NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING

Tuesday, October 12, 2004
1:00-4:00 p.m.
The Hamilton Crowne Plaza Hotel
14th and K Street, NW
Washington, DC 20005

AGENDA

I. OPENING OF MEETING

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

II. ROLL CALL OF MEMBERS

Nancy J. Wong

III. OPENING REMARKS: AND INTRODUCTIONS

Chairman Erle A. Nye, Chairman of the Board, TXU Corp. and *Vice Chairman John T. Chambers,* Chairman and CEO, Cisco Systems, Inc.

The Honorable Thomas Ridge, Secretary, DHS

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

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

IV. 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 Police Department, NIAC Member

	B. RISK MANAGEMENT APPROACHES TO PROTECTION	*Thomas E. Noonan*, Chairman, President, & CEO, Internet Security Systems, Inc.; NIAC Member and *Martha Marsh*, President & CEO, Stanford Hospitals & Clinics; NIAC Member
	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
V.	**FINAL REPORTS AND DELIBERATIONS**	*Chairman Erle A. Nye* Presiding
	A. FINAL REPORT ON HARDENING THE INTERNET	*George H. Conrades,* Chairman & CEO Akamai Technologies; NIAC Member
	B. ***Deliberation and Approval of Recommendations of Final Report***	*NIAC Members*
	C. **FINAL REPORT ON THE THE COMMON VULNERABILITY SCORING SYSTEM**	*Vice Chairman John T. Chambers; and John W. Thompson,* Chairman & CEO, Symantec Corporation; NIAC Member
	D. Deliberation and Approval of Recommendations of Final Report	*NIAC Members*
	E. FINAL REPORT AND DISCUSSION ON PRIORITIZATION OF CYBER VULNERABILITIES	*Martin G. McGuinn, Chairman & CEO* Mellon Financial Corporation, NIAC Member
	F. ***Deliberation and Approval of Recommendations of Final Report***	*NIAC Members*
VI.	**NEW BUSINESS**	*Chairman Erle A. Nye; NIAC Members*
VII.	**ADJOURNMENT**	*Chairman Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON
Chairman Nye; Vice Chairman Chambers; Mr. Berkeley; Mr. Carty; Mr. Conrades; Mr. Davidson; Gen. Edmonds; Chief Gallegos; Ms. Grayson; Ms. Marsh; Dr. Rose; Ms. Ware and Mr. Webb

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL
Mr. Barrett and Mr. McGuinn

MEMBERS ABSENT:
Governor Ehrlich; Mr. Hernandez; Mr. Holliday; Ms. Katen; Commissioner Kelly; Mr. Martinez; Mr. Noonan; Mayor Santini-Padilla; and Mr. Thompson

STAFF DESIGNEES PRESENT MONITORING PROCEEDINGS:
Mr. John Puckett (for Mr. Holliday); Mr. Jonathan White (for Ms. Katen); Mr. Peter Allor (for Mr. Noonan); and Mr. Rob Clyde (for Mr. Thompson)

OTHER DIGNITARIES PRESENT:
U.S. Government: The Honorable Tom Ridge, Secretary of the Department of Homeland Security; Mr. R. James Caverly, Director, Infrastructure Coordination Division (ICD) of the Department of Homeland Security; and Ms. Nancy J. Wong, Information Analysis and Infrastructure Protection Directorate of the Department of Homeland Security and Designated Federal Officer for the NIAC.

I. OPENING OF MEETING

Ms. 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 staff from DHS, Chairman Erle A. Nye, Vice Chairman John T. Chambers, all Council members and their staffs present and on the teleconference line, 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 ninth meeting of the National Infrastructure Advisory Council and the fourth meeting of the year 2004. Ms. Wong then proceeded to call roll.

II. ROLL CALL

Ms. Nancy Wong called the roll.

She said the Council had been working very hard over the last quarter on finalizing more studies and sets of recommendations. Consequently, the Council had a very full agenda and with a great deal of pleasure she turned the meeting over to Chairman Nye to continue the official proceedings of the meeting and to introduce the other speakers.

III. OPENING REMARKS: AND INTRODUCTIONS

Chairman Erle A. Nye, Chairman of the Board, TXU Corp. and *Vice Chairman John T. Chambers*, Chairman and CEO, Cisco Systems, Inc.

The Honorable Tom Ridge, Secretary, DHS

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

Chairman Nye thanked Ms. Wong and those attending for being at the meeting promptly. He said the Council appreciates all the support it has received and was pleased with the closed briefing session earlier that morning. Chairman Nye then began the opening remarks by saying it was an honor for him to introduce and Secretary Tom Ridge from the Department of Homeland Security. He thought everyone had followed the Secretary's activities over the last two years very closely. The Council admires what he has done and appreciates the relationship it has with his office as well as with the White House. He asserted it was truly a privilege to have the Secretary attend the meeting. He turned the floor to the Secretary.

Secretary Ridge thanked Chairman Nye for his gracious introduction and acknowledged the Chairman's leadership, presence, and participation on the Homeland Security Advisory Council (HSAC). The HSAC appreciates the fact that in addition to his NIAC responsibilities, he found time to meaningfully participate. The Secretary also said it was a pleasure to work with Vice Chairman John Chambers once again and thanked him for his sustained involvement and interest in supporting this Homeland Security effort from its first days. He thanked everyone else for their attendance, acknowledging he was aware busy people have many things to do. There is a significant time requirement associated with working on the Council, but it really is the intellectual confrontations, perspective, and recommendations offered by the Council that are absolutely invaluable to DHS and its mission.

Secretary Ridge continued, saying the Department had been in business now for about twenty months. From a corporate viewpoint, everything going on under the Homeland Security umbrella basically constitutes mergers, acquisitions, divestitures, and some start-ups involving about 180,000 people. As the Council might imagine, this number of people poses quite a dilemma for the integration of financial management systems, procurement systems, and human resource systems. There is a business line activity and integration occurring that has actually had the Department call on some members of the Council for assistance.

He wanted to focus on one of these start-ups, the Information Analysis and Infrastructure Protection Directorate. The Secretary noted he was aware some of the Council's earlier and current work products and recommendations dealt with vulnerability assessments and risk assessments—this work is absolutely critical to IAIP's efforts. He understood the Council was addressed by several speakers from this unit in the morning session to discuss threat information, especially how it is analyzed, digested, and determined to be actionable or worth sharing with the private sector. DHS is trying to develop a permanent system to bolster general information sharing with different economic sectors-- specifically sharing information appropriate either to a particular institution or particular entity. The best example and most recent example is when the Department had general threat information relevant to the financial services sector. This data was specifically important to five institutions publicly identified as in Northern New Jersey, New York City, and Washington, DC. Through the work of the global coalition securing information about terrorists' identities, operations, capabilities, and capacity for expansion, DHS is learning more about their methods from recently seized detainees. It is clear they know how to operate within the 21st century world of the Internet. Some of this information was gleaned from hard drives and removable disks of those who have been apprehended overseas. Over the coming years, the Department will gather more and more information about terrorists and potential threats. How this information is digested and distributed to the private sector is of great importance. The Department must determine if the information is crucial to a private sector entity—whether they need to know it or not and whether they need to act upon it or not. This points to the sustained importance of participation on the NIAC. This sharing of information had never really been considered before, but now must be done in a robust and comprehensive way as a response to threats.

To that end, DHS is experimenting with a few approaches. There is an information sharing network called the Homeland Security Information Network. It is an Internet-based system that goes to Governors and their respective Homeland Security Advisors as well as the 50 largest urban areas. DHS also works in cooperation with the Federal Bureau of Investigation (FBI). DHS is running four pilot programs off of the Homeland Security Information Network to connect that network to discreet individual companies in those areas considered to be operating critical infrastructure. DHS' strategy is to err on the side of sharing as much information as possible whether it is actionable or not. At the very least, this information could be stored in a corporate database as background information or material. This effort is very much in development right now because DHS is really about the integration of a nation more than it is a simple department. DHS is more than 180,000 people from nearly two dozen disparate groups joining together. DHS is basically building and sustaining relationships with partners at the state and local levels as well as in the academic communities and private sector. One of the most critical pieces of this permanent, sustained relationship is the development of the information flow to and from the Department's partners. This is a very high priority for DHS because it cannot maximize its ability to either prevent or detect potential attacks without this partnership. One thing DHS has learned from detainees is an increase in diligence and more security is actually a deterrent in and of itself. Every day in which there is no attack, the enemies must postpone an attack, or find another target that gives the Department another 24 hours to fortify the country. The challenge DHS faces is to build the system and create a comfort level with information sharing in both directions. This is another example of how private sector participation is so important. It is far more than quarterly meetings or recommendations; the Council is in many ways the sounding board for the kind of infrastructure DHS builds, the kind of information it shares, and how that data is leveraged.

Secretary Ridge said the Council will present some final reports regarding the Internet today, Hardening the Internet, Prioritizing Cyber Vulnerabilities, and the Common Vulnerability Scoring System. Within the Infrastructure Protection division there have been significant changes and the new Director of the National Cyber Security Division (NCSD) should be appointed soon. Secretary Ridge concluded his remarks and thanked the Council.

Chairman Nye thanked the Secretary and said the Council was flattered by his attendance. He asked if the NIAC had any questions or comments for Secretary Ridge.

Vice Chairman Chambers said the Department is undertaking a series of mergers few would have the courage to do. One of the most important things DHS does is bringing these organizations together and encouraging them to interact. He asked the Secretary how the Department had the discipline to have one view of its customer.

Secretary Ridge said DHS recognized from its first days that mergers are fraught with pitfalls. Mergers in the private sector must first get through regulatory processes, approval processes, and the federal system—this gives them between twelve and eighteen months to smooth things out and begin that integration process prior to making the formal changes. The Federal Government does not have this luxury. One thing DHS did have was a sense of unity built upon sensitivity to the mission. He said the realities of 9/11 elevated the importance of the work being done in Homeland Security. This work has been going on for years, but no one has really paid attention.

The task of integrating disparate groups is a key to the Department's mission. A great example of this is the One Face at the Border Initiative. The day national ports of entry opened under DHS, there were DHS employees wearing one uniform. Previously this had been the domain of the Immigration and Naturalization Services (INS), US Customs, and the former Department of Agriculture. A year and a half later, it is one uniform, there is cross training, the same pay schedule, the same overtime schedule and the Department has more people who can do more things. It is a flexible workforce with a surge capacity to adequately handle volume spikes caused by more airlines showing up than anticipated, for example.

