05
Erle A. Nye, Chairman

ATTACHMENT A:
Status Report on the Intelligence Process and Work Products Regarding Critical Infrastructures

NIAC Intelligence Coordination Working Group

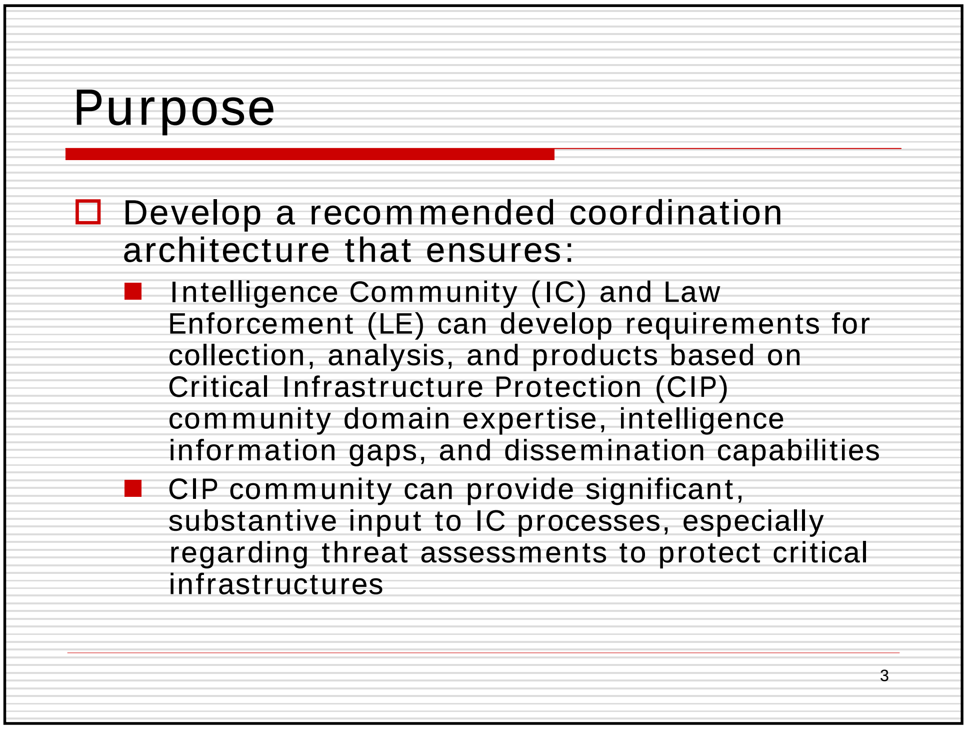
Status Report
January 11, 2005

John Chambers
President & CEO
Cisco Systems, Inc.

Gilbert Gallegos
Chief of Police
Albuquerque, NM

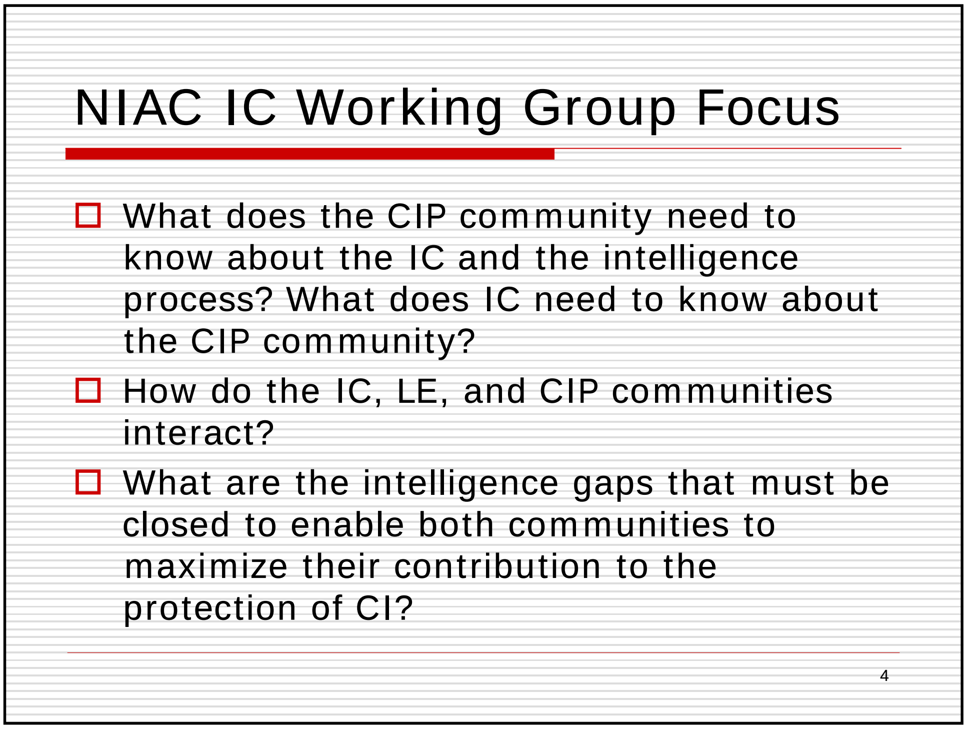
To Review……

- □Purpose
- □Working Group Focus
- □Current Actions



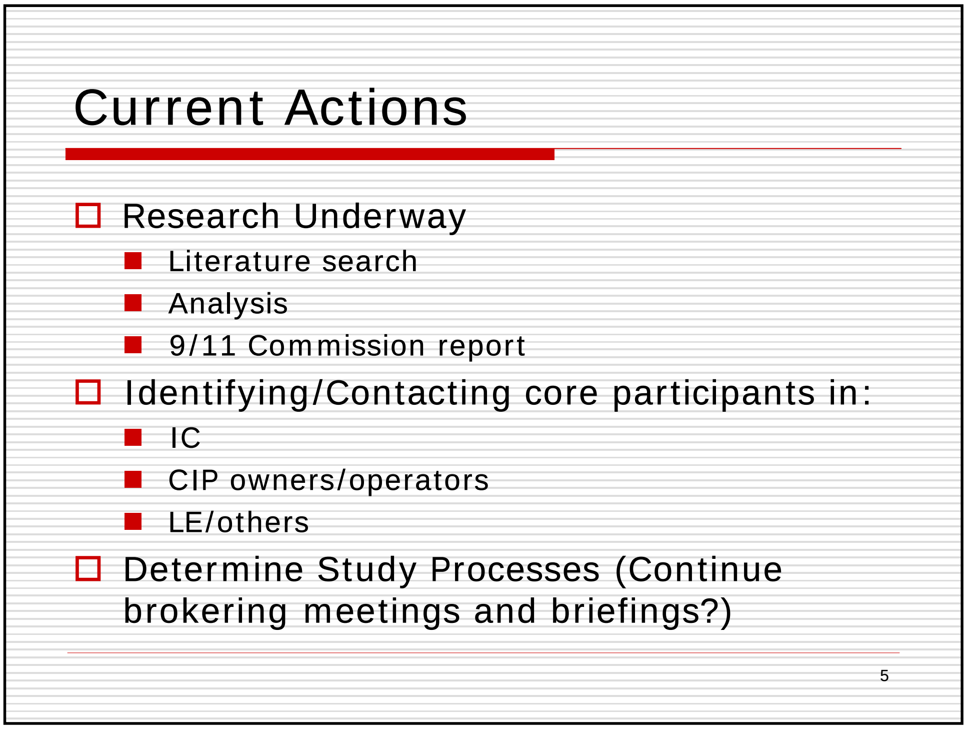
Purpose

- □ Develop a recommended coordination architecture that ensures:
  - Intelligence Community (IC) and Law Enforcement (LE) can develop requirements for collection, analysis, and products based on Critical Infrastructure Protection (CIP) community domain expertise, intelligence information gaps, and dissemination capabilities
  - CIP community can provide significant, substantive input to IC processes, especially regarding threat assessments to protect critical infrastructures



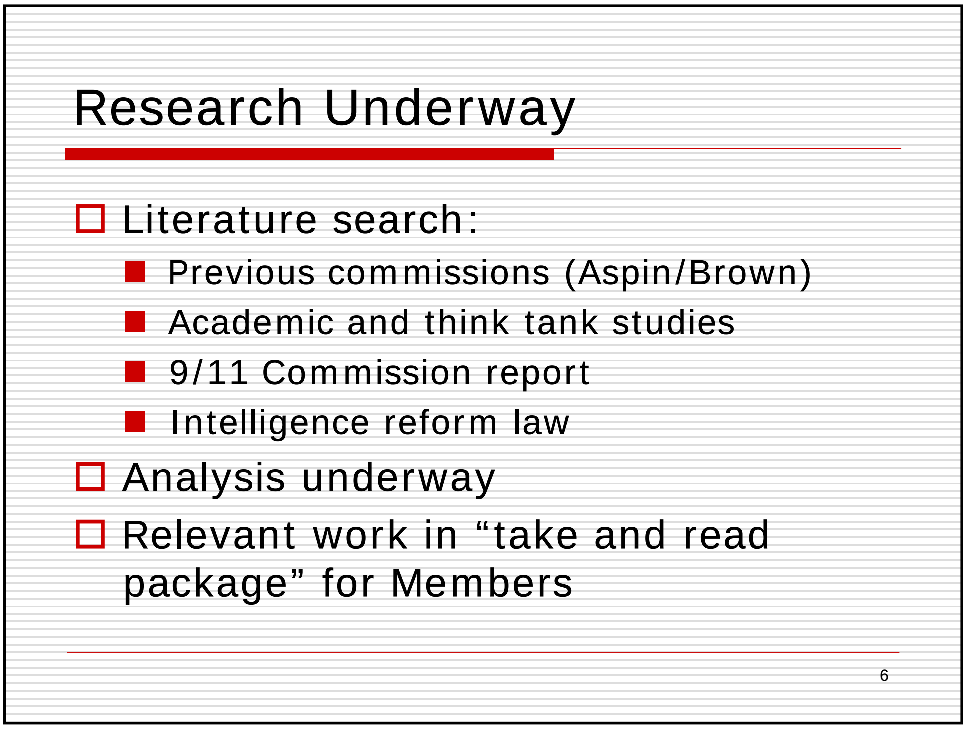
NIAC IC Working Group Focus

- □ What does the CIP community need to know about the IC and the intelligence process? What does IC need to know about the CIP community?
- □ How do the IC, LE, and CIP communities interact?
- □ What are the intelligence gaps that must be closed to enable both communities to maximize their contribution to the protection of CI?



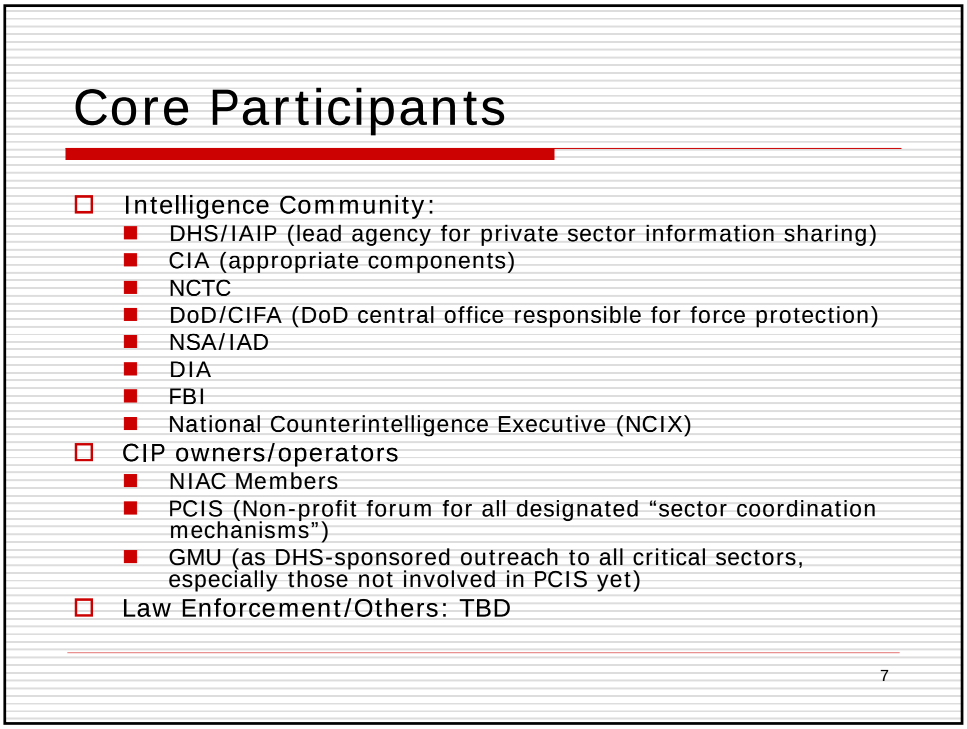
Current Actions

- □ Research Underway
  - Literature search
  - Analysis
  - 9/11 Commission report
- □ Identifying/Contacting core participants in:
  - IC
  - CIP owners/operators
  - LE/others
- □ Determine Study Processes (Continue brokering meetings and briefings?)