Secretary Ridge said another one of the main challenges was internal branding. DHS has such wide responsibility that just about everyone is its customer. America is its customer; it is DHS' mission to integrate the country. The Department also has to serve states and local governments as well as the private sector.

The Secretary said another major challenge is the integration of what might be referred to as the business line or business services. The Department started with nineteen procurement systems and is now down to eight on its way to one. DHS also started with several human resource systems, this will also be pared down to one. Within probably the next thirty to sixty days there will be a two year plan outlining the building of a pay-for-performance system within the Department. There are twelve or so financial management systems right now as the Department heads to a lone management system. He said he hoped the Vice Chairman's question was answered.

Mr. Carty asked about the move to centralize the intelligence work of the CIA. He asked the Secretary's thoughts.

Secretary Ridge said everyone has embraced the notion of a National Intelligence Director having budget authority. He said he thought it would help the Department by having one person responsible to oversee the budget and how information is categorized. He asserted he was confident the position would protect DHS' fiscal interests. If it is done correctly, it should be a positive in the long run.

The Secretary brought up another difference between the private and public sectors is how capital is generated. Corporations can generate their own capital whereas agencies and departments have to seek appropriations from Capitol Hill. While DHS cannot be run strictly as a business there are certain business principles applicable. The Department also has the Milestone Project—DHS basically knows where it wants to be and sets a timeline around achieving those goals. Someone is assigned the responsibility of getting the Department to that point and is accountable if they do not.

Vice Chairman Chambers complimented the Secretary and his staff and said they had been a joy to work with and very challenging in a constructive way. He asked if there were any items the Secretary would like the Council to invest more time in or if there were any areas where the Council might improve.

Secretary Ridge said he could not underestimate the value of the Council's service. That is basically all the Department can ask of it and is one of the reasons the Presidents convened it in the first place. The government particularly appreciates the work on cyber security the Council does. This is a significant partnership as far as detection, prevention and vulnerability assessment are concerned. The government has been forced to rely more on the private sector than it ever has. In some areas, the government does not have the capacity internally to do everything the private sector can do; this is one reason the government greatly appreciates the assistance of the private sector and all that the Council does. The Secretary concluded that the Council should continue delivering the same high quality work as it has done thus far.

Chairman Nye thanked the Secretary again for his attendance and said the Council valued the opportunity he had been given to serve and was very proud of what the government has accomplished in a relatively short period of time. He said there is much more to be done but some comfort has to be taken in what has been accomplished thus far. The Council applauds this and appreciates the time the Secretary had spent with it. The Chairman said the Council looked forward to another opportunity to serve if there was the need, he thanked the Secretary again.

Secretary Ridge thanked the Council..

Chairman Nye then turned the meeting to Mr. R. James Caverly for his update on the National Response Plan (NRP) and the National Infrastructure Protection Plan (NIPP).

Mr. Caverly thanked the Chairman and extended the regrets of Assistant Secretary Liscouski for not being able to attend. He said there were two subjects he wanted to discuss with the Council. The first is the National Response Plan; which had been previously circulated to the members for comment. Those comments had been returned and incorporated and the document has gone into a final draft form. The most important part of the NRP is its recognition of the interaction between the private and public sectors in the event of a catastrophic disaster event. He said most domestic incidents to which the Federal Government has responded to have shown the private sector's ability to make judgments on its own as to when issues must be mitigated and when they need to be restored. The National Response Plan recognizes the threat potential of catastrophic incidents on a central level that need coordination. The private sector annex recognizes this and provides mechanisms for coordination to ensure the private sector's role as well as the government's role. It ensures these activities complement one another and do not complicate either's responsibility.

Mr. Caverly said the next point he wanted to go over was the NIPP. This was sent out for comments and this feedback was being incorporated before the document was forwarded to the Secretary, who will then forward it to the President. As soon as there is a document accepted by the President, the document will then be distributed to the members of the Council. The NIPP addresses both the activities that need to take place between DHS, sector-specific agencies, and the intersection of these areas across interdependencies. One of the significant advances in the latest draft which has changed from the version last distributed is the organization around the concept of a sector coordinating council--a broadly representational council for the sector. These councils are being organized in those sectors that do not have one. The financial and food and agriculture sectors already have such councils. The water sector is very close to forming their council. Councils will be instituted across each of the thirteen critical infrastructure sectors and the four key resource areas. The other dynamic component of this effort is DHS' formation of a complementary government coordinating council to ensure meetings between the appropriate agencies and their specific private sector coordinating councils. For example, linking the energy sector, the Department of Energy, and the National Electricity Reliability Council (NERC) would be ideal. These efforts will come into being shortly and will allow for implementation. The implementation of the National Infrastructure Protection Plan will be driven by the actions of the owners and operators of these coordinating councils. DHS will also work very closely with sectors broadly represented in this way to move this plan to the next step, implementation. Mr. Caverly concluded and thanked Chairman Nye.

Chairman Nye asked if there were any questions or comments for Mr. Caverly.

Vice Chairman Chambers echoed some of the items previously discussed. The reason these reports have been so effective is the considerable amount of time members themselves as well as the Study Groups put into the work. There have repeatedly been issues that appeared to be fairly easy topics, but turned out to be very difficult undertakings. He said the Council has seen a marked ability and willingness to work together in order to produce meaningful results, incorporating lessons learned from its federal counterparts.

Chairman Nye thanked the Vice Chairman and said he agreed and stated the feedback from the White House has been very positive. He said he felt it is not often one's advice is actually heeded, much less genuinely appreciated. The quality of the work flows out of the activity produced by all the members. The Chairman hoped the Council could maintain its focus and commitment as this work is materially important and truly makes a positive difference. He encouraged each of the members to continue to put their best efforts forward. He anticipated the Council would have a few more appointees by the next meeting. There are four or five industry categories being researched now and several representatives from those industries have been vetted by the White House. These appointees will help with the future agenda. There are three items discussed at the last meeting of the NIAC and each of those projects is up and running. Additionally, the Council has three items up for final approval.

He said each member should have been provided with the draft minutes from the July meeting.

Mr. Berkeley motioned for a vote on the approval of the minutes. This motion was seconded and the minutes were put to a vote. They were unanimously approved. Chairman Nye thanked the Council and moved on to status reports on current initiatives.

He called on Vice Chairman John Chambers and Chief Gilbert Gallegos to introduce the first item--Intelligence Process and the Work Products Regarding Critical Infrastructure.

IV. 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 Police Department NIAC Member

Chairman Nye then moved into the first status report on the Intelligence Process and Work Products Regarding Critical Infrastructures from Vice Chairman Chambers and Chief Gallegos.

Vice Chairman Chambers began by saying the charge of the Intelligence Coordination Working Group initially sounds like a logical approach, but it is a classic business problem. The Working Group opens by analyzing what needs to be done in terms of the data architectures regarding information sharing. Like most of the other projects the Council has undertaken, the first step is to define the most basic need. To really define the need, there must be an understanding of the intelligence community's needs. Thus far, the Working Group has seen the community's willingness to share information so as to understand the fundamental requirements for maintaining the private sector's critical infrastructure. He said over the next few slides, he and Chief Gallegos will jointly discuss the Working Group. He asked if Chief Gallegos had any comments.

Chief Gallegos thanked the Vice Chairman and said the Council is moving into a new arena by addressing intelligence and the Study Group's efforts should reflect this. The Working Group should be able to deliver a product not only to the private sector, but also to various government agencies throughout the country so the information can be appropriately utilized. Chief Gallegos said the 9/11 Commission was very critical of the lack of communication between intelligence communities in that information culled by these different groups was really never assessed or clearly analyzed. Now the private sector is being added to the equation, requiring a significant change in strategy around assessing and sharing the information in a useful way. He said the Working Group has a high learning capability and the private sector is needed to meaningfully deal with the information gathered everyday.

Vice Chairman Chambers said the work begins with both sides educating the other, almost Intelligence 101 and Private Sector 101. This information exchange will help the Study Group get off to a strong start. The Vice Chairman asked Chief Gallegos to outline the Working Group's scope and key priorities.

Chief Gallegos said the main goal is to develop policy recommendations.

Chief Gallegos said the first slide addresses the process of dealing with information, he said that as a police chief, he was accustomed to handling criminal intelligence information, but this kind of intelligence speaks to terrorism and threats to national critical infrastructure. The Working Group and Study Group will develop processes and implementation methods at each and every level—this will require a comfort level between the intelligence community and the private sector. The intelligence community's roster should be broadened to include more people to address this. Going back to the 9/11 Commission critique that these different intelligence field aspects failed to effectively communicate, it is crucial that there be lucid communication between the public and private sectors. Again, this will require integration of information and processes and a systematic method to access that information. Chief Gallegos said he thought there would be a learning and educational element that Council members will have to undertake.

Vice Chairman Chambers said one of the key points in addressing the intelligence community issue is having the same terminology. The intelligence community focuses on foreign threats while domestic threats are handled by law enforcement and DHS. The Vice Chairman said it is important to examine how sectors use information provided by the intelligence community in coordination with domestic threat information culled from DHS and law enforcement. Sectors need to constructively use this data and establish a consistent process that will remain consistent through its implementation. There are some critical questions the sectors must confront:

- How do sectors prioritize which threats they react to?
- How do they break these down by time issues or a sense of urgency and how do potential threats apply to specific companies?

Vice Chairman Chambers said the Council can share sector expertise with the intelligence community and learn from them simultaneously.

Chief Gallegos said developing a clearance system for all elements of the infrastructure is critical because much of this information is highly sensitive. If this information is going to be put to good use, it must be presented clearly and effectively and with safeguards to ensure the information against misuse. There is also an effort underway to secure clearances for Council members. Mr. John Macgaffin is aiding the Study Group with this endeavor and within six to nine months there should be a solid product. Additionally, it is important to receive feedback from the Council as to what the next steps should be. Mr. Macgaffin should be help the Study Group take action very quickly.

Vice Chairman Chambers said he approved of the first few steps of the Study Group and asked Chairman Nye to open the floor for any questions that members may have.

Chairman Nye said the Working Group and its Study Group appear to have started quite well and it is important to remember this is a large project and will take some time. He asked the Council if there were any questions for Vice Chairman Chambers or Chief Gallegos.

Mr. Carty asked for a list of the current members of the Working Group.

Vice Chairman Chambers said that so far the members are Vice Chairman Chambers, Chief Gallegos, Mr. Al Berkeley, Gen. Al Edmonds, and Mr. Tom Noonan.

Vice Chairman Chambers asked if there were any other member of the Council interested in joining the Working Group.

Chairman Nye said Mr. Carty would make a good addition and thanked him.

With no more new volunteers, Chairman Nye thanked the Vice Chairman and Chief Gallegos and opened the floor to Ms, Martha Marsh to discuss risk management approaches.

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 & Clinics; NIAC Member

Ms. Marsh thanked the Chairman and extended Mr. Noonan's regrets for not being able to attend. A member of the Study Group, Mr. Peter Allor from Internet Security Systems and Mr. Scott Blanchette from Stanford Hospital and Clinics were on hand to answer questions.

Ms. Marsh said the Working Group's agenda is to address the key values, focus, intended outcomes, next steps, and timeline for the Working Group and its Study Group. During the July meeting of the NIAC, the Council identified private sector risk management experiences and attributes that might bolster existing government efforts to protect national critical infrastructure. While the private and public sectors seek similar outcomes--reduced exposure to undesirable consequences-- these entities assess risk management and accept risks differently. Accordingly, the Council convened a Working Group to explore the private sector's risk management philosophies, methodologies, and outcomes. The Working Group's goal is to gauge these activities' usefulness for inclusion in government infrastructure protection planning programs. The Council's broad representation of industries reliant on formalized, scientific, and tested risk management methodologies will yield a successful effort.

Ms. Marsh said the Working Group envisions the Council adding value in different ways. First, from a very high level the private sector relies upon three basic risk management drivers:

1. the probability or likelihood of an adverse event
2. the potential outcome of an adverse event; and
3. the efficiency or cost effective allocation of risk management resources to avoid an adverse event.

The balancing of these three drivers is a core component of nearly all private sector leadership roles. As industry remains focused on cost efficiency and effectiveness, failure to manage these constraints may induce a critical or even fatal outcome for private sector management. For example, failure to manage risk in a just-in-time supply chain may cripple business operations. She continued, saying the expansion of excessive resources on supply chain risk management may squander profits and reduce corporate value. Neither of these outcomes is desirable.

Secondly, the public sector is undergoing a risk management transformation. For nearly fifty years, the Federal Government focused its national defense on risk inherent in a bilateral world. This historical risk management model focused on the low probability, high impact clash between the United States and the Soviet Union. Today, the Federal Government continues to transition risk management to a world presenting threats at a higher probability--perhaps on a scale not previously seen in U.S. history. This transition illuminates the challenges the Federal Government will continue to face in reducing this distributed risk. Effective risk management, efficient allocation of resources, and a focus on value are all tenets of the private sector risk management model and needs to become core components of federal practice over time. The Working Group intends to use the NIAC's resources to identify risk management philosophies, methods and outcomes used by the private sector and make appropriate recommendations to strengthen public sector risk management efforts.

The Working Group will focus on three specific efforts:

1. a baseline assessment,
2. a benchmark analysis, and
3. a valuable deliverable capturing the lessons derived from the first two efforts.

First, the Working Group will work with DHS to assess the existing body of knowledge across multiple government agencies to better understand current public sector risk management methodologies, practices, philosophies, and decision models. Secondly, the Study Group will benchmark this body of knowledge against comparable private sector solutions. A part of this benchmark comparison will include the identification of three sub-items:

1. The Working Group will benchmark the state of public risk management efforts against state of private sector efforts.
2. The Working Group will identify focus areas not previously addressed or not fully matured in private sector risk management models, and
3. The Working Group will capture differences between risk management trade-offs that differ between the two models.

The Working Group and its Study Group will focus on developing a valuable deliverable. For example, an inherent private sector focus is the return on invested capital. This specific focus on return may have limited utility in a government risk management model. The Study Group may be able to identify ways to tailor this historical corporate focus for government use. Instead of a return on invested capital, the Working Group might suggest the Council recommend focusing on realized value from invested capital. This realized value will not specifically tie to a quantitative dollar return, but might qualitatively help the government adopt corporate risk management methodologies.

Ms. Marsh said risk management is a broadly defined category; when defining an outcome, the Working Group will have many variables to consider. She reasserted its strategic focus will be on delivering a valuable product. The Working Group is actively working through a mid-point decision for the April 2005 NIAC meeting. At this point, it will identify the utility and sufficiency of existing risk management methodologies. In addition, it will have a more concrete understanding of the feasibility of producing a solid deliverable within the scope, scale, and resources available through the Council's Working Group structure. Having said that, Ms. Marsh suggested there are numerous plausible deliverables this effort might generate. The Working Group might recommend modifying risk management focus, methods, or philosophies. The Study Group might work toward developing a revised risk management scoring system or might identify areas where the Federal Government more efficiently used risk management resources. An update will be provided at the next NIAC meeting where more tangible outcomes will be delineated.

Ms. Marsh summarized the next steps. The Study Group will enlist the support of representatives from across the Council. Private sector contributors with specific, scientific, and tested risk management methodologies will immensely aid the effort. Participants from the finance, energy, chemical, and transportation sectors would be welcome contributors to this effort. The broadest possible private sector coverage will yield the best possible outcome. More importantly, the Study Group needs resources to understand risk management and provide very specific feedback on the methodologies being collected, aggregated, and assessed over the coming months. Mr. Allor from ISS and Mr. Blanchette from Stanford Hospital and Clinics will be leading the Study Group for this effort. She said there is much to do leading up to the mid-point decision date, so volunteers would be greatly appreciated.

Ms. Marsh discussed the timeline in terms of the Working Group's plans. She stated she thought this group is very important based on prior discussions and the intersection of public and private sector interfaces regarding risk assessment and management. She asked if the Council had any questions.

Chairman Nye asked Ms. Marsh if the Prioritization of Cyber Vulnerabilities Working Group would have had valuable, relevant information to assist in the risk management undertaking.

Ms. Marsh said she had spoken to Ms. Susan Vismor from the Cyber Vulnerabilities Study Group earlier this afternoon and a more frequent interface would be helpful. .

Chairman Nye encouraged those with capabilities or interests in this area to support this effort. He asked if there were any questions.

Vice Chairman Chambers said the insurance industry might be a strong contributor to the Study Group.

Ms. Wong stated the need for more than Information Technology and Healthcare representation and she reinforced the need for private industry participation with the Council. She said she thought it would be extremely challenging to have the nation managing public sector risks differently than managing private sector risks. Both parties look at public safety in the same light. The integration and mutual understanding of this issue is very important to national policy.

Ms Marsh thanked Ms. Wong for the comment and said she agreed with her.

Ms. Ware volunteered to join the Working Group.

Mr. Howard Schmidt from eBay also volunteered to participate as a member of the Study Group.

Chairman Nye thanked them both and asked if there were any further questions or comments. There were none and he thanked Ms. Marsh for her presentation.

Chairman Nye then moved to the third status report. He said this Working Group addresses assuring adequate national intellectual capital to secure cyber-based critical infrastructures and is led by Mr. Alfred Berkeley, III and Dr. Linwood Rose.

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 and Vice Chairman Chambers and began by reviewing the Working Group's background from July 13th Council meeting. Dr. Rose thanked Mr. Ken Watson and Mr. Rick Holmes for joining in the Study Group's initial discussions and developing its agenda. The work is really motivated by a number of concerns. The Working Group was first concerned with America's global competitiveness in developing technically skilled workers. The Working Group was concerned about the fact that China and India those countries are graduating engineers and students from other technical areas at a much more rapid rate than the United States. Additionally, there is a fear that America's relative position to other countries, regarding analytical skills and computation methods is weak.

Initially, the Study Group focused its efforts on ensuring there are education policies in place to promote American competitiveness throughout the world. The Study Group was also concerned about research in colleges and universities as well as within private industry; industries that appear to need reinforcement include cyber-security and information security. The Study Group also discussed initiating awareness campaigns.

There are five central issues that drive the work of the Study Group. Dr. Rose said he had briefly touched upon education policy, but there are other issues needing to be addressed. He said it is important to develop incentives to attract quality students to programs providing resources to government, industry, and academia. Similarly, the Study Group is also concerned about attracting faculty to these programs to create a core on American campuses to provide instruction at the baccalaureate and advanced degree levels. Finally, there are some issues with the quality of the existing programs and a syllabus review might be needed to examine the preparation of computer scientists and information security specialists. This review is to ensure these students are adequately prepared to enter the work world and meet its existing needs. The Study Group views the cyber corps program as a measure with great potential but it still might be appropriate to see if it is meeting its original goals.

Dr. Rose said he and Ms. Ware agree that it might be appropriate for the Study Group to look not just at cyber-security specialists, but also look at infrastructure protection specialists to ensure there are enough students to handle the physical environments in infrastructure sectors throughout the country.

The Study Group is primarily interested in researching two topics. The first topic looks into adequately addressing the kind of research needed to meet the requirements of the various infrastructure sectors. Dr. Rose continued by saying the Study Group is generally interested in network and information security. Secondly, the Study Group must be sure sufficient funds are being focused in research areas to ensure needs will be satisfied. Those are some areas that the Working Group would like to explore further and make recommendations for the Council to consider.

Dr. Rose said another facet of the Working Group's work is the investigation of impediments to both research and the transfer of research results to business and industry—specifically, intellectual property laws. Dr. Rose said he had already alluded to the issue that there may not be an adequate pool of prepared people actually involved in research activities in the United States.

Addressing awareness, Dr. Rose said the Study Group initially felt it was a necessary topic. However, after further discussion, it might be more appropriate to focus on education, workforce preparation, and research. There are already a number of national organizations, professional organizations, and government entities studying awareness and the Study Group did not think it could make a unique contribution in that area. Unless the Council feels otherwise, Dr. Rose recommended dropping that item from the Working Group's agenda so as to devote more attention to the first two areas. The status report reviews activities that have occurred to date and gives some specific information about the topics the group intends to cover.

Dr. Rose said the Working Group is in the same position as the other Working Groups regarding next steps. Additionally, Dr. Rose encouraged other Council members to participate.

Chairman Nye thanked Dr. Rose and Mr. Berkeley and said the Working Group has put forth a very thorough work outline. There is an open question around awareness and he said his inclination is to follow the recommendation of those who have studied it more closely. Unless there is a contrary view, the Council will remove the awareness component of the charter as Dr. Rose suggested. Chairman Nye asked if there were any more questions or comments.