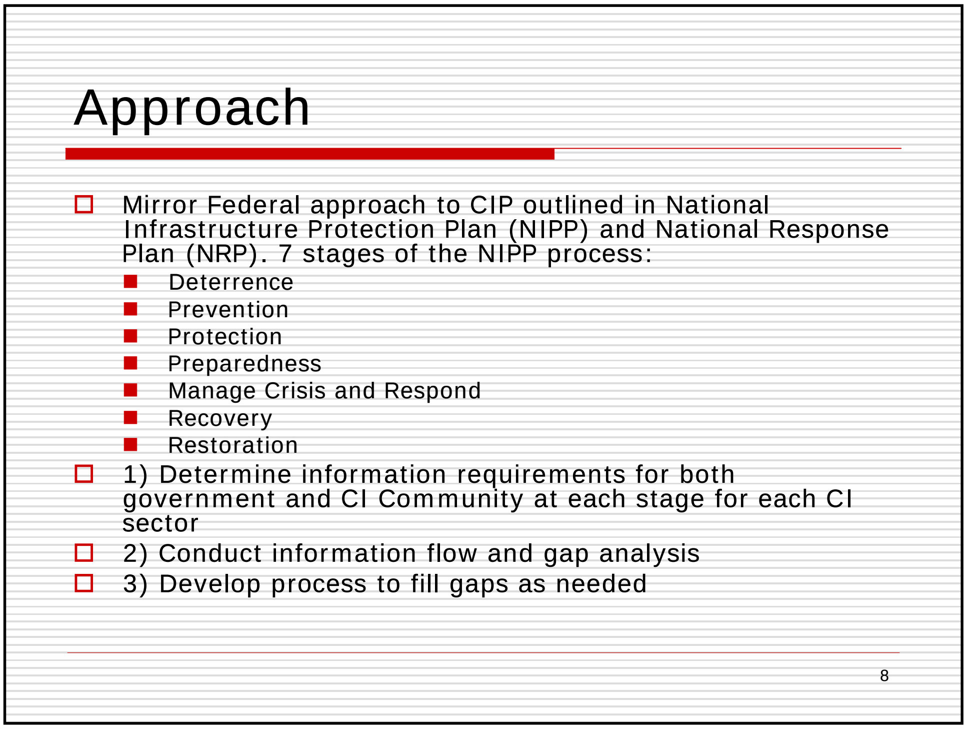
Research Underway

- □ Literature search:
  - Previous commissions (Aspin/Brown)
  - Academic and think tank studies
  - 9/11 Commission report
  - Intelligence reform law
- □ Analysis underway
- □ Relevant work in “take and read package” for Members



Core Participants

- □ Intelligence Community:
  - DHS/IAIP (lead agency for private sector information sharing)
  - CIA (appropriate components)
  - NCTC
  - DoD/CIFA (DoD central office responsible for force protection)
  - NSA/IAD
  - DIA
  - FBI
  - National Counterintelligence Executive (NCIX)
- □ CIP owners/operators
  - NIAC Members
  - PCIS (Non-profit forum for all designated “sector coordination mechanisms”)
  - GMU (as DHS-sponsored outreach to all critical sectors, especially those not involved in PCIS yet)
- □ Law Enforcement/Others: TBD



Approach

- □ Mirror Federal approach to CIP outlined in National Infrastructure Protection Plan (NIPP) and National Response Plan (NRP). 7 stages of the NIPP process:
  - Deterrence
  - Prevention
  - Protection
  - Preparedness
  - Manage Crisis and Respond
  - Recovery
  - Restoration
- □ 1) Determine information requirements for both government and CI Community at each stage for each CI sector
- □ 2) Conduct information flow and gap analysis
- □ 3) Develop process to fill gaps as needed

Timeline

□ Brief NIAC on IC (complete Oct 2004)

□ Brief IC on CIP community and needs (first quarter 2005)

□ Read/analyze existing studies (first quarter 2005)

□ Convene core group for analysis/recommendation development (Apr 2005)

□ Develop recommendations/write report (Jul 2005)

□ Final report (Oct 2005)

Discussion

□ Questions?

ATTACHMENT B:
Status Report on Risk Management Approaches to Protection

Risk Management Approaches to Protection

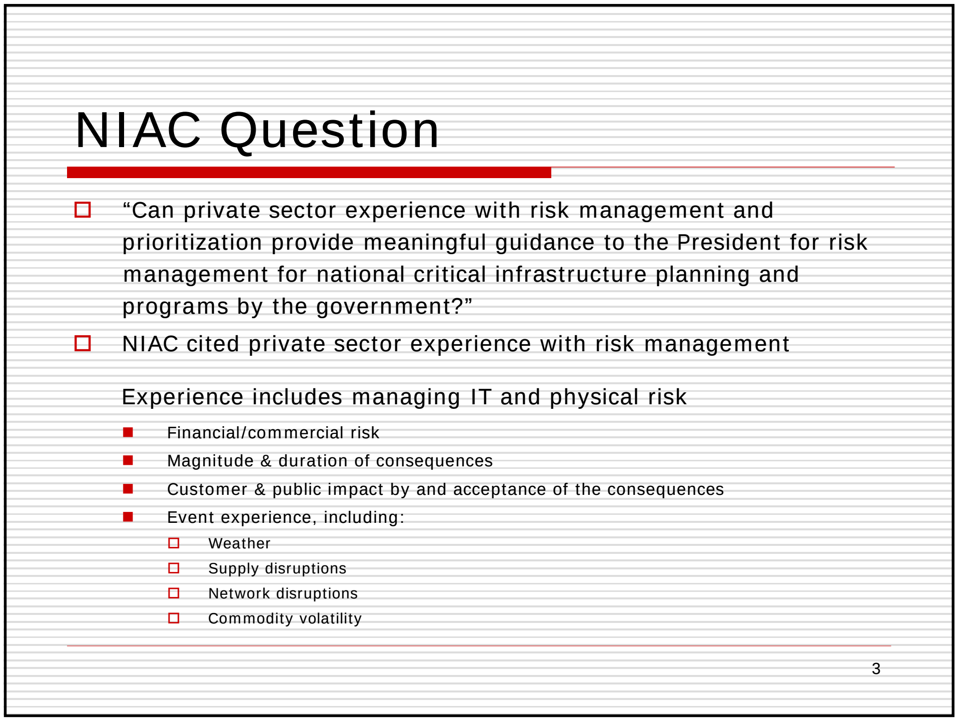
January 2005

Martha Marsh
President & CEO
Stanford Hospital and Clinics

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

Agenda

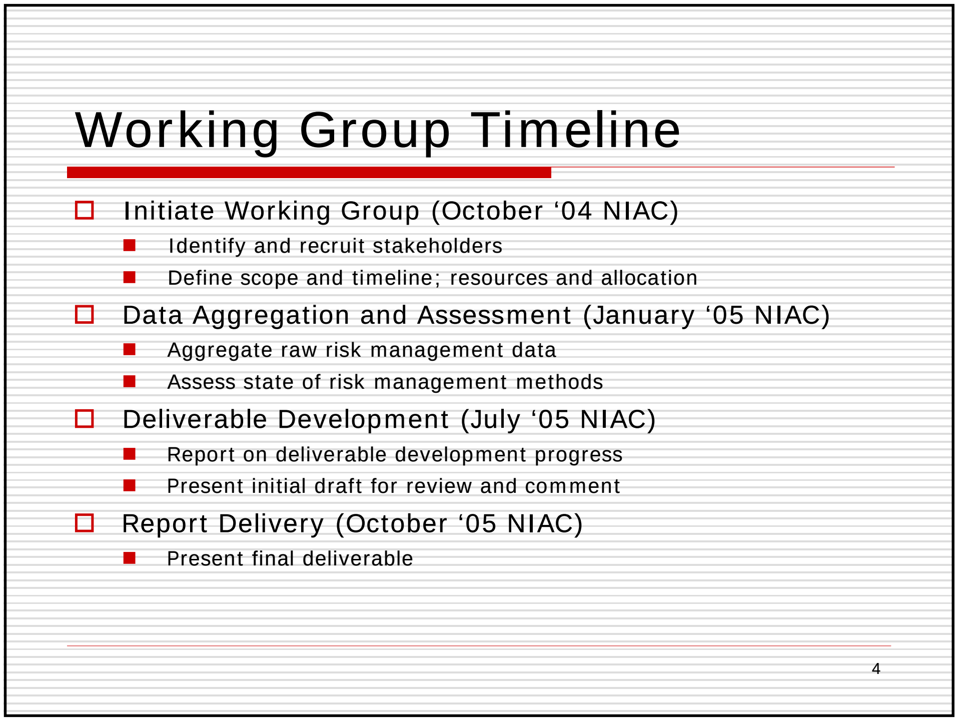
- □ NIAC Question
- □ Working Group Timeline
- □ Working Group Focus
- □ Initial Working Group Findings
- □ Next steps
- □ Discussion



NIAC Question

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

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



Working Group Timeline

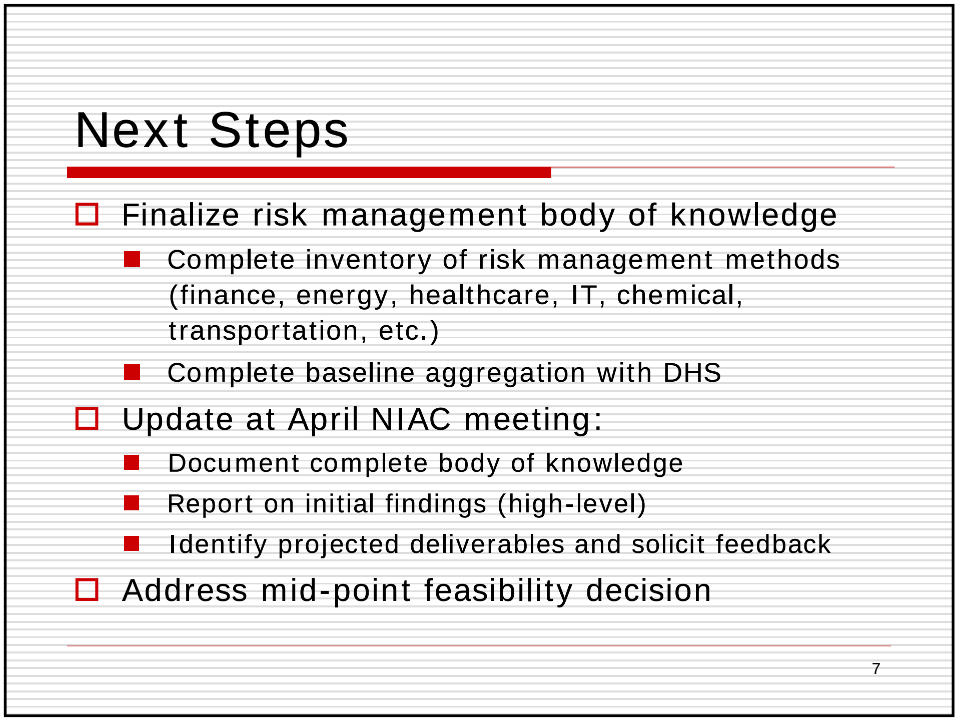
- □ Initiate Working Group (October ‘04 NIAC)
  - Identify and recruit stakeholders
  - Define scope and timeline; resources and allocation
- □ Data Aggregation and Assessment (January ‘05 NIAC)
  - Aggregate raw risk management data
  - Assess state of risk management methods
- □ Deliverable Development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

Working Group Focus

- □ Working Group initiated efforts to:
  - Aggregate and assess existing government risk management methodologies, practices, philosophies, and decision models
  - Aggregate and assess existing private sector risk management methodologies, practices, philosophies, and decision models
  - Identify risk management commonalities and differences between strategic risk management efforts and operational risk management efforts

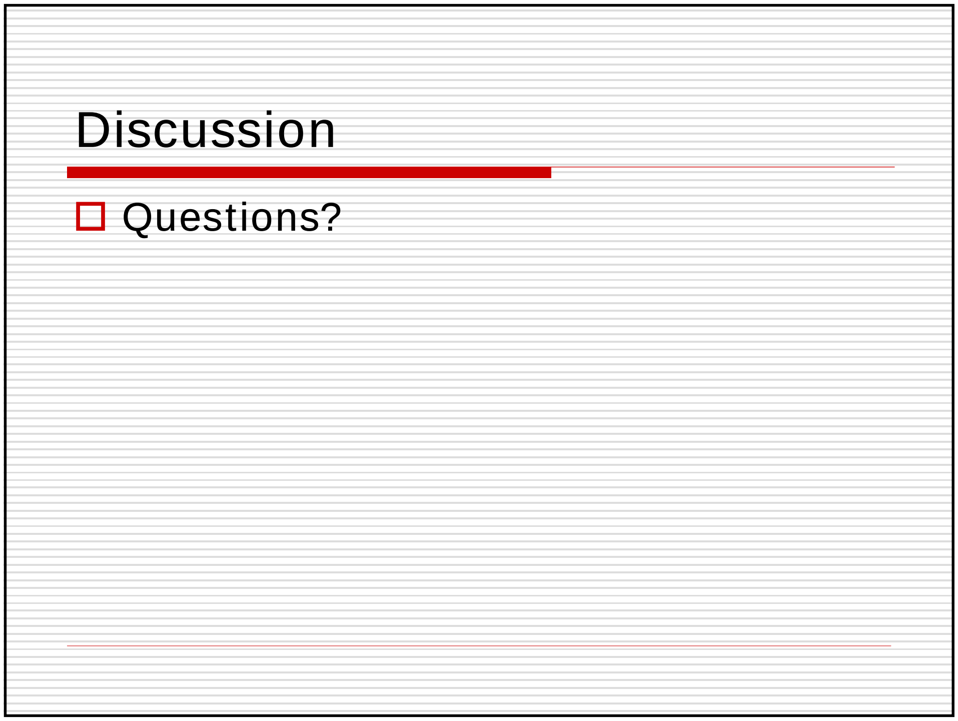
Initial Working Group Findings

- □ Varied risk management data collection experiences
  - Data collection obstacles, proprietary information
- □ Differentiation between strategic and operational risk management data points:
  - Operational risk management data points more common across industries
  - Strategic risk management data points less common across industries
- □ Continuing to seek input from a number of non-traditional sources
  - Academia, industry associations, etc.



Next Steps

- □ Finalize risk management body of knowledge
  - ■ Complete inventory of risk management methods (finance, energy, healthcare, IT, chemical, transportation, etc.)
  - ■ Complete baseline aggregation with DHS
- □ Update at April NIAC meeting:
  - ■ Document complete body of knowledge
  - ■ Report on initial findings (high-level)
  - ■ Identify projected deliverables and solicit feedback
- □ Address mid-point feasibility decision



Discussion

- □ Questions?

ATTACHMENT C:
Status Report on Assuring Adequate National Intellectual Capital to Secure Cyber-Based Critical Infrastructures

National Infrastructure Advisory Committee

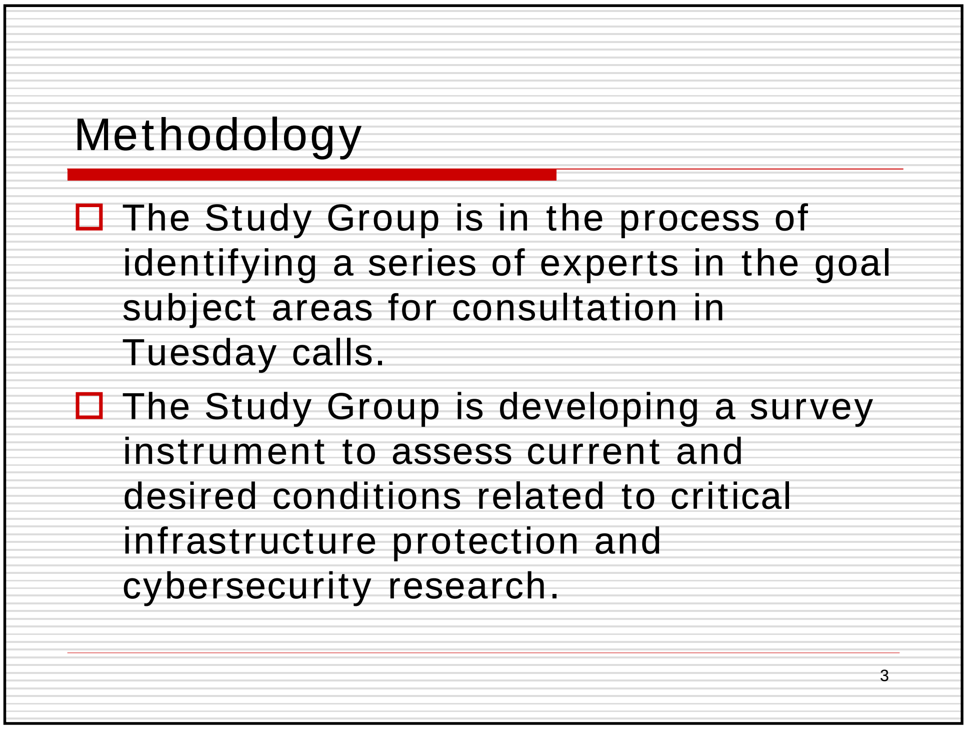
Education and Workforce Preparation Working Group

Subsection #1: Research

December 22, 2004

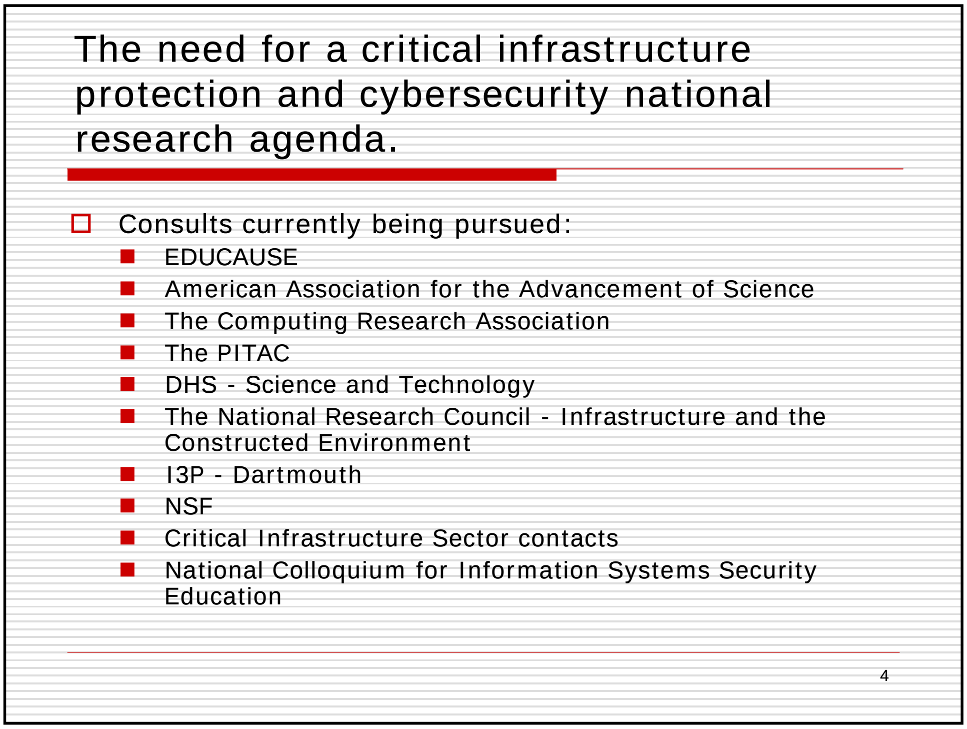
NIAC Research Working Group

- The Working Group is addressing four areas. Initial efforts will focus on:
  - The need for a critical infrastructure protection and cybersecurity national research agenda.
  - Adequacy of the funding base for critical infrastructure protection and cybersecurity related research.
- The Working Group will then address the following two goals:
  - Research products "time-to-market" issues.
  - Adequacy of the related research national talent pool.



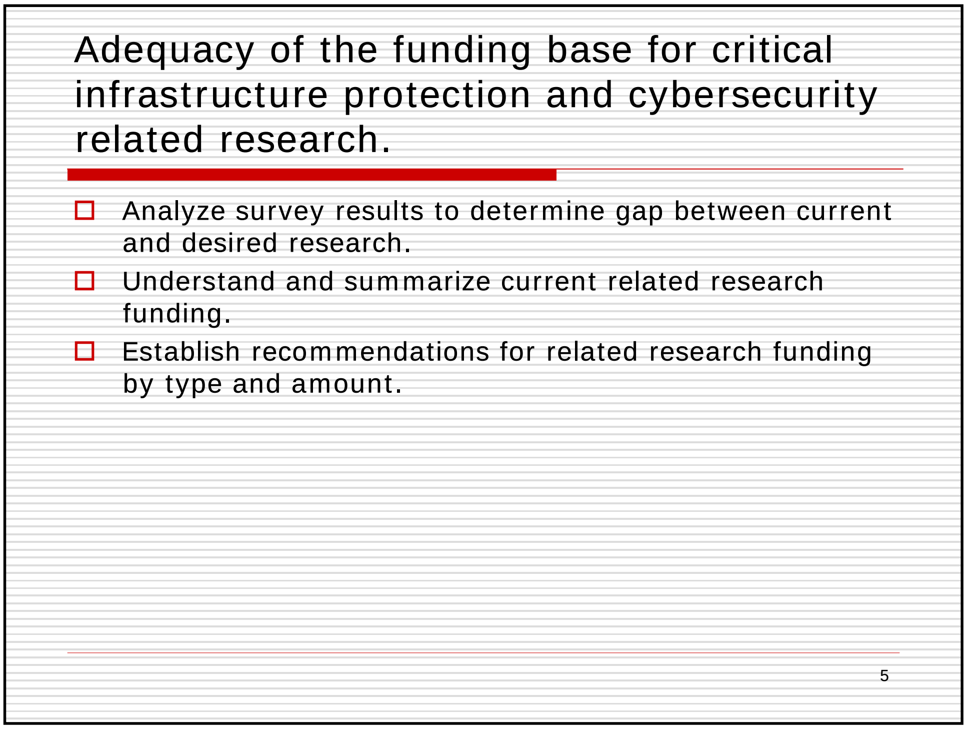
Methodology

- □ The Study Group is in the process of identifying a series of experts in the goal subject areas for consultation in Tuesday calls.
- □ The Study Group is developing a survey instrument to assess current and desired conditions related to critical infrastructure protection and cybersecurity research.



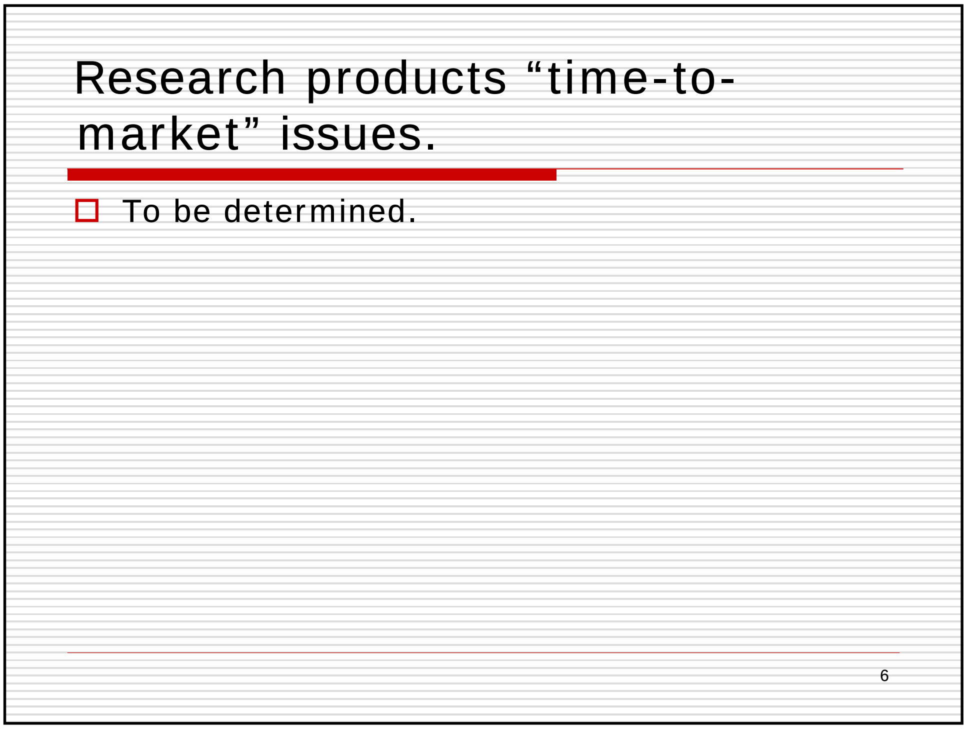
The need for a critical infrastructure protection and cybersecurity national research agenda.

- □ Consults currently being pursued:
  - EDUCAUSE
  - American Association for the Advancement of Science
  - The Computing Research Association
  - The PITAC
  - DHS - Science and Technology
  - The National Research Council - Infrastructure and the Constructed Environment
  - I3P - Dartmouth
  - NSF
  - Critical Infrastructure Sector contacts
  - National Colloquium for Information Systems Security Education



Adequacy of the funding base for critical infrastructure protection and cybersecurity related research.

- □ Analyze survey results to determine gap between current and desired research.
- □ Understand and summarize current related research funding.
- □ Establish recommendations for related research funding by type and amount.



Research products “time-to-market” issues.

- □ To be determined.

Adequacy of related research national talent pool.

- □ To be determined.