Vice Chairman Chambers stated this is a very important issue as some other countries are generating four to ten times the number of engineers and also often encouraging or even requiring in as much as 25 percent of those to focus on areas such as mathematics, science, or computer technology. If this is not remedied, the U.S. will face an uphill battle in the global market. The Vice Chairman voiced his strong support for this effort—it is an area where government must help and research. Many of the companies members of the Council work for have been a direct result of government investment. He said he thought the status report an excellent starting point.

Chairman Nye said this country often takes for granted a stream of creative ideas it has always enjoyed. He asked if there were any other comments. There were none, so the Chairman moved on to final report and recommendations of the Internet Hardening Working Group.

V. FINAL REPORTS AND DELIBERATIONS

Chairman Erle A. Nye Presiding

1. FINAL REPORT ON HARDENING THE INTERNET

George H. Conrades, Chairman & CEO
Akamai Technologies; NIAC Member

Mr. Conrades thanked Chairman Nye and said he was delighted to present the final progress report from the Internet Hardening Working Group. He said that by calling the presentation a final progress report, he meant there are some editorial changes to be made before transmission to the White House. Those minor changes aside, the content is ready for discussion and approval. The substance of the recommendations is similar to those made in the prior reviews to the Council. A key part of these recommendations center around adoption of current best practices. There is a tremendous body of existing knowledge which the private sector controls. The recommendations' focus is to sponsor and encourage research to better understand adoption and deployment rates and decision processes. Mr. Conrades said the presentation will summarize each recommendation and will go beyond current best practices to address research and development, empowering Internet service providers (ISPs), and law enforcement agencies. The Study Group has had an active and sustained contribution by more than 30 people—all of them very knowledgeable about the Internet and some of them were even there at its creation 35 years ago. He said the Working Group has focused on problems and definitions and a discussion on the issues involved will help clarify the recommendations. With that, Mr. Conrades turned the floor over to Mr. Andy Ellis to continue with the presentation.

Mr. Ellis thanked Mr. Conrades and said he intended to cover the Study Group's background and methodology. At the October 14, 2003 NIAC Meeting, President Bush asked the Council what could be done to harden the Internet. This is a pretty open question and as the Study Group matured, the members began to examine different ways of interpreting the phrase "hardening the Internet." The group decided to look at study from an infrastructural perspective. One of the key issues is to ensure a common infrastructure for national e-commerce that fosters communication. The Study Group did not tightly focus on protecting the e-businesses themselves, although there are some recommendations that do touch on this.

The Study Group's mission was to develop guidance based on best practices, and as previously mentioned, a wealth of best practices already exists. He said there are four pages in the appendix of the final report listing organizations publishing best practices. Some of this infrastructure advice is aimed at network operators and some is geared towards end-users and corporations to protect their own devices. Additionally, the Study Group also evaluated long-term technologies and strategies for making wholesale upgrades to infrastructure in order to improve current technologies and protocols. Ultimately, policy recommendations will be based on this guidance.

There were two Study Groups in existence for most of the Working Group's life. One focused on infrastructure protection and the other focused on the customer environment. In recent months, these Study Groups have merged to produce one set of conclusions to the Working Group. The group did meet weekly and Mr. Ellis thanked Mr. Conrades, Ms. Grayson, and Mr. Berkeley. These three were very active through the Study Groups' lifespan and having their active participation was truly beneficial to the group.

Fundamentally, the Study Group's challenges came in two areas. The first involves the protocols in place for the infrastructure—routing and name service infrastructures--and the way in which these systems are deployed. The protocols provide opportunities for attackers to impact availability or integrity of the infrastructure. Mr. Ellis said this is a problem as is the ease of gaining access to compromised computers in homes and offices to launch distributed denial of service attacks.

The Working Group's recommendation areas can be broken into three categories:

1. Education and awareness,
2. Understanding the adoption of security of practices and improving the percentage of people adopting these practices, and
3. Research.

Businesses maintaining the Internet infrastructure are concerned with bringing new technologies to market with an economically feasible upgrades path. That makes economic sense for the businesses that maintain infrastructure. The Study Group thinks it is important to empower ISPs to act to protect themselves against aggressors and allow the law enforcement and justice system to focus on attackers who are performing criminal activity, removing the financial incentives that currently make it a profitable business to be a criminal on the Internet.

For the recommendation addressing education and awareness, it is crucial to understand the reasoning behind adopting security best practices. The aforementioned partnerships advocating best practices were developed by talking with personnel both on the Study Group and elsewhere. Mr. Ellis said as a security professional, he was unfamiliar with ninety percent of the publication of those practices—something consistent across the entire Study Group. There is no coherent awareness campaign that reaches out across the board to everyone. When security professionals were not being targeted by or ever even see these campaigns, one wonders how many non-professionals actually come across these awareness initiatives. The industry must understand why some people are exposed to and understand these campaigns and their adoption rates so it can better tailor and target future initiatives to critical system owners.

Within the research and development arenas, there will be recommendations dealing with new tools and protocols, the ability to provide scalable and operationally implemented technologies from a security perspective, as well as key research on development areas. To empower these systems, security professionals need to reduce the ability of criminals while increasing their own abilities.

Mr. Ellis said he would discuss the first recommendation on behalf of Mr. Conrades in three parts. He said this recommendation was really the seminal recommendation from the entire report. It is important to understand why some people adopt security best practices and why some do not. What are the decision paths? How is risk management used to decide which best practices are going to be adopted and which will not? Once this understanding is achieved, security professionals can then provide end users with tools to make better decisions. There may be an absence of education about the long-term impacts of not adopting security best practices, but providing firms and organizations with some background may increase the odds for adoption. Adoption must be understood and measured for use as a metric to effectively gauge all future awareness campaigns. There are standard technologies applied within the infrastructure environment to ensure packets can only come from legitimate, authorized locations and to ensure infrastructure providers are appropriately routing traffic. This is a best current practice many tier one providers implement but is neglected by many tier two and three providers. Advocating this from the Council's bully pulpit is a direct way to influence agencies to adopt these best practices.

The third part of the first recommendation targets the country's Internet security awareness. Unprotected end-users are unwittingly having their machines used in a massive network for distributed denial of service attacks. These people are already targeted by awareness programs, albeit ineffectively. The Study Group examined an anecdotal study from one service provider suggesting 40 percent of users regularly implement security patches. 40 percent also begin patching their systems if there is an exploit reported. The remaining twenty percent will never implement security patches on their systems. These statistics may or may not be universally true, but it's very difficult to obtain solid information on these phenomena. The numbers affected suggest the capacity for an attack is quite large. Reducing this weakness and ensuring system maintenance at an appropriate security level is critical to protecting cyber infrastructure.

The fourth component ties into the Education and Awareness Working Group. Ensuring an understanding of how to properly provide instruction on secure software development is important to protecting the Internet's core and ensuring software defects are not rapidly spreading. As Ms. Vismor discussed earlier, the number of security vulnerabilities in systems is increasing. There must be better development practices, development methodologies, and management processes applied to the system.

The fifth piece targets enterprises and the oversight for major collections of computer systems. There are already awareness activities aimed at boards of companies. Again, as with reaching to tier-two and tier-three network partners, small and medium businesses also need to be informed. This education campaign must continue and there needs to be a single voice advocating security awareness and security management techniques.

Moving into research, the Study Group began by discussing route and packet filtering. While filtering is a step toward improving infrastructure security, there ultimately should be an automated route registry infrastructure. There is not much disagreement about this within the Internet community but there is disagreement on how to implement the registry and the best way to reach a state of automated infrastructure. Fundamental to many of these discussions is the idea that any proposal account for the network providers' financial constraints and their hardware limitations. Additionally, it is important to look at approaches to operational risks in emergencies when the state of the Internet must be rapidly adjusted and to ensure any protocol will have the flexibility to handle all major issues preventing the implementation of an automated route registry infrastructure. Research provides a means and method of improving technology and is a key recommendation.

Security management tools are an area where the capabilities of security professionals must align those of network providers. There must be better technologies to track and manage the wealth of information available on the Internet. As network providers frequently upgrade technologies, security technologies must be upgraded at the same rate. If this is not possible, then there is the chance more data than can be monitored will be moving and it will be more difficult to detect attacks underway.

This issue exposes the need to specifically fund the ability to collect data. Obviously, data must be collected before it can be analyzed. The Study Group also sees a need for sustained and improved funding to analyze flaws in large systems. Networks and the software they use are becoming increasingly complex. It is beyond the ability of a developer to immediately recognize or understand flaws they may have written into their code. The software and networks are simply too complex. Having tools to intelligently detect flaws detected in communications infrastructures could prevent the release of flawed infrastructure and protocols before they are out in the field.

The third recommendation speaks to the need to improve information sharing within the Internet industry itself. Information sharing mechanisms have been shown to aid other infrastructures; this should be done for the Internet. The ability for providers and vendors to focus on Internet problems and to interact with intelligence and law enforcement agencies will be critical to giving the private sector first responder abilities.

The second part of the third recommendation is geared toward addressing the large amount of inconsistencies in law enforcement operations at both the national and local levels. Any Internet Service Provider can certainly describe their interactions with law enforcement. Law enforcement resources should be strengthened at both levels, ensuring focus on Internet security breaches. Law enforcement should also all have consistent training, forensic capabilities, and a judicial infrastructure supporting them that is equally trained and prepared to support them. This judicial infrastructure should provide an Internet investigative capability to reduce a criminal's incentive to attack infrastructure and also should also increase the potential penalty for cyber crime. Mr. Ellis thanked the Council and concluded his presentation.

Chairman Nye thanked Mr. Ellis and Mr. Conrades and asked the Council if there were any questions or comments.

Chief Gallegos asked if there were examples in which some states handled the law enforcement aspect of these recommendations better than others. Around the nation, some states really lag behind others in the capability to effectively conduct cyber investigations.

Mr. Conrades said conversations with law enforcement professionals produced feedback suggesting the environments they work in are not consistent. As a first step, there is the need for consistent training across the law enforcement spectrum. He stated there is a striking difference in communication quality from law enforcement professionals across the country.

Seeking clarification, Mr. Berkeley asked if there was any best practices deployment data, especially regarding route and packet filtering.

Mr. Conrades said it was very difficult to get service providers to share that information. He knew DHS had undertaken some studies in gather more ISP information, but it is still a very difficult task. This kind of information is considered to be at the company-confidential level and is guarded for the state of their own security.