National Infrastructure Advisory Committee

Education and Workforce Preparation Working Group

Subsection #2: Workforce Preparation

December 22, 2004

NIAC Education and Workforce Preparation Working Group

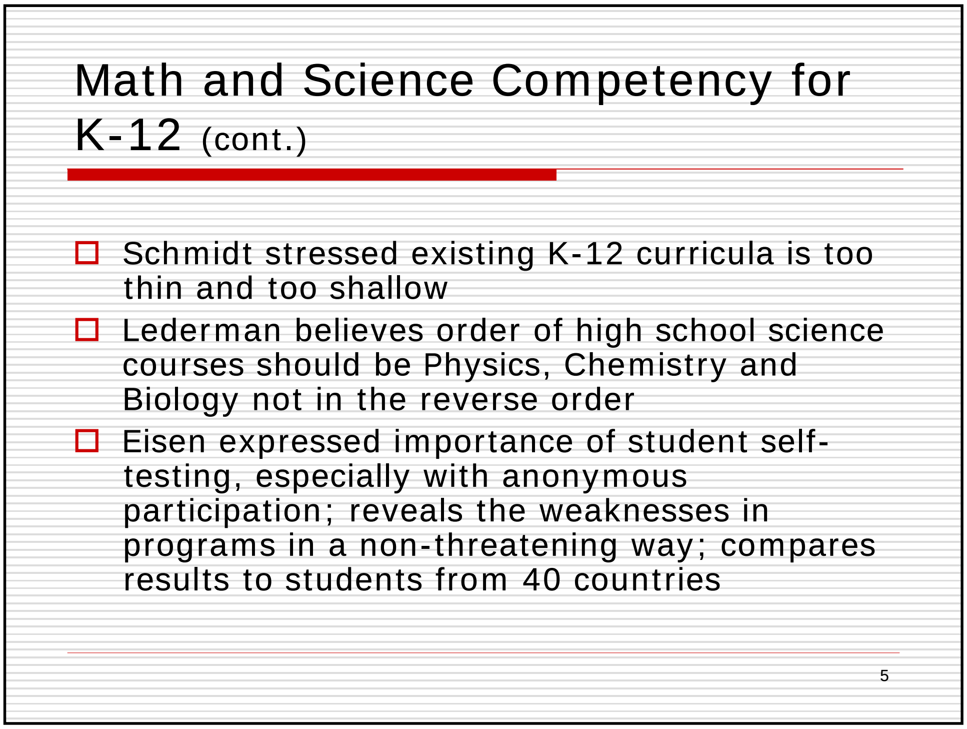
- The Working Group is addressing seven areas:
  - Math and science competency of K-12 learners.
  - Incentives to attract students into technical fields, specifically information assurance and cyber security.
  - Content and delivery of information assurance and cyber security curricula.
  - Usefulness and availability of cyber security certification programs
  - Efficacy of CyberCorps program.
  - Competitiveness of U.S. education internationally.
  - Timeliness of security clearances

Methodology

- Identify a series of experts in different aspects of our questions
- Investigating innovative solutions
- Concentrating on successful pilot programs

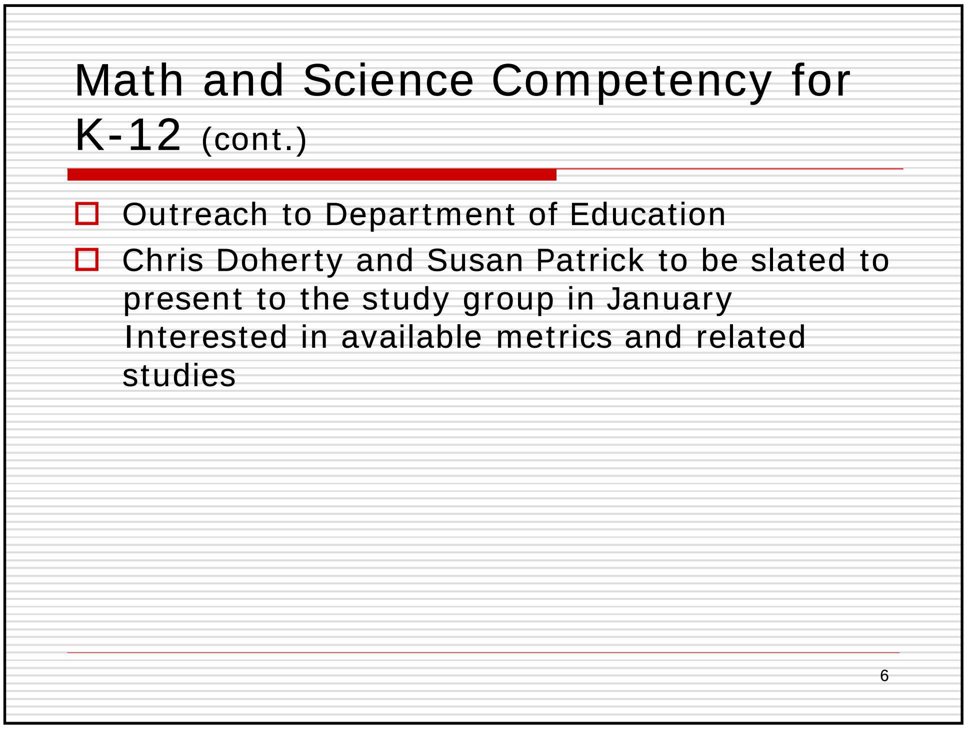
Math and Science Competency for K-12

- Bill Schmidt of Michigan State University briefed results of the 3rd and 4th International Math and Science Surveys, and the lessons from the analysis of results
- Nobel Laureate Leon Lederman, former Director of Fermi Lab, briefed benefits of a specific scheme to re-order the sequence in which science courses are taught
- Phyllis Eisen of the National Association of Manufacturers about www.getsmarter.org



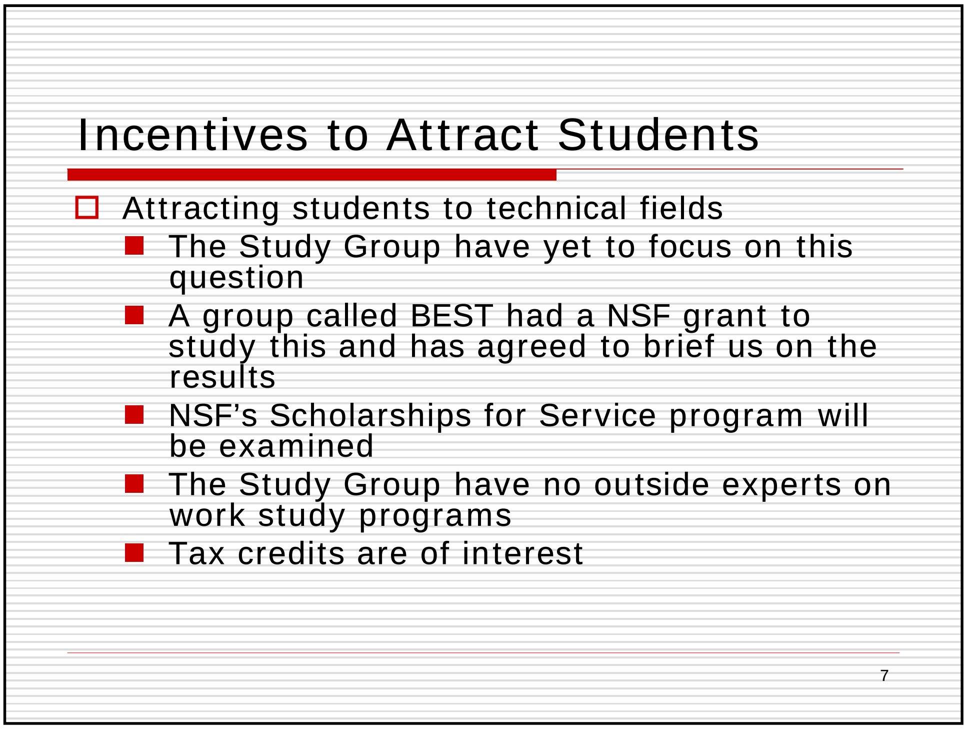
Math and Science Competency for K-12 (cont.)

- □ Schmidt stressed existing K-12 curricula is too thin and too shallow
- □ Lederman believes order of high school science courses should be Physics, Chemistry and Biology not in the reverse order
- □ Eisen expressed importance of student self-testing, especially with anonymous participation; reveals the weaknesses in programs in a non-threatening way; compares results to students from 40 countries



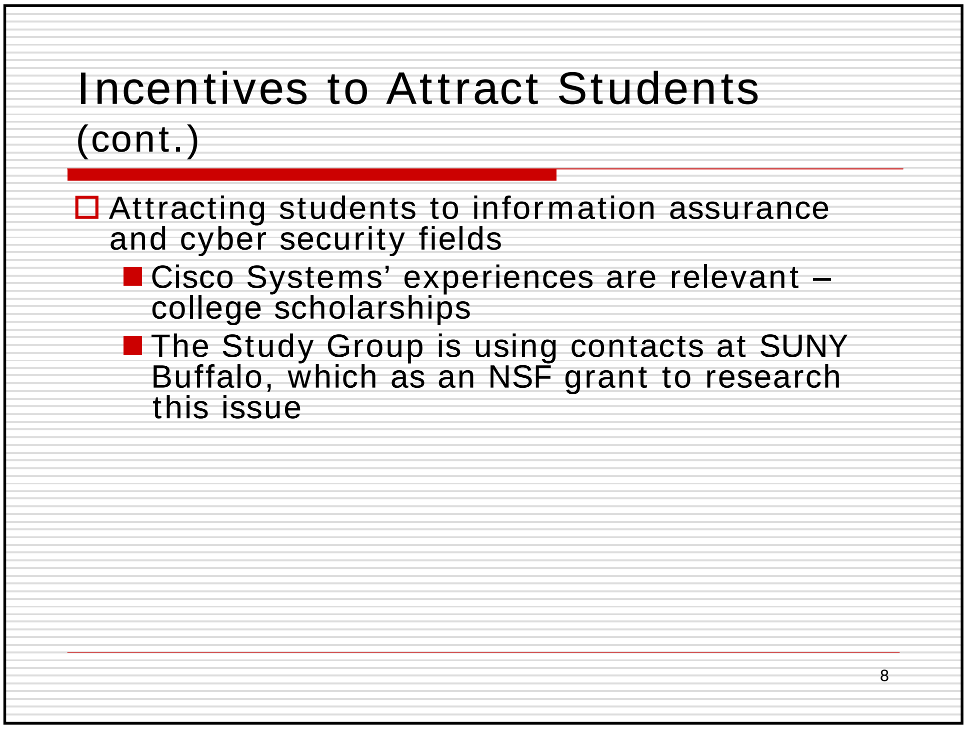
Math and Science Competency for K-12 (cont.)

- □ Outreach to Department of Education
- □ Chris Doherty and Susan Patrick to be slated to present to the study group in January Interested in available metrics and related studies



Incentives to Attract Students

- □ Attracting students to technical fields
  - The Study Group have yet to focus on this question
  - A group called BEST had a NSF grant to study this and has agreed to brief us on the results
  - NSF's Scholarships for Service program will be examined
  - The Study Group have no outside experts on work study programs
  - Tax credits are of interest



Incentives to Attract Students (cont.)

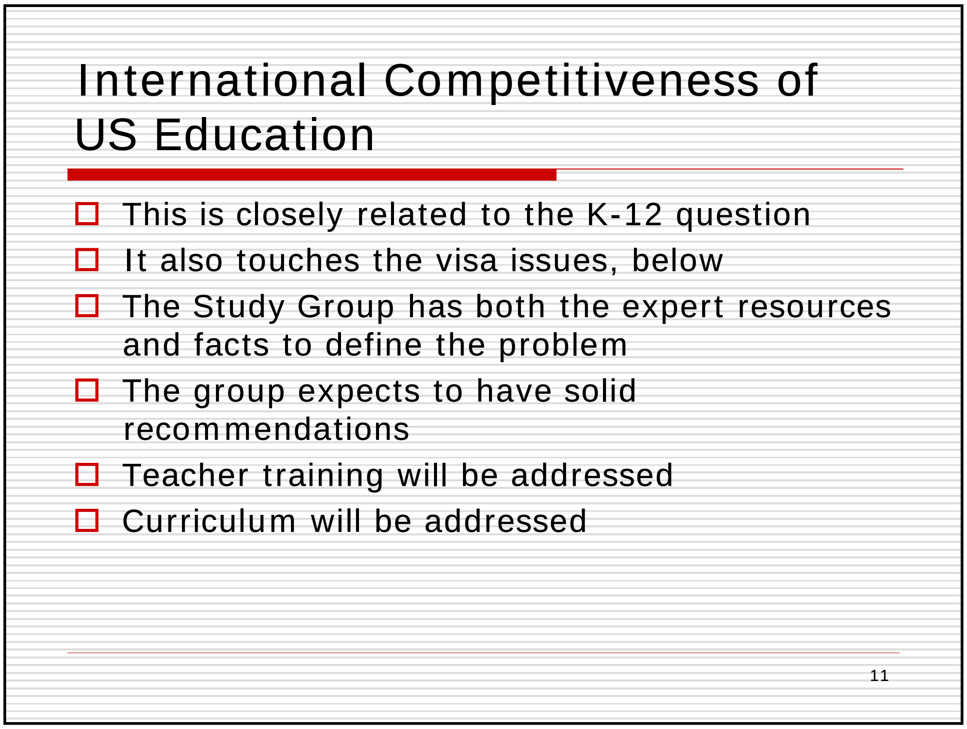
- □ Attracting students to information assurance and cyber security fields
  - Cisco Systems' experiences are relevant – college scholarships
  - The Study Group is using contacts at SUNY Buffalo, which as an NSF grant to research this issue

Cyber Security Curricula

- Curricula Development:
- Equipment Donation:
  - Centers of Academic Excellence in Information Assurance Education (CAE/IAE) universities receiving equipment - 28
  - Total institutions supported by donations - 45
  - Purdue, West Virginia University and Mesa Community College

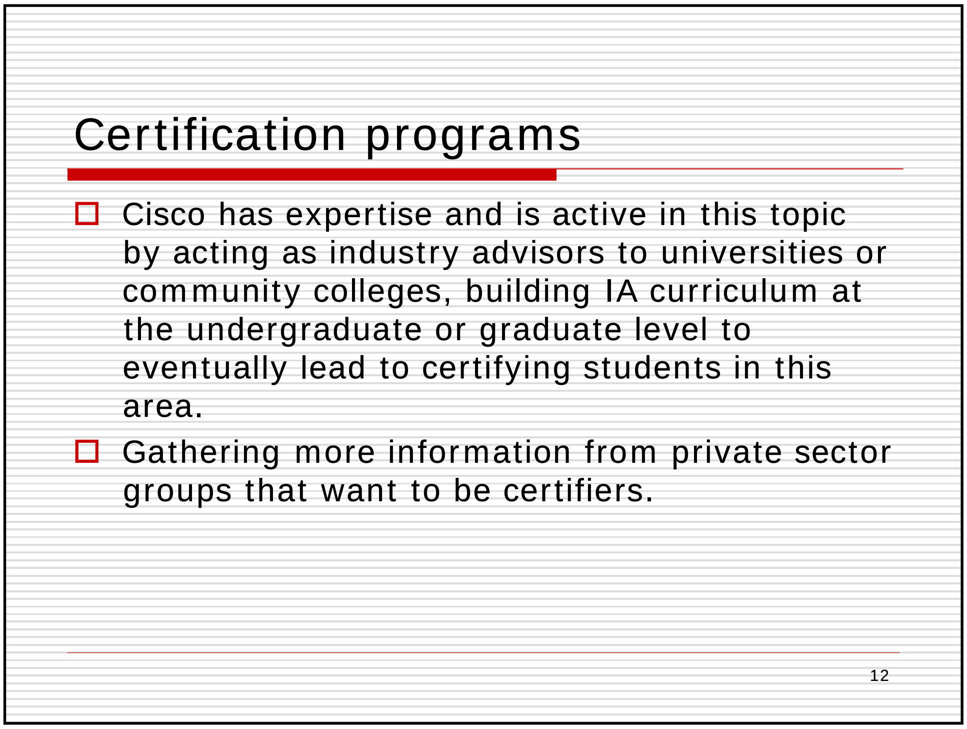
Efficacy of CyberCorps

- The Study Group has expertise and knowledge to cover this on the committee
- Talking with SUNY Buffalo and gathering information
- Dr. Diana Gant, who is the program director, will brief group
- DHS staff is acquiring some background material for group