Vice Chairman Chambers congratulated Mr. Conrades' Working Group and said this assignment was a difficult one but was handled very well. He said he felt members of the NIAC would implement the best practices alone and perform some of the recommended research. While there is no such thing as a completely secure environment, these recommendations potentially make it very difficult on the criminals.

Vice Chairman Chambers moved that the Council accept the Hardening the Internet final report. The motion was seconded.

Chairman Nye asked if before the actual vote, the Working Group cared to discuss the call for legal remedies to enforce the implementation of these best practices.

Mr. Conrades said there had been discussion around the regulatory environment, especially as they related to corporations. The Study Group looked at what factors actually made end users adopt these best practices, evaluating the success of different kinds of regulation like Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), or the Federal Information Security Management Act (FISMA). These are all going to be solid data points and will aid in the understanding the value of industry regulation and in providing legal incentives.

Chairman Nye thanked Mr. Conrades and asked if there were any more questions or comments. Seeing there were none, the Chairman called for a vote. The report was unanimously approved.

Chairman Nye thanked the Working Group again and said he thought this was a very helpful report and will go a long way towards continuing the Council's reputation.

Chairman Nye moved on to the final report and recommendations from the Common Vulnerability Scoring System. He asked Vice Chairman Chambers to begin the presentation.

2. FINAL REPORT ON THE THE COMMON VULNERABILITY SCORING SYSTEM	*Vice Chairman John T. Chambers; and John W Thompson,* Chairman & CEO, Symantec Corporation; NIAC Member

Vice Chairman Chambers thanked the Council for the opportunity to share the Working Group's final report and lone action item. Mr. John Thompson is traveling but his remarks will be ably presented by Mr. Rob Clyde, Chief Technology Officer at Symantec. This report spun off the vulnerability discussion at the July meeting of the NIAC. The first cut at this task seemed like it would be a very simple, but it turned out to be much more complex. The Working Group believes it will provide a new and effective standard method for scoring vulnerabilities. While the Working Group will make this recommendation, the Council should view this as a methodology, not as a tool or a job. This group must find a permanent home in order to provide regularly updated tools and to distribute recommendations. Each member of the Council should have received a final copy of the report.

The key concepts of the report is assigning different scores to an issue based on a three factors.

1. Severity,
2. Urgency, or

3. Priority.

This approach can be easily replicated and applied throughout the members' respective firms. Vice Chairman Chambers emphasized that four members of the Study Group have actually implemented this system and are already receiving benefits from it. The Vice Chairman then turned the floor over to Mr. Clyde.

Mr. Clyde thanked the Vice Chairman and reiterated the system is in fact an initial methodology, but the Study Group believes it is workable. There are already organizations using it and Symantec has committed to incorporating it into its own scoring process—a process used by many around the world. The Study Group just completed incorporating the changes recommended by the NIAC members after the report was distributed for initial evaluation and trial. Those changes are now in place and the updated document has been distributed for final review. The development team assembled earlier will remain in place and be available for training and assistance until an actual home is decided upon.

As previously discussed, the system must be updated periodically. Tools will need to be built for use by both end-users and vendors alike. The Study Group will ask for the Council's help to identify a vendor-neutral permanent location that is also not beholden to any specific or single government entity. This location must also have a demonstrated capability and experience in dealing with and scoring vulnerabilities.

Looking at the CVSS itself, there are three basic parts or subsections to the scoring method. Each method builds upon the previous one. The base score is the first calculation done and incorporates invariable metrics that do not change over time regardless of the environment or time. The temporal score modifies the base score and hinges on the existence of an available exploit or whether mitigations or other solutions are in place. The temporal score also may change overtime. The environmental score modifies the combined base and temporal score and becomes the final score-- it is specific to individual user environments.

Continuing further, Mr. Clyde said the base score represents the vulnerability's innate characteristics and does not change over time. A key component of the base score is the measurement of the vulnerability's impact in three key areas:

- Data confidentiality,
- Data integrity, and
- Information availability.

Data confidentiality refers to whether the vulnerability will allow an unauthorized third-party to access private information. Data integrity refers to whether the unauthorized third-party will be able to change or tamper with that data. Finally, information availability refers to whether the vulnerability allows someone to deny service to authorized users, preventing them from accessing the information they need. All three of these are quite serious and are taken into account as a component of the base score. The base score essentially measures severity.

Mr. Clyde continued by discussing the temporal score which builds upon and modifies the base score. Unlike the base score, the temporal score can change over time. For example, hackers may develop exploit tools that actually take advantage of the vulnerability. Clearly, these tools increase the likelihood the vulnerability will have a negative impact around the world. This might modify the base score. On the positive side, vendors might produce patches or develop workarounds or mitigations that positively modify the base score. Like the base score, the Study Group expects the temporal score to be something vendors calculate and publish. Typically, this is something vendors put together. Because time exposure can affect the seriousness of a vulnerability, the temporal score could be thought of as a measure of urgency.

The third and final score is the environmental score. If a firm has an effective operating system with a vulnerability throughout the enterprise, the environmental score will likely be high. On the other hand, if that vulnerable operating system does not exist anywhere in the company, the environmental score may be low, perhaps even zero. The environmental score includes provisions for a vulnerability's potential for collateral damage. Collateral damage might include physical damage, human casualties, or significant financial losses. This allows the user flexibility to modify the temporal base score to account for these critical issues. Additionally, it also allows for future growth of this methodology as physical and cyber security worlds continue to converge. Another way to think of the overall environmental score is as a measurement to determine priority.

The final issue with which the Working Group is faced is determining permanent hosting of the CVSS to work with vendors, users, and coordinators to develop tools so each of these groups can make use of this methodology. At this point, Mr. Clyde turned the floor back to Vice Chairman Chambers.

Vice Chairman Chambers thanked Mr. Clyde and all the members of the Working Group and its Study Group. Additionally, he thanked the four organizations that implemented the CVSS:

- Symantec
- Union Pacific
- Akamai
- American Waterworks

Vice Chairman Chambers then asked the Council to approve the final report. Also, with the Council's agreement, the Working Group wished to submit this methodology to the Internet Engineering Task Force (IETF) as a best practice "Internet Draft." Finally, he said it was also important to discuss finding a home for this methodology. He said he would mention some of the suggestions, not ranking them in any particular order. The Computer Emergency Response Team at Carnegie Mellon is a unit with years of experience and respect as a multi-vendor coordinator, and close collaboration with DHS on US CERT. A second site might be the Forum of Incidence Response and Support Teams, a global organization of cyber incident responders. A third host might be Netter which is already hosting the common vulnerability and exposure database used by Department of Defense and worldwide incident response teams. The Vice Chairman again suggested the Council approve the report and form a small subcommittee. He said he and Mr. Thompson would be happy to head that and to review these organizations, recommendation, and to transition this responsibility in thirty days. He again thanked the Council.

Chairman Nye thanked Vice Chairman Chambers and Mr. Clyde and asked if there were any questions or comments.

Mr. Carty asked the Vice Chairman if the potential hosts actually entertain the possibility of providing a home for the system.

Vice Chairman Chambers responded, saying he thought they all would very much entertain the possibility. The Council needs to look at each of their capabilities. Some of them might be more qualified than others. He said this was the reason he recommended two individuals take responsibility for making hosting suggestions and was open for constructive criticism.

Mr. Davidson asked if the Working Group contemplates a revenue stream to support an operation that is hosted somewhere.

Mr. Clyde said this is clearly a methodology, but all the tools have not been put together thus far. Some of the examples Vice Chairman Chambers listed as potential hosts for this system might consider a way to recoup some of the costs they would incur in development. It might also fall into the category of something that some of these groups would be capable of gaining a government grant for as well. He said he imagined some companies would be quite interested in having such tools and even consider paying for that right. Certainly, there are companies that will be providing these types of scores and that will be of use to customers. So there will be indirect revenue if you will that would come from that kind of a service.

Chairman Nye asked if there were any further comments or questions.

Chief Gallegos moved for a vote to accept the report and it was seconded. The report was unanimously accepted.

Chairman Nye thought without formally creating a subcommittee, the committee comprised of Vice Chairman Chambers and Mr. Thompson should proceed with the implementation phase. He said the Council appreciates them taking on the additional responsibility and he trusted they would report back on what they determined.

Ms. Ware thanked Vice Chairman Chambers and Mr. Thompson for their work, saying she thought it had practical and tactical applications.

Mr. Berkeley asked if it might be worth doing a Harvard Business Review article or publicizing it in some other way to better advertise these findings.

Vice Chairman Chambers said the two organizations will both be available for input and sharing and will contact the four current adoptees to obtain feedback. He said he thought the idea of a Harvard Business Review is also a good idea.

Chairman Nye said the Vulnerability Scoring report has potential for current application and he thought it would reap benefits. With that, Chairman Nye turned the floor to Mr. Martin McGuinn, Chairman of the Prioritization of Vulnerabilities Working Group.

3. FINAL REPORT AND DISCUSSION ON PRIORITIZATION OF CYBER

Martin G. McGuinn, Chairman & CEO
Mellon Financial Corporation, NIAC Member

VULNERABILITIES

Mr. McGuinn thanked Chairman Nye and said this presentation is an update on the activities of the Prioritization of Cyber Vulnerabilities Working Group. Since the last meeting in July, the subject of cyber vulnerabilities has continued to cause concern and generate research. Several new studies have been released, including the most recent version of the Symantec Internet Threat Report. Some of the trends identified in this report are very interesting and include the fact that the average time between a vulnerability's announcement and the appearance of an exploit has shrunk to 5.8 days. This implies organizations have less than a week to patch all their systems affected by the vulnerability. An average of 48 new vulnerabilities are appearing in software codes each week. The number of systems infected by covertly installed "bots" has grown from two thousand to thirty thousand computers. In the first six months of 2004, worm traffic was observed originating from four percent of the Internet address space controlled by Fortune 100 companies. Over the past six months, Symantec documented more than 4,496 new Windows viruses and worms. This is over 4.5 times the number identified in the same period during 2003. The first malicious worm for mobile devices was reported and it is expected that attempts to exploit mobile devices will only escalate.