International Competitiveness of US Education

- This is closely related to the K-12 question
- It also touches the visa issues, below
- The Study Group has both the expert resources and facts to define the problem
- The group expects to have solid recommendations
- Teacher training will be addressed
- Curriculum will be addressed



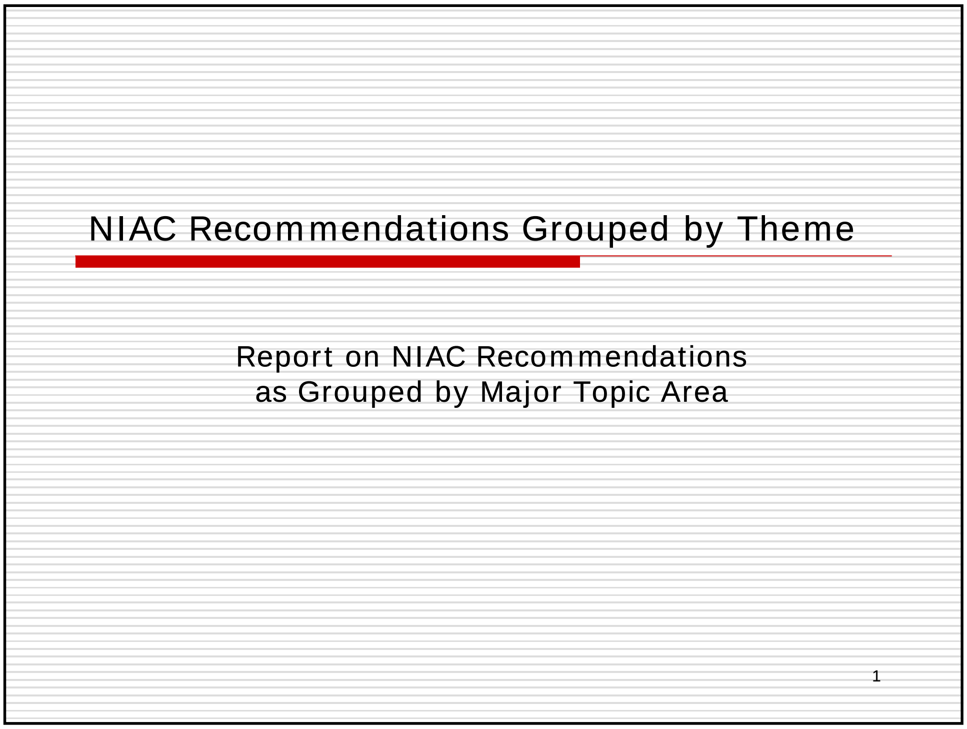
Certification programs

- Cisco has expertise and is active in this topic by acting as industry advisors to universities or community colleges, building IA curriculum at the undergraduate or graduate level to eventually lead to certifying students in this area.
- Gathering more information from private sector groups that want to be certifiers.

Timeliness of Security Clearance Process

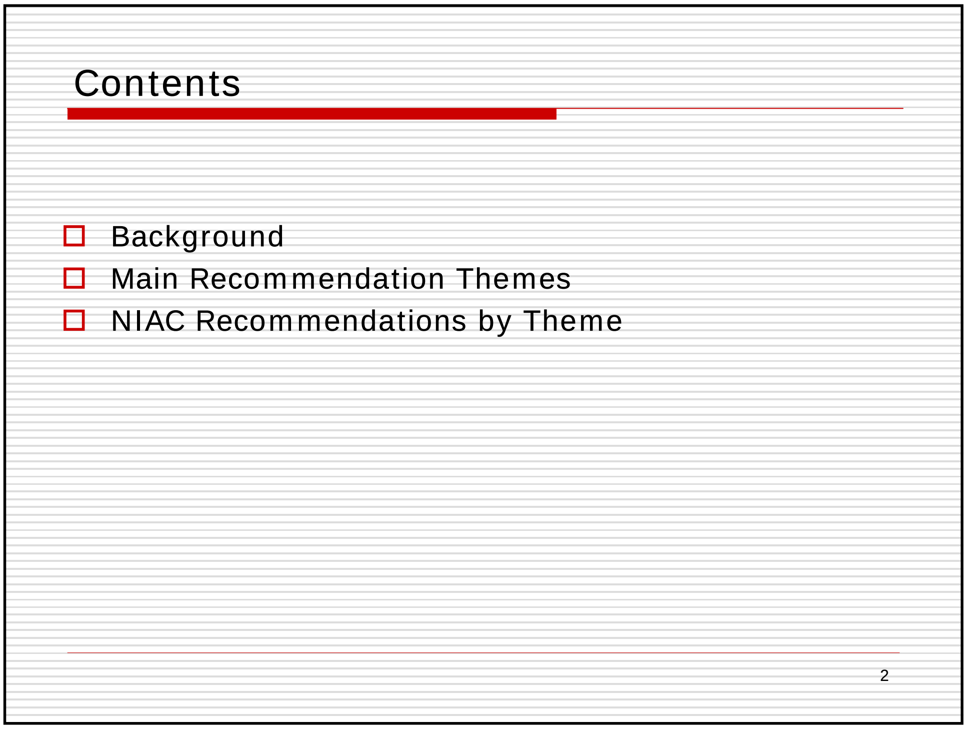
- □ The Study Group plans to tap into the National Academies project on this subject, managed by CSIS
- □ The group has not addressed it yet.

ATTACHMENT D:
Summary of NIAC Recommendations by Subject Area



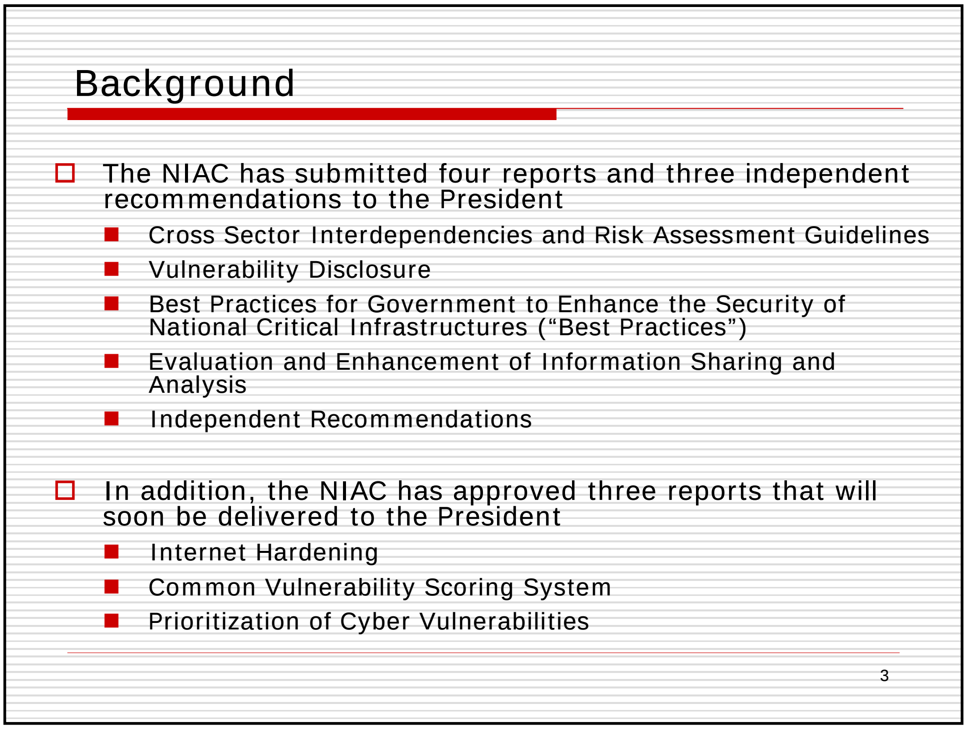
NIAC Recommendations Grouped by Theme

Report on NIAC Recommendations
as Grouped by Major Topic Area



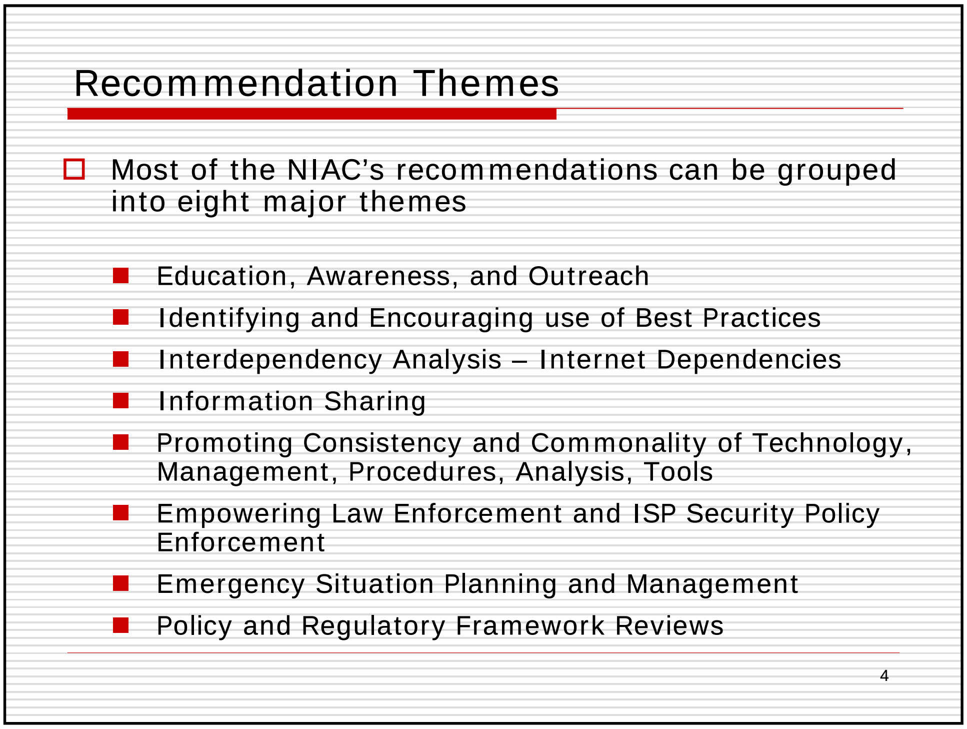
Contents

- □ Background
- □ Main Recommendation Themes
- □ NIAC Recommendations by Theme



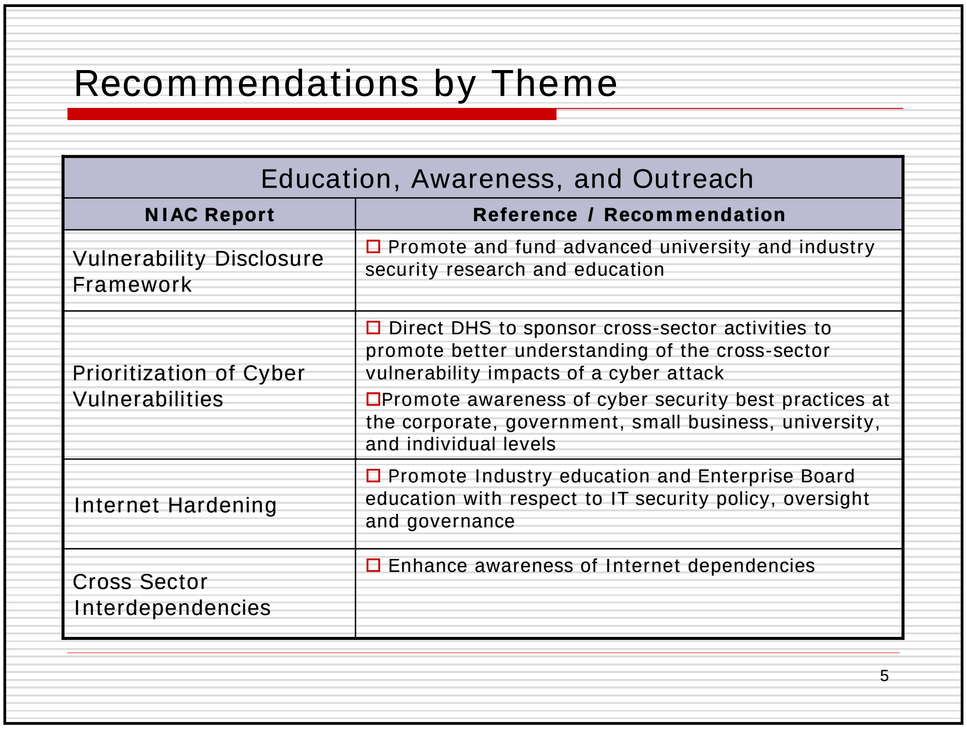
Background

- The NIAC has submitted four reports and three independent recommendations to the President
  - Cross Sector Interdependencies and Risk Assessment Guidelines
  - Vulnerability Disclosure
  - Best Practices for Government to Enhance the Security of National Critical Infrastructures (“Best Practices”)
  - Evaluation and Enhancement of Information Sharing and Analysis
  - Independent Recommendations
- In addition, the NIAC has approved three reports that will soon be delivered to the President
  - Internet Hardening
  - Common Vulnerability Scoring System
  - Prioritization of Cyber Vulnerabilities