Mr. McGuinn continued, saying the composition of these attacks is always evolving. Using the recent Trojan Horse "JFScott" as an example, this malicious code was inserted on to at least 630 web servers including well-known sites such as the Kelly Blue Book car pricing service and Minerva Health, a provider of online financial services for the healthcare industry. Users visiting these sites had software surreptitiously downloaded onto their machines. The software recorded their keystrokes and transmitted back to their attackers. This stolen information could be used to determine people's credit card numbers and passwords. A Russian virus ring is suspected of initiating the attack and the FBI and Scotland Yard are investigating. The virus was designed to evade current anti-virus products would not detect the malicious code. He said once the major Internet service providers became aware of the attacks, they blocked access to the Russian website that served as a launch pad. This incident was reported in the September edition of computer magazine Institute of Electrical and Electronics Engineers (IEEE). Mr. McGuinn said this anecdote provides some perspective on information to be discussed concerning the results of the Study Group's survey.

Mr. McGuinn stated the report will outline findings based upon the Study Group's research and survey. He noted the information's confidentiality of the information provided dictated the update will be an extract of the more sensitive update provided earlier to the Study Group.

Mr. McGuinn briefly reviewed the purpose of the Working Group. The group is attempting to rank the impact of cyber attacks on various sectors. This task is in response to a question originally posed by President Bush at the July 22, 2003 meeting when he asked if the Council is ranking areas vulnerable to cyber attacks. At that time, he introduced the Study Group Chair, Ms. Susan Vismor, to continue

Ms. Vismor thanked Mr. McGuinn as well as other members of the Study Group. She extended a special thanks to Mr. Scott Borg, a Study Group member from Dartmouth University who provided the Study Group with precepts outlining the survey's methodology and design. The survey's distribution was intended to reach key representatives of critical infrastructures. This was discussed at both the July and April meetings of the Council and differs from the Department of Justice survey in that it works with a much smaller subset. With a smaller subset, the Study Group could obtain more illustrative data to review and use to draw conclusions.

The Study Group asked respondents to identify three key network information systems and how their respective organizations used them. In order to gather economic metrics around the systems, the Study Group asked for revenues driven by these systems. Many respondents were unwilling to provide their revenue numbers and some did not track revenue at an application level. From that perspective, direct economic metrics are difficult to derive. The Study Group did ask about implications to national security and emergency preparedness, receiving responses from many on these categories. In terms of these organizations' dependency on other critical infrastructures, the respondents were asked to rank these dependencies so as to generate a weighted average ranking to determine the most critical infrastructure.

The survey asked the organizations to evaluate possible consequences of various types of cyber attacks to key systems. Ms. Vismor said this was an interesting point—when the survey was first being compiled, the Study Group thought a chief threat would stem from an attacker accessing information on a system, seeing codes, or inserting false data. This viewpoint was altered by the emergence of the "JFScott" virus. Consequently, the survey was really not as forward looking as it could be in terms of attack types and this gap needs to be addressed when organizations are doing disaster recovery and business continuity planning.

The Study Group's first key finding is that dependency on network-based systems is pervasive across all sectors. Components of critical infrastructure rely on a variety of network-based systems. Based on the findings, the Study Group identified the crucial sector upon which all other sectors must depend. To further expound on the dependencies of network-based systems, Ms. Vismor did use the Slammer virus as an example. This is probably the largest attack against the Internet in history. In theory, there are over four billion IP addresses, Slammer scanned through every one of these addresses in less than fifteen minutes. She said this is analogous to an automated dialing system dialing all the phone numbers in the world in fifteen minutes--not everyone would answer but it would create a lot of network congestion. Although Slammer was not intended to take down critical systems or inflict massive damage, it wreaked havoc. It took down a major airline's reservation system, shut down one of the nation's largest banks and made 13,000 automated teller machines (ATMs) unavailable. It forced the emergency 911 dispatching system in suburban Washington to resort back to paper. 300,000 cable modems went dark in Portugal, all of South Korea lost their web access, and 27 million people lost cell phone or Internet services. The estimated cost is approximately $1 billion. This is just one small example of a risk. The answer to the President's question on whether or not the Council is ranking critical infrastructures' vulnerabilities to cyber attacks is multi-faceted. The degree that any sector is vulnerable to a cyber attack is dependent on a number of characteristics.

Ms. Vismor carried on with the third key finding, an answer to the President's question. The degree that any sector is vulnerable to a cyber attack depends upon several characteristics:

- The type of attack
- The scope of the impact
- The time of the attack

- The duration of the outage

In terms of the final key finding, a number of respondents referred to their current capabilities for disaster recovery. While the transition to a back-up system is not generally as efficient as the original primary system, it does provide some protection. This was not something the Study Group initially targeted but appeared in the comments of people indicating attacks would not be as damaging as feared because there were already good practices and close, thorough business continuity.

Ms. Vismor then began to address the recommendations the Working Group developed. The first recommendation would direct sector agencies to cooperate with each of the critical infrastructure sectors so as to more closely examine the risks and vulnerabilities of providing critical services over network-based systems. In reviewing the findings with DHS, continued work to explore these types of issues appeared to be potentially beneficial. The sector agency should aid in facilitating these efforts. While there is benefit to working across sectors, there is also benefit in further identifying critical failure points within a sector. During a time of crisis, these critical areas could be providing an indication of priority consideration where appropriate.

The Working Group's second recommendation flows from the first recommendation and would direct DHS and lead agencies to identify potential failure points across federal government systems and to encourage similar cross-sector analysis by the private sector in concert with DHS, provided DHS can assure protection of sensitive results. Clearly, there are critical applications within sectors that can be thought of as points of failure. Sectors should understand what failure points exist and should work to mitigate issues around them. For example, mitigation strategies could include determining where there is redundancy, either across sectors or within the company itself.

Ms. Vismor proceeded to outline the third recommendation--encouraging sector and cross-sector coordinating groups to establish and/or support cyber security best practices or sector standards. Some sectors have established best practices regarding cyber security issues and hedge management. For example, the energy sector is working on the update to Cyber Security Standard 1200--Cyber Security Standard 1300. Through the BITS industry group, the financial services sector has developed best practices concerning telecommunications diversity and redundancy.

The Working Group's fourth recommendation would advise DHS to sponsor cross-sector exercises to help sectors better understand the impact of a cyber attack on their own sector as well as the other sectors on which they depend. The best way to prepare a response to a major cyber attack is to practice what steps might be taken in such an event. DHS should provide a mechanism to foster this understanding in a cross-section of key players in critical sectors, government, and emergency services to prepare these interdependent areas for the roles they might play in a cyber attack.

The fifth recommendation is to instruct federal agencies to include cyber attack scenarios in protective measures in their disaster recovery planning and to encourage sector coordinating groups to include these scenarios and protective measures in their disaster recovery planning. The Working Group recommends federal agencies address cyber attacks in their own disaster recovery planning. In reviewing information on the Sans Institute website, it is exceedingly clear government agencies are frequently targeted by hackers. From this data, a clear question arose. How many government and military sites were hacked in 100 days? The answer was 37 sites. By spring 2001, there had been one site reported as defaced. The second part of the recommendation addresses the private sector. The Working Group recommends sector coordinating groups encourage private companies to include cyber attacks as a scenario they mitigate in their respective business recovery plans. The only way to effectively know how to deal with such an attack is through planning and practice.

The sixth recommendation encourages law enforcement to prosecute cyber criminals, identify thieves, and publicize these efforts. Cyber crime must be viewed as a criminal act. The Working Group is encouraged that companies and government are beginning to see positive developments in this area. For example, Microsoft has established a $5 million reward fund for apprehending cyber criminals. This action led to the arrest of the Sasser worm creator and a $250,000 reward to the informant. Unfortunately, there is also a trend in which the motive for hacking is moving away from leisure activity to an opportunity for illegal income. The increased use of “bots” has been reported; they are a threat as they globally scan networks for weaknesses. Six arrests were made in four different countries where cyber criminals were using extortion to illegally obtain money. In addition to the expense and productivity loss hackers create, it is also important from a strategic standpoint to be able to separate digital graffiti and crime from attacks sponsored by other governments and/or terrorist networks.

The seventh recommendation promotes awareness of cyber security best practices on the corporate, government, small business, university, and individual levels. Ms. Vismor referred to NASA’s effectiveness in prompting an initiative to identify and address high priority vulnerabilities through best practices. NASA reduced the number of vulnerabilities on their 80,000 systems from 1.3 per machine to less than .16 per machine in twelve months. They continued to work on eradicating vulnerabilities and over the next twelve months reduced it further to fewer than seven vulnerabilities per thousand systems. With this final point, Ms. Vismor turned the floor back to Mr. McGuinn who concluded the presentation.

Chairman Nye thanked both Mr. McGuinn and Ms. Vismor for their very thoughtful and thorough report. He asked the Council if there were any questions or comments.

Vice Chairman Chambers said his experience chairing a Working Group addressing a similar topic provided him some insight on the true difficulties of the task assigned to Mr. McGuinn and his Working Group. He said Ms. Vismor did an excellent job of summarizing the findings and the Working Group’s recommendations and he thanked the group for accomplishing its goal. The Council realizes some of the answer depends on prioritization and some of the next steps might almost rival Sarbanes-Oxley in terms of the time needed to properly prioritize a firm’s vulnerabilities. He suggested the final report include a modification to recommend its aid in prioritizing what had already been done. The Vice Chairman reiterated he thought the group did an excellent job and handled a challenging task.

Mr. Conrades noted a number of recommendations from the different Working Groups seemed to be triangulating around similar recommendations, something he hoped might add weight to the Council’s recommendations. He stated he thought this was a good development, saying it is always a good sign when different groups coming from different angles keep returning to common themes.

Chairman Nye asked if there were any further questions or comments. Hearing none, he said it was appropriate for the Council to consider the approval of this report.

There was a motion made to vote and it was seconded. The report was unanimously approved and the Chairman thanked the Working Group again, lauding them for their work.

Ms. Wong asked for a clarification as to Vice Chairman Chambers' suggestion the recommendations be submitted to DHS.

The Vice Chairman said he thought the complexity of some of the things the Council is asking for should be prioritized by DHS. Many of the items requested are very complex and might require substantial time, resources, and funding. This being the case, there are two options. Either more work be done by the Working Group or the recommendations are sent to DHS to prioritize which elements of the recommendation go forward. He said he did not think the former was wise and the latter seemed the best course of action. He suggested the recommendation go forward with the appropriate caveat.

Ms. Wong said the charter of the NIAC allows and encourages this Council to provide advice directly to certain agencies such as DHS and other sector specific agencies who deal with critical infrastructure protection. The course of action is the Council's choice.

Vice Chairman Chambers said the Council has to make the call. This endeavor is quite complex and might require a huge amount of resources. He liked Ms. Wong's offer of consolidating common themes but ensuring compliance with the President's original task. He said he wanted to be sure the Council did not put an unreasonable burden on any organization affected by its recommendations including the White House, DHS, or the NIAC itself.

Mr. McGuinn agreed with this approach.

Chairman Nye interpreted the next steps as submitting this to the White House per usual protocol with the advice of allowing DHS to prioritize the recommendations. He again thanked the Working Group for their efforts under difficult circumstances. The Council certainly appreciated their hard work.

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

There was no new business.

VII. ADJOURNMENT *Chairman Erle A. Nye*

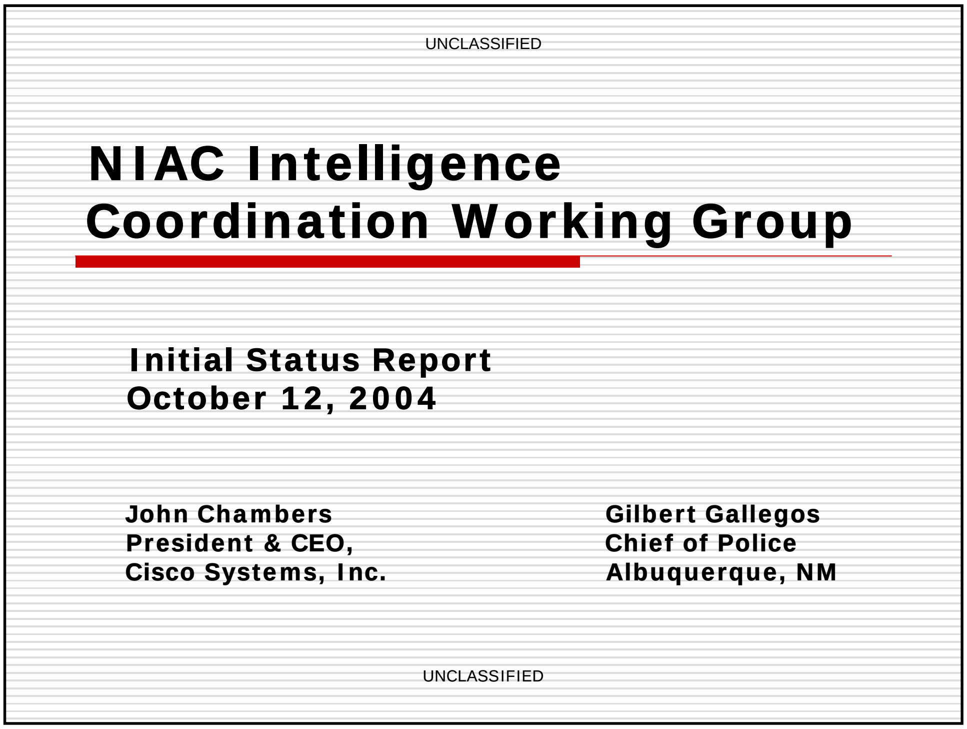
Chairman Nye said he wanted to mention that Mr., Archie Dunham, Chairman and CEO at ConocoPhillips, has retired and resigned from the Council Chairman Nye said he was a good contributor and he had personally written to him to express the Council's appreciation.

Chairman Nye thanked the Council and all those in attendance for their participation and said he looked forward to the next meeting in January. He encouraged everyone who had not yet signed on to the new Working Groups to join in. He said the Council had been very diligent and faithful and he wished everyone the best. With that closing, Chairman Nye adjourned the meeting.

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

By: ______________________ Dated: 1/11/2005
Erle A. Nye, Chairman

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

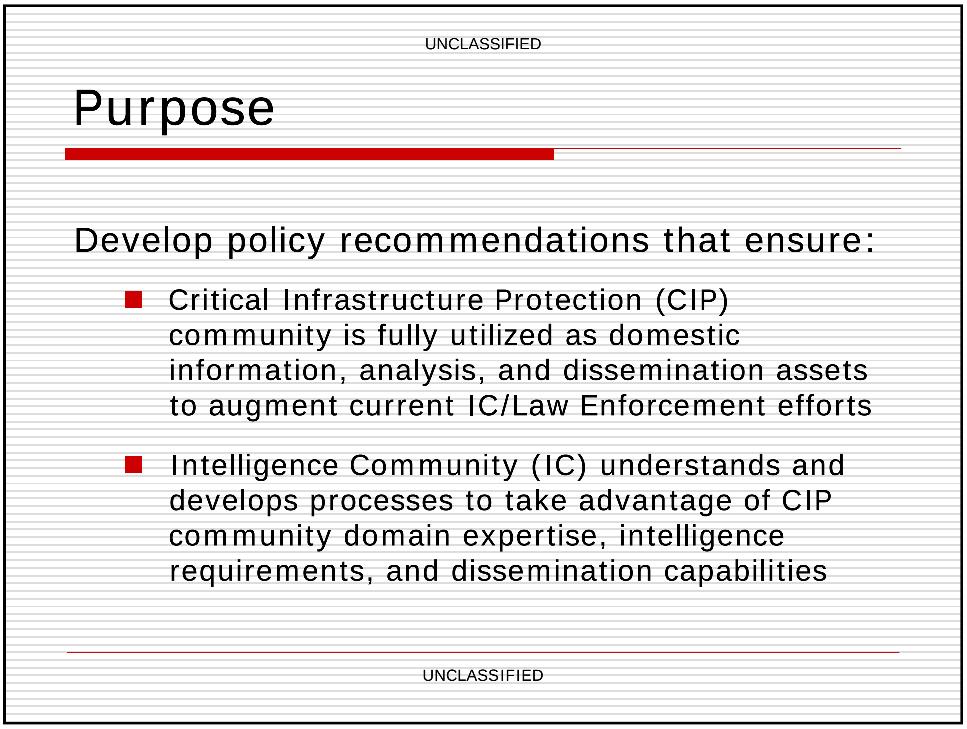


NIAC Intelligence Coordination Working Group

Initial Status Report
October 12, 2004

John Chambers
President & CEO,
Cisco Systems, Inc.

Gilbert Gallegos
Chief of Police
Albuquerque, NM



Purpose

Develop policy recommendations that ensure:

- Critical Infrastructure Protection (CIP) community is fully utilized as domestic information, analysis, and dissemination assets to augment current IC/Law Enforcement efforts
- Intelligence Community (IC) understands and develops processes to take advantage of CIP community domain expertise, intelligence requirements, and dissemination capabilities

NIAC IC Working Group Focus

- □ In what ways can the Intelligence Community (IC) help the CIP community?
- □ In what ways can the CIP community help the IC?

Who is the Intelligence Community?

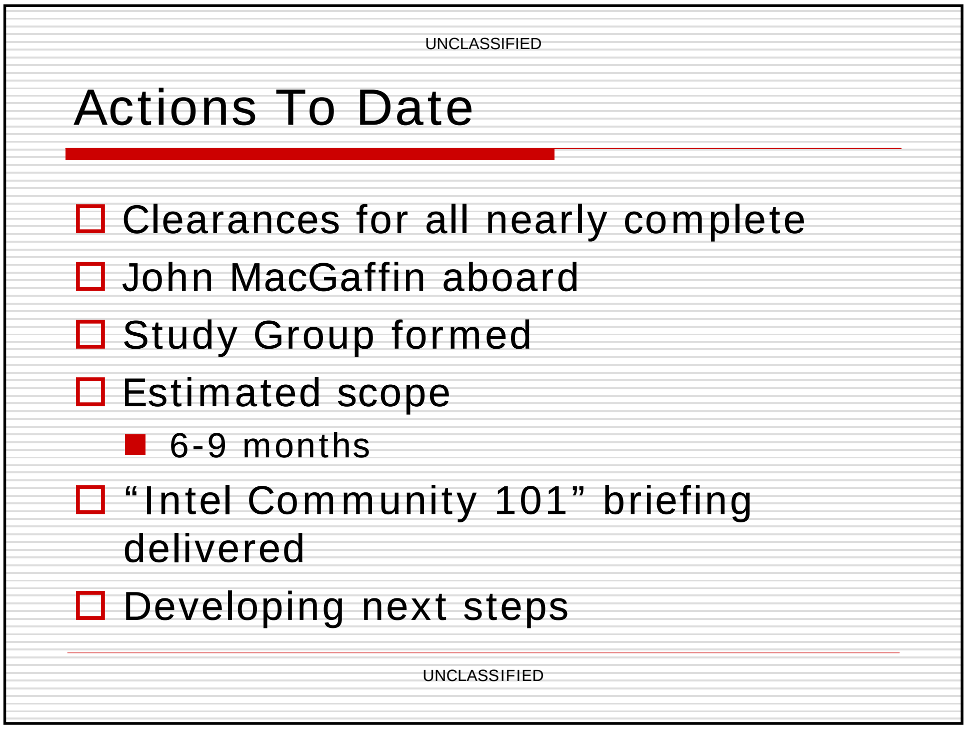
- □ Department of Defense
  - Defense Intelligence Agency
  - Air Force Intelligence
  - Army Intelligence
  - Navy Intelligence
  - Marine Corps Intelligence
  - National Geo-spatial Intelligence Agency
  - National Reconnaissance Office
  - National Security Agency
- □ Central Intelligence Agency
- □ Department of Energy
- □ Department of Homeland Security
  - Information Analysis Division
  - Coast Guard Intelligence
- □ Department of State
- □ Department of Treasury
- □ Federal Bureau of Investigation

Who is the Critical Infrastructure Protection Community?