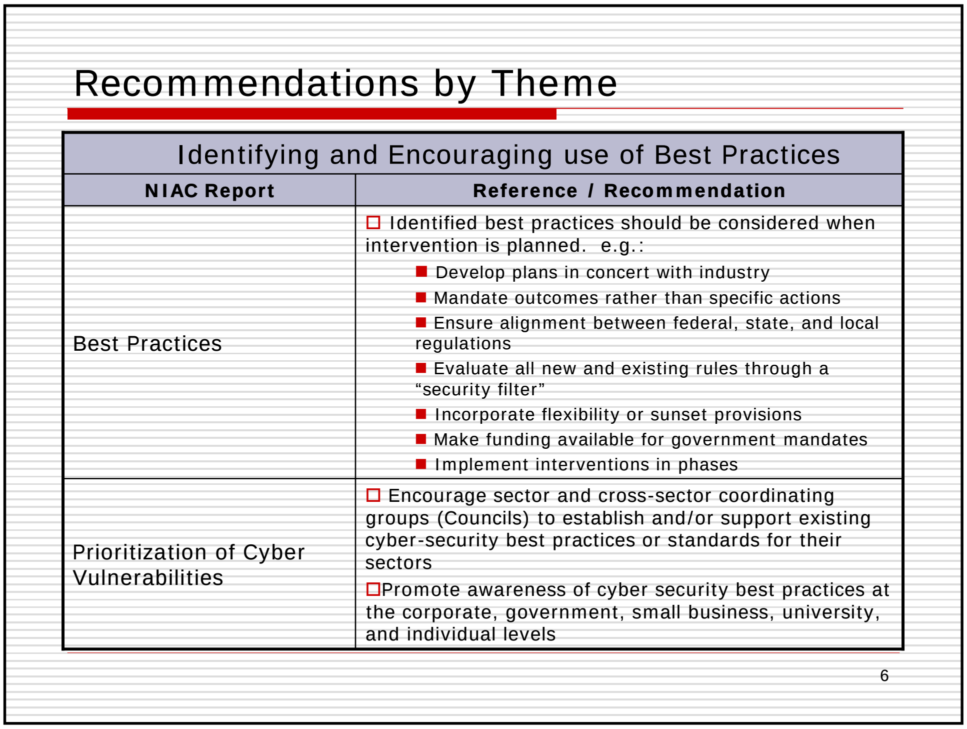
Recommendation Themes

- Most of the NIAC’s recommendations can be grouped into eight major themes
  - Education, Awareness, and Outreach
  - Identifying and Encouraging use of Best Practices
  - Interdependency Analysis – Internet Dependencies
  - Information Sharing
  - Promoting Consistency and Commonality of Technology, Management, Procedures, Analysis, Tools
  - Empowering Law Enforcement and ISP Security Policy Enforcement
  - Emergency Situation Planning and Management
  - Policy and Regulatory Framework Reviews



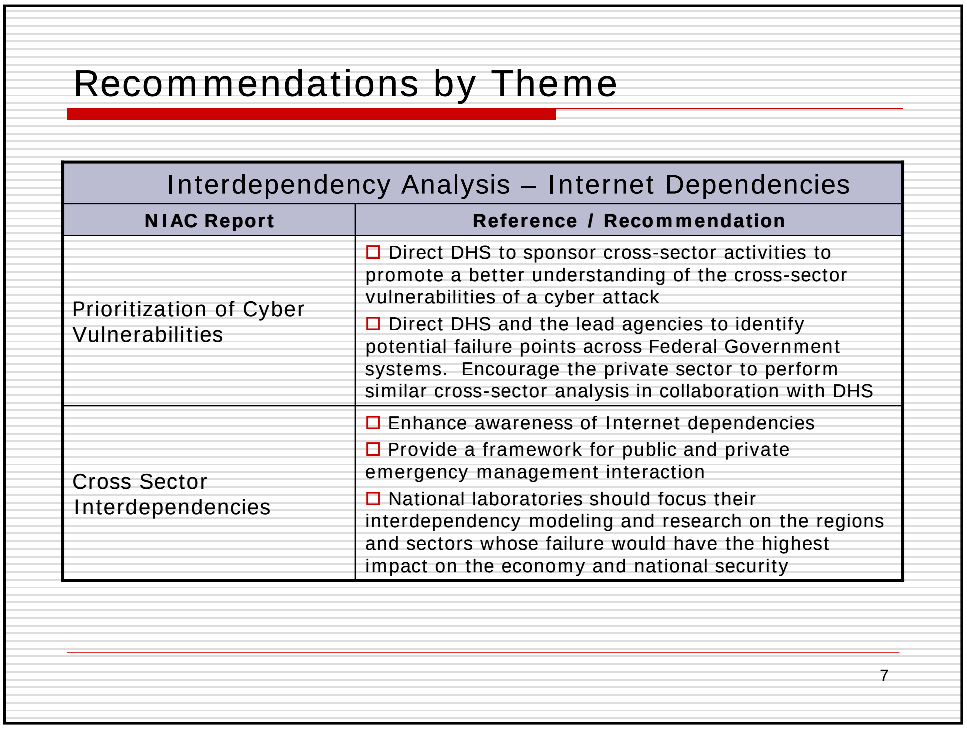
Recommendations by Theme

Education, Awareness, and Outreach	
NIAC Report	**Reference / Recommendation**
Vulnerability Disclosure Framework	□ Promote and fund advanced university and industry security research and education
Prioritization of Cyber Vulnerabilities	□ Direct DHS to sponsor cross-sector activities to promote better understanding of the cross-sector vulnerability impacts of a cyber attack □Promote awareness of cyber security best practices at the corporate, government, small business, university, and individual levels
Internet Hardening	□ Promote Industry education and Enterprise Board education with respect to IT security policy, oversight and governance
Cross Sector Interdependencies	□ Enhance awareness of Internet dependencies



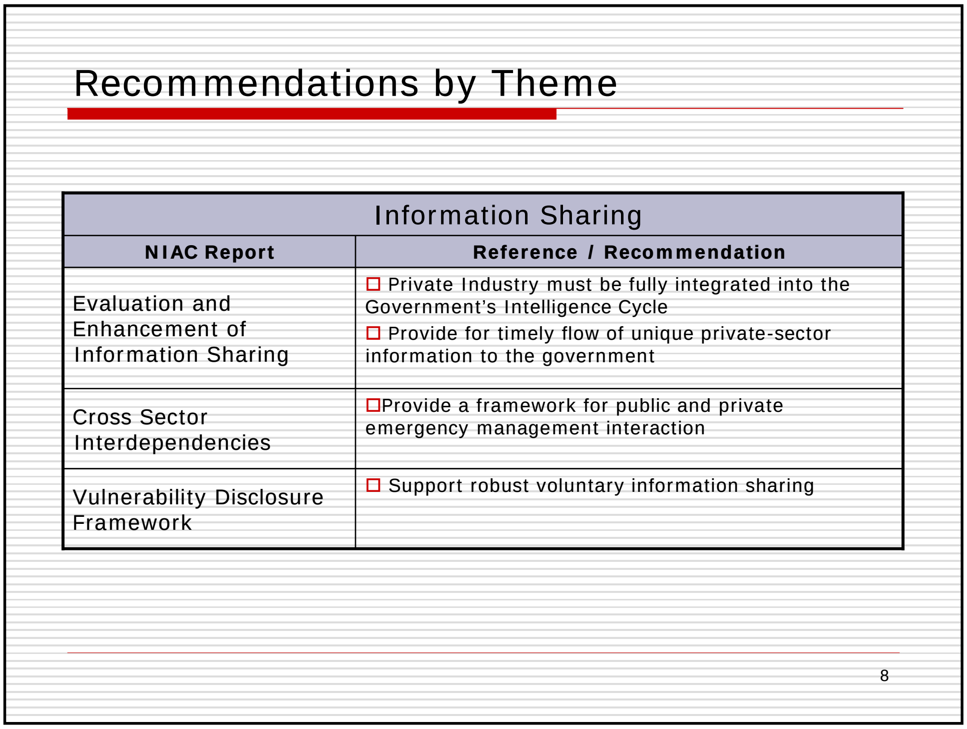
Recommendations by Theme

Identifying and Encouraging use of Best Practices	
NIAC Report	**Reference / Recommendation**
Best Practices	□ Identified best practices should be considered when intervention is planned. e.g.: ■ Develop plans in concert with industry ■ Mandate outcomes rather than specific actions ■ Ensure alignment between federal, state, and local regulations ■ Evaluate all new and existing rules through a “security filter” ■ Incorporate flexibility or sunset provisions ■ Make funding available for government mandates ■ Implement interventions in phases
Prioritization of Cyber Vulnerabilities	□ Encourage sector and cross-sector coordinating groups (Councils) to establish and/or support existing cyber-security best practices or standards for their sectors □Promote awareness of cyber security best practices at the corporate, government, small business, university, and individual levels



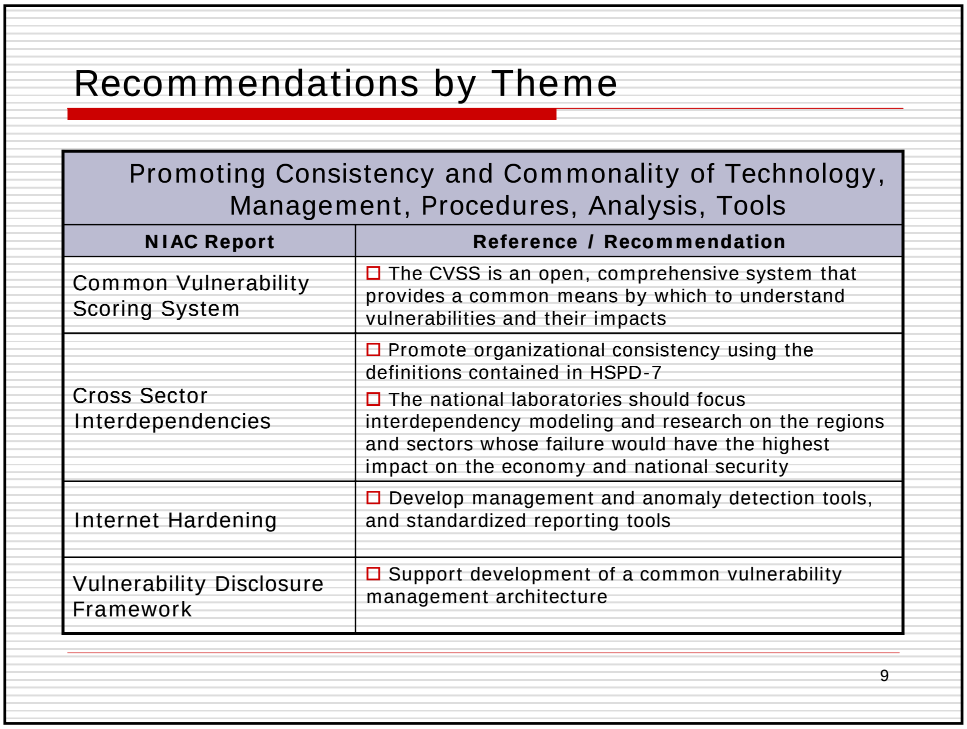
Recommendations by Theme

Interdependency Analysis – Internet Dependencies	
NIAC Report	**Reference / Recommendation**
Prioritization of Cyber Vulnerabilities	□ Direct DHS to sponsor cross-sector activities to promote a better understanding of the cross-sector vulnerabilities of a cyber attack □ Direct DHS and the lead agencies to identify potential failure points across Federal Government systems. Encourage the private sector to perform similar cross-sector analysis in collaboration with DHS
Cross Sector Interdependencies	□ Enhance awareness of Internet dependencies □ Provide a framework for public and private emergency management interaction □ National laboratories 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



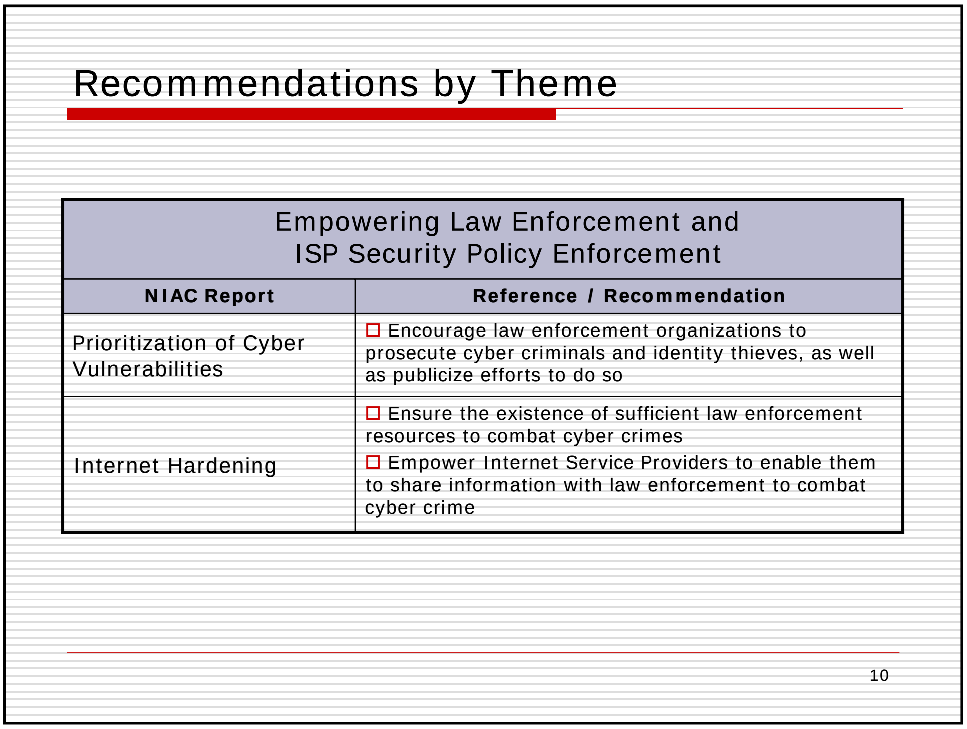
Recommendations by Theme

Information Sharing	
NIAC Report	**Reference / Recommendation**
Evaluation and Enhancement of Information Sharing	□ Private Industry must be fully integrated into the Government's Intelligence Cycle □ Provide for timely flow of unique private-sector information to the government
Cross Sector Interdependencies	□Provide a framework for public and private emergency management interaction
Vulnerability Disclosure Framework	□ Support robust voluntary information sharing



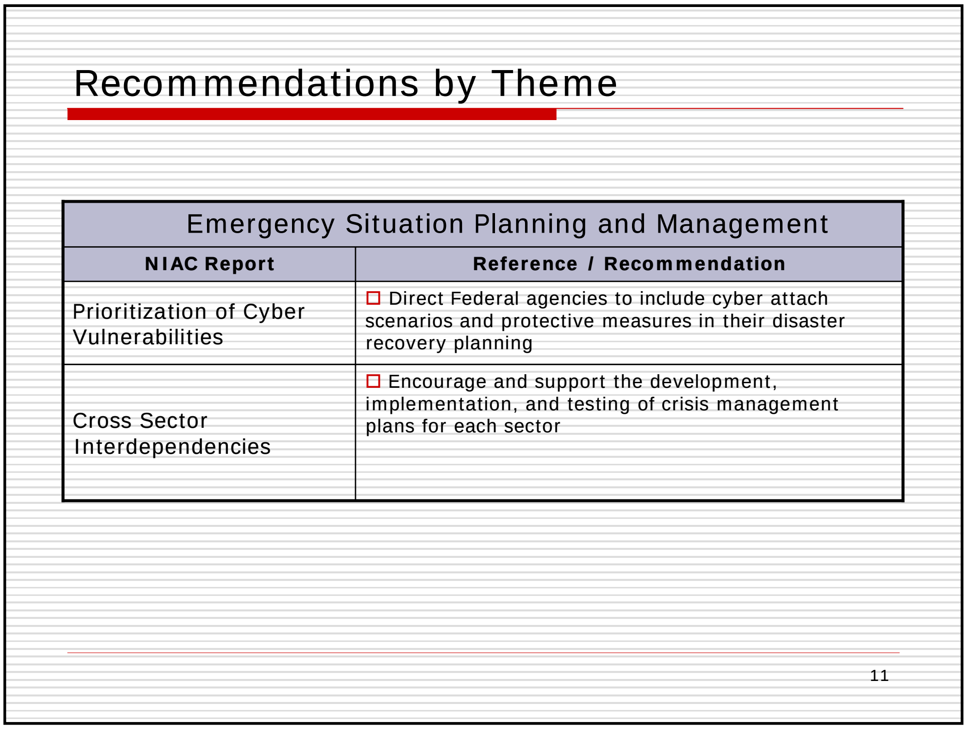
Recommendations by Theme

Promoting Consistency and Commonality of Technology, Management, Procedures, Analysis, Tools	
NIAC Report	**Reference / Recommendation**
Common Vulnerability Scoring System	□ The CVSS is an open, comprehensive system that provides a common means by which to understand vulnerabilities and their impacts
Cross Sector Interdependencies	□ Promote organizational consistency using the definitions contained in HSPD-7 □ The national laboratories should focus interdependency modeling and research on the regions and sectors whose failure would have the highest impact on the economy and national security
Internet Hardening	□ Develop management and anomaly detection tools, and standardized reporting tools
Vulnerability Disclosure Framework	□ Support development of a common vulnerability management architecture



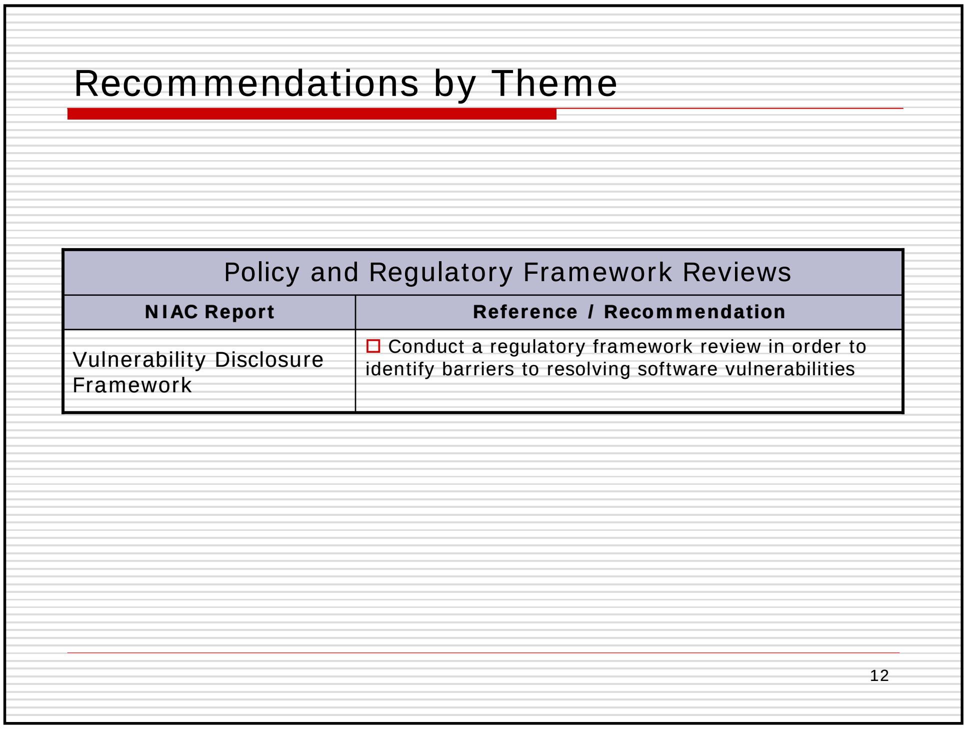
Recommendations by Theme

Empowering Law Enforcement and ISP Security Policy Enforcement	
NIAC Report	**Reference / Recommendation**
Prioritization of Cyber Vulnerabilities	□ Encourage law enforcement organizations to prosecute cyber criminals and identity thieves, as well as publicize efforts to do so
Internet Hardening	□ Ensure the existence of sufficient law enforcement resources to combat cyber crimes □ Empower Internet Service Providers to enable them to share information with law enforcement to combat cyber crime



Recommendations by Theme

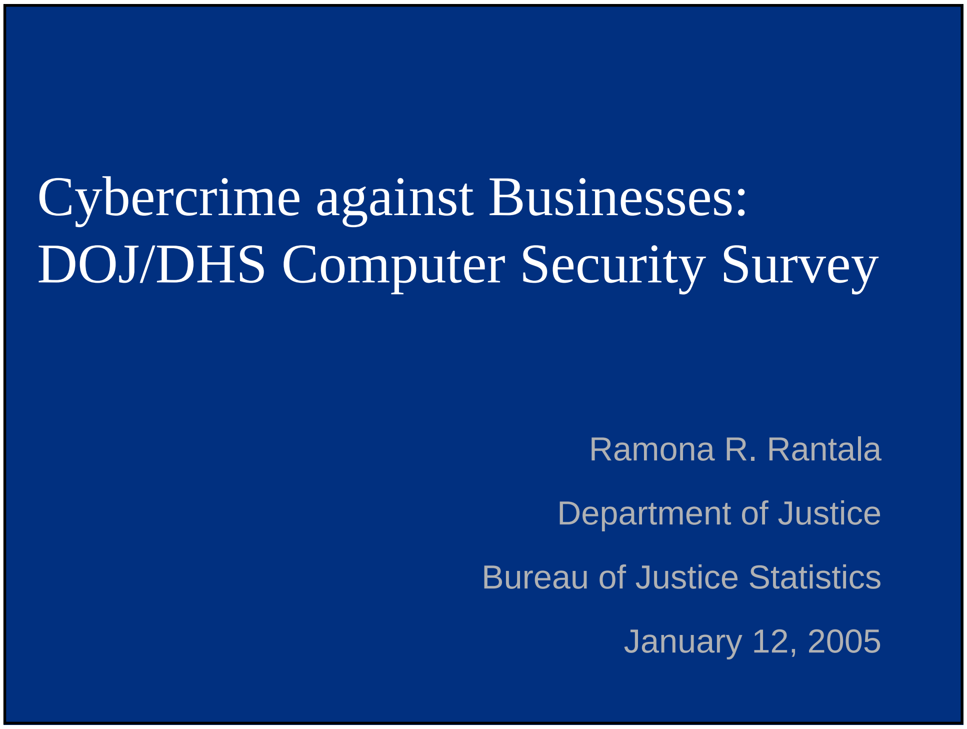
Emergency Situation Planning and Management	
NIAC Report	**Reference / Recommendation**
Prioritization of Cyber Vulnerabilities	□ Direct Federal agencies to include cyber attach scenarios and protective measures in their disaster recovery planning
Cross Sector Interdependencies	□ Encourage and support the development, implementation, and testing of crisis management plans for each sector



Recommendations by Theme

Policy and Regulatory Framework Reviews	
NIAC Report	**Reference / Recommendation**
Vulnerability Disclosure Framework	□ Conduct a regulatory framework review in order to identify barriers to resolving software vulnerabilities

ATTACHMENT E:
Presentation and Discussion of Cyber Crime Against Businesses



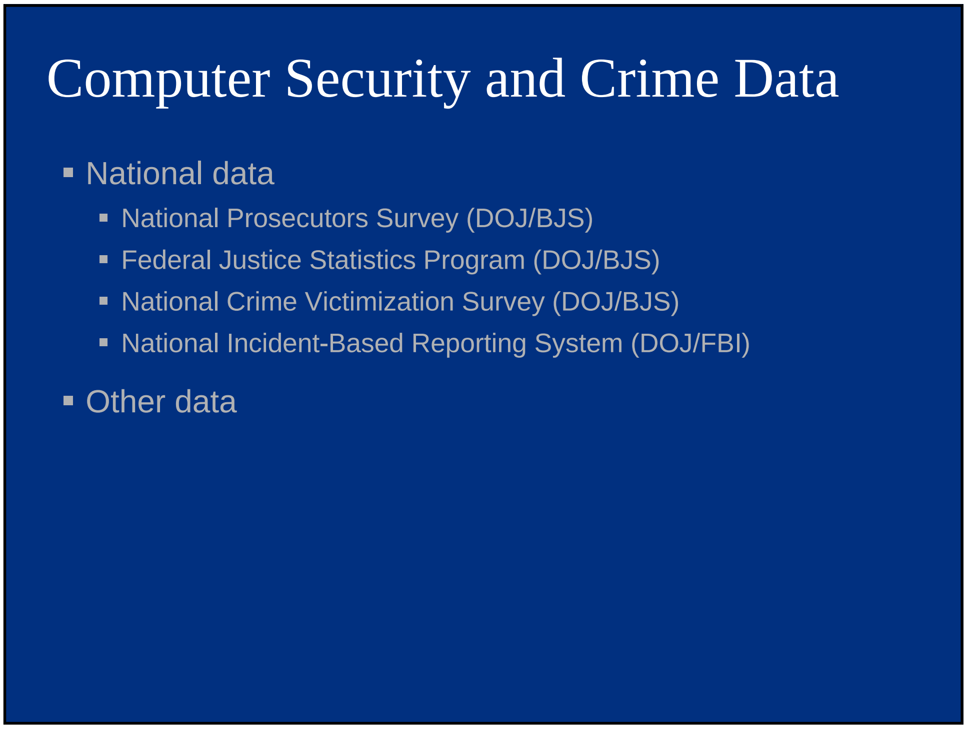
Cybercrime against Businesses: DOJ/DHS Computer Security Survey

Ramona R. Rantala

Department of Justice

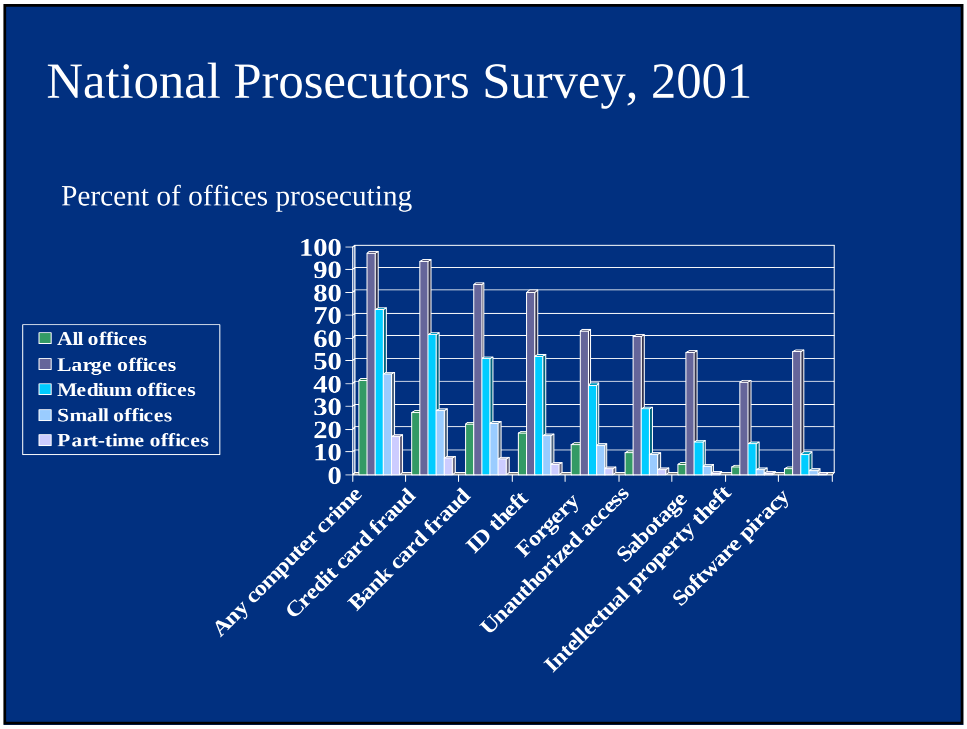
Bureau of Justice Statistics

January 12, 2005



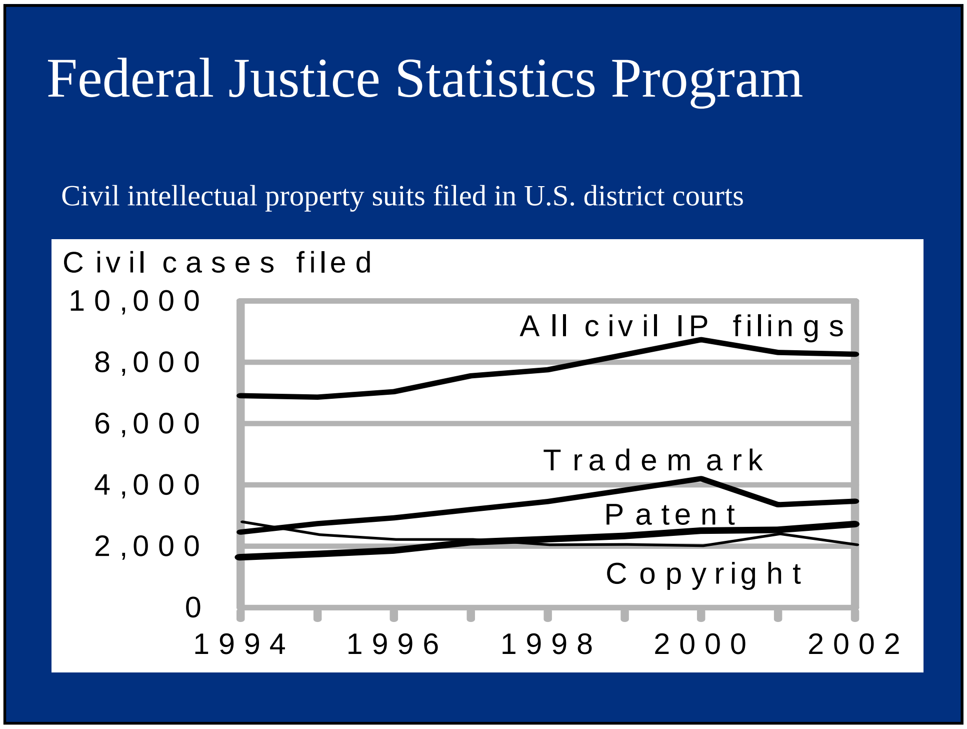
Computer Security and Crime Data

- National data
  - National Prosecutors Survey (DOJ/BJS)
  - Federal Justice Statistics Program (DOJ/BJS)
  - National Crime Victimization Survey (DOJ/BJS)
  - National Incident-Based Reporting System (DOJ/FBI)
- Other data



National Prosecutors Survey, 2001

Percent of offices prosecuting

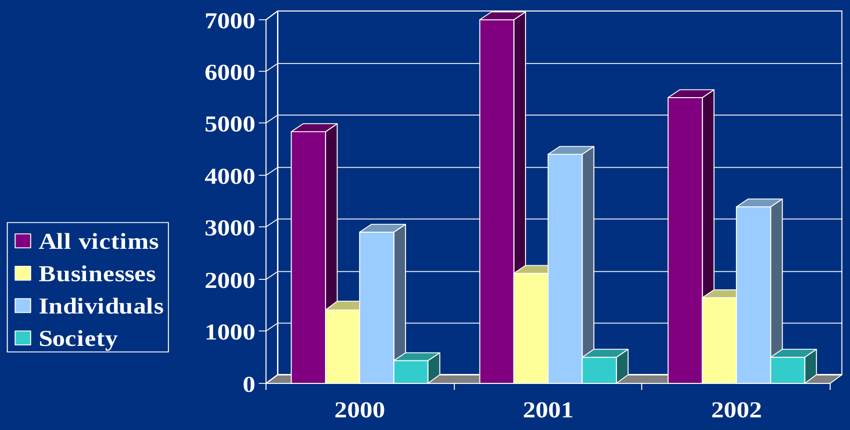


Federal Justice Statistics Program

Civil intellectual property suits filed in U.S. district courts

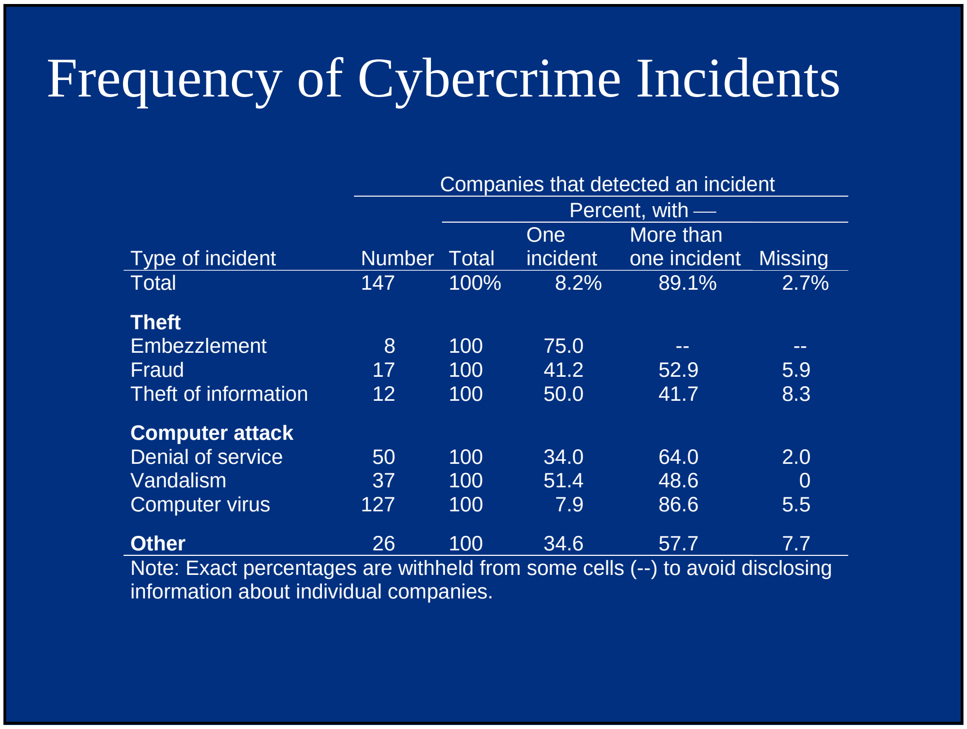
National Incident-Based Reporting System

Victims of computer crime



2001 Computer Security Survey Pilot

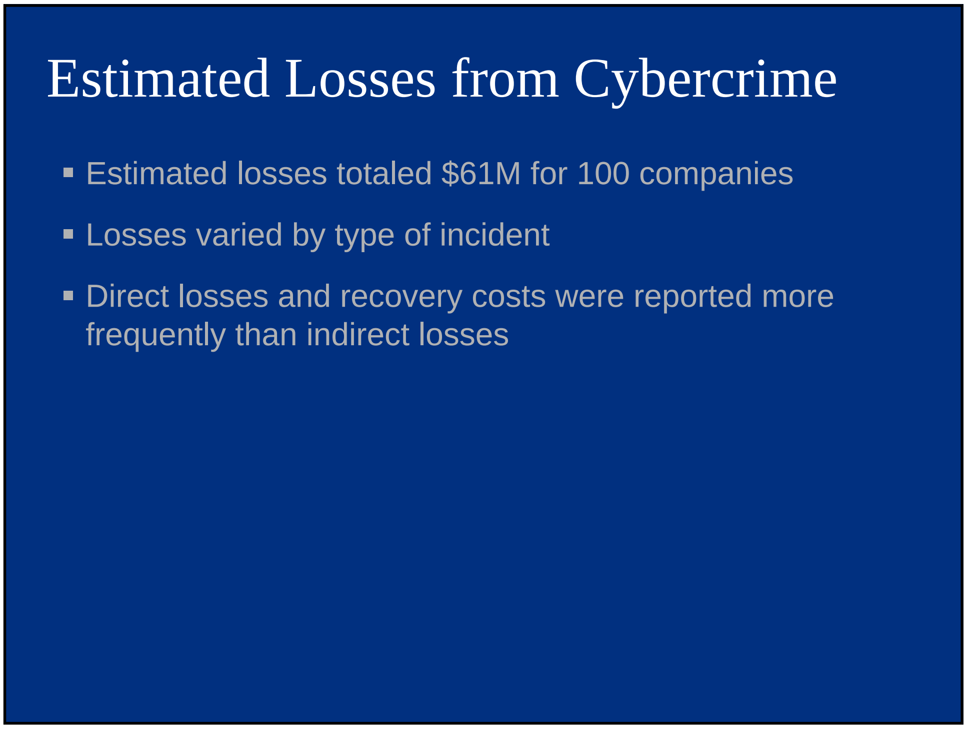
- Feasibility test
- Of the 500 sampled companies, 208 responded
- 95% of respondents used computers
- Nearly 75% of companies with computers were victimized by cybercrime
- Computer viruses were most common



Frequency of Cybercrime Incidents

	Companies that detected an incident				
		Percent, with —			
			One	More than	
Type of incident	Number	Total	incident	one incident	Missing
Total	147	100%	8.2%	89.1%	2.7%
Theft					
Embezzlement	8	100	75.0	--	--
Fraud	17	100	41.2	52.9	5.9
Theft of information	12	100	50.0	41.7	8.3
Computer attack					
Denial of service	50	100	34.0	64.0	2.0
Vandalism	37	100	51.4	48.6	0
Computer virus	127	100	7.9	86.6	5.5
Other	26	100	34.6	57.7	7.7

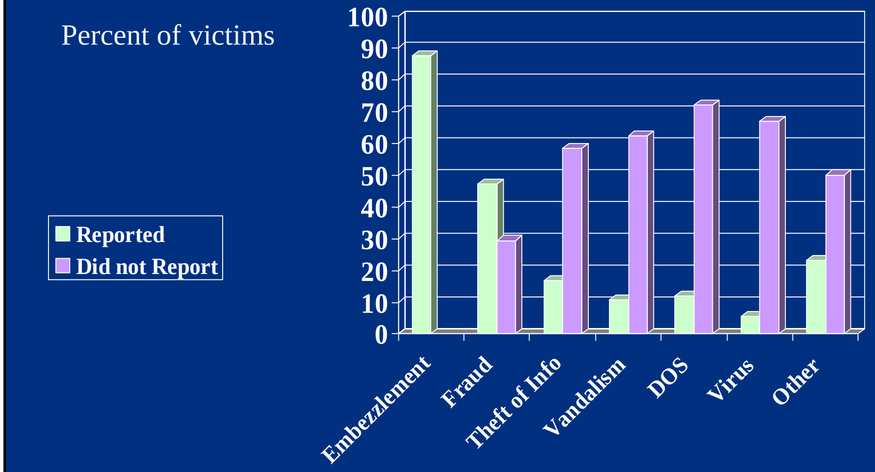
Note: Exact percentages are withheld from some cells (--) to avoid disclosing information about individual companies.



Estimated Losses from Cybercrime

- Estimated losses totaled $61M for 100 companies
- Losses varied by type of incident
- Direct losses and recovery costs were reported more frequently than indirect losses

Reporting Incidents to Authorities



Safeguards against Intrusions

- Computer security technology
  - Used by 91% of companies with computers
  - Anti-virus software most common
- Computer security practices
  - Employed by 83% of companies with computers
  - 135 companies had business continuity or disaster recovery programs

2004 Computer Security Survey

- Bureau of Justice Statistics in partnership with Department of Homeland Security
- First nationally representative study of computer security among U.S. businesses
- Revised survey instrument based on 2001 pilot
- Reviewed and vetted by
  - FBI and Infragard
  - Economic Security Working Group (Dept. of Commerce)
  - Electric Power ISAC (NERC)
  - President's Information Technology Advisory Committee
  - Joint Council on Information Age Crime

Homeland
Security