- □ Information Technology
- □ Telecommunications
- □ Chemical
- □ Transportation
  - ■ Mass transit
  - ■ Aviation
  - ■ Maritime
  - ■ Ground/surface
  - ■ Rail
  - ■ Pipeline systems
- □ Emergency Services
  - ■ Firefighters
  - ■ Law enforcement
  - ■ Emergency medical
- □ Postal and Shipping
- □ Financial Services
  - ■ Banking
  - ■ Brokerages
  - ■ Insurance
- □ Energy
  - ■ Electric power
  - ■ Oil & natural gas
- □ Water Treatment, Storage, & Delivery
- □ Agriculture
- □ Food Safety
- □ Health Care
- □ National Monuments and Icons
- □ Defense Industrial Base

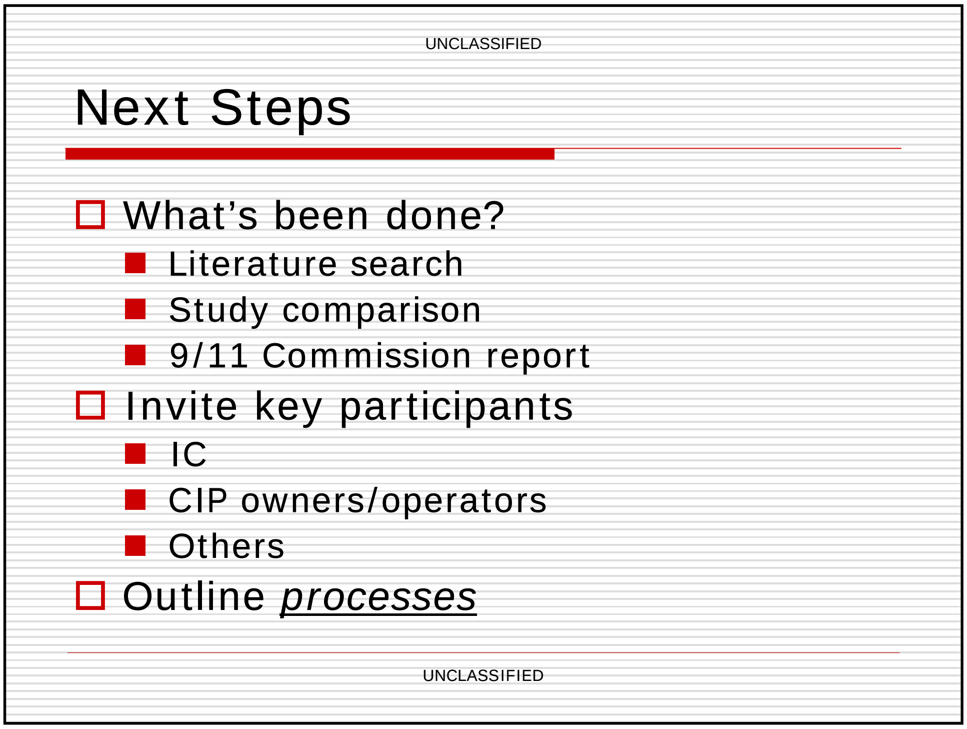
Intersection between IC and CIP

- □ Identification of foreign threats to US CIP interests
- □ Dissemination of foreign threat information to US CIP interests
- □ Disruption of foreign threats to US CIP interests where the disruption is carried out on foreign soil
- □ Coordination with US law enforcement when threat comes ashore in the US, or when threat is domestic



Actions To Date

- Clearances for all nearly complete
- John MacGaffin aboard
- Study Group formed
- Estimated scope
  - 6-9 months
- “Intel Community 101” briefing delivered
- Developing next steps



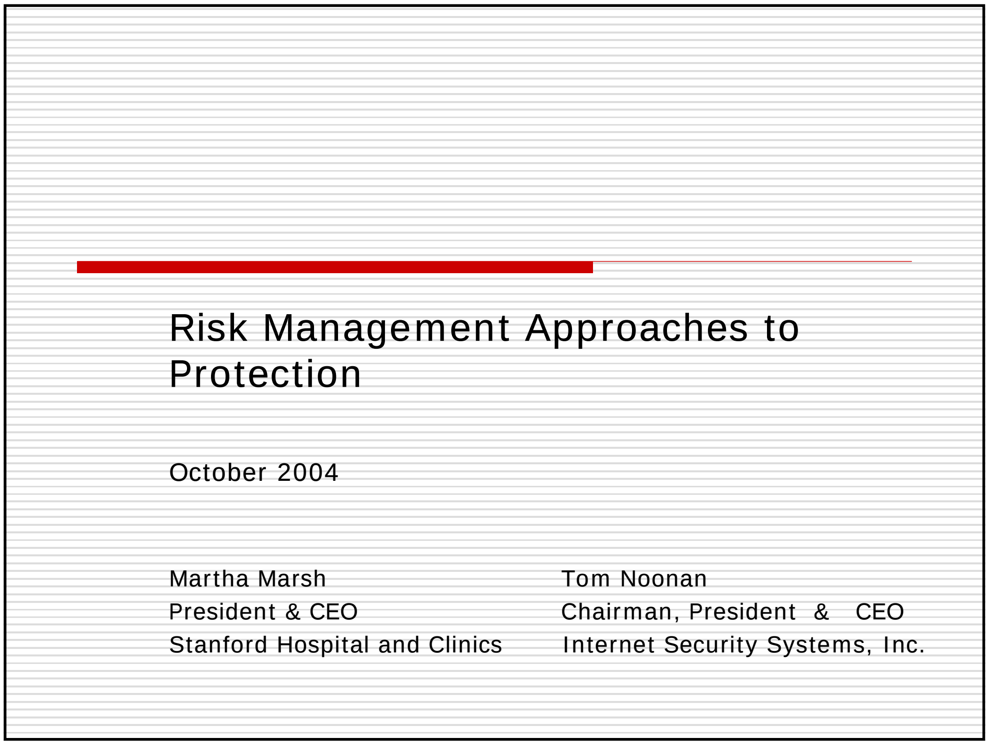
Next Steps

- What’s been done?
  - Literature search
  - Study comparison
  - 9/11 Commission report
- Invite key participants
  - IC
  - CIP owners/operators
  - Others
- Outline *processes*

Discussion

- Questions?

ATTACHMENT B:
Status Report on Risk Management Approaches to Protection

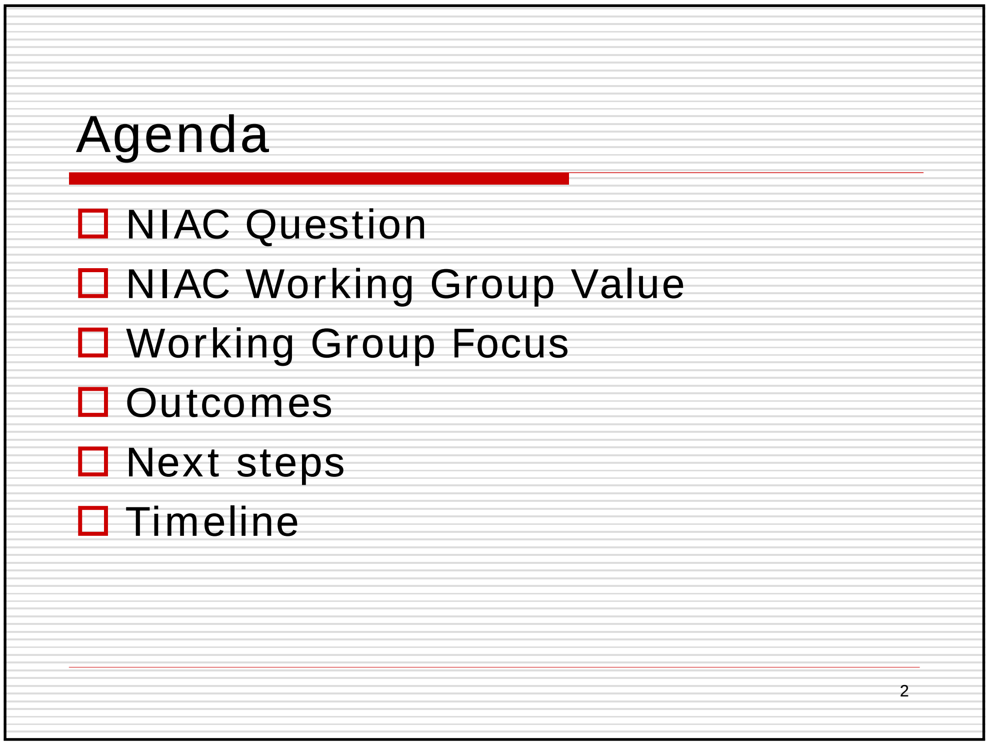


Risk Management Approaches to Protection

October 2004

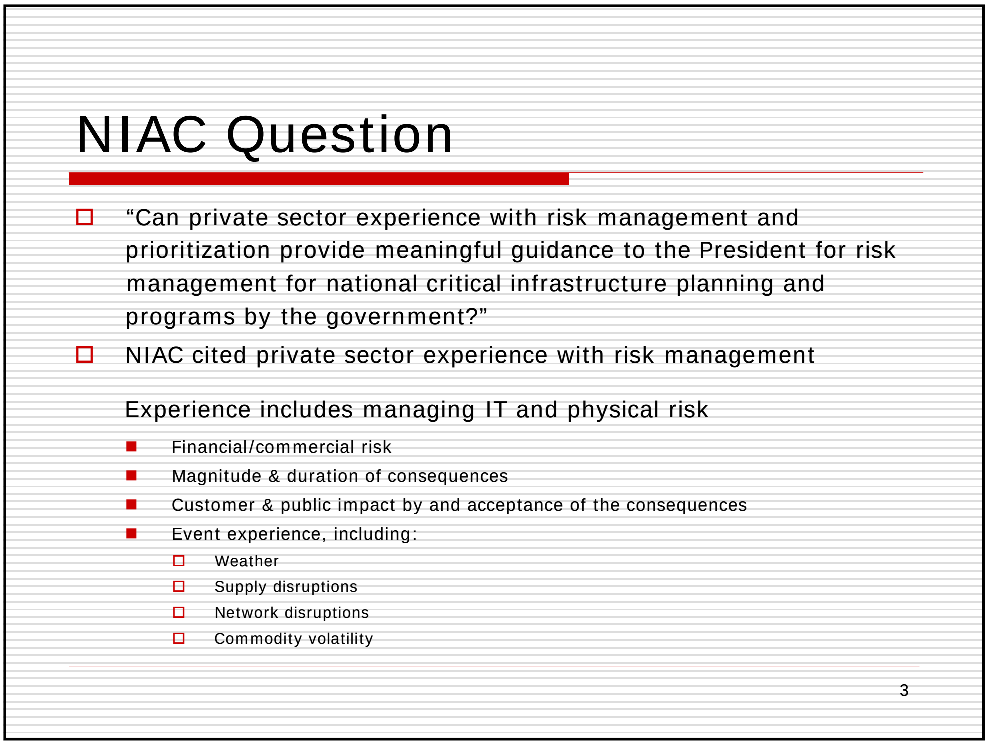
Martha Marsh
President & CEO
Stanford Hospital and Clinics

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



Agenda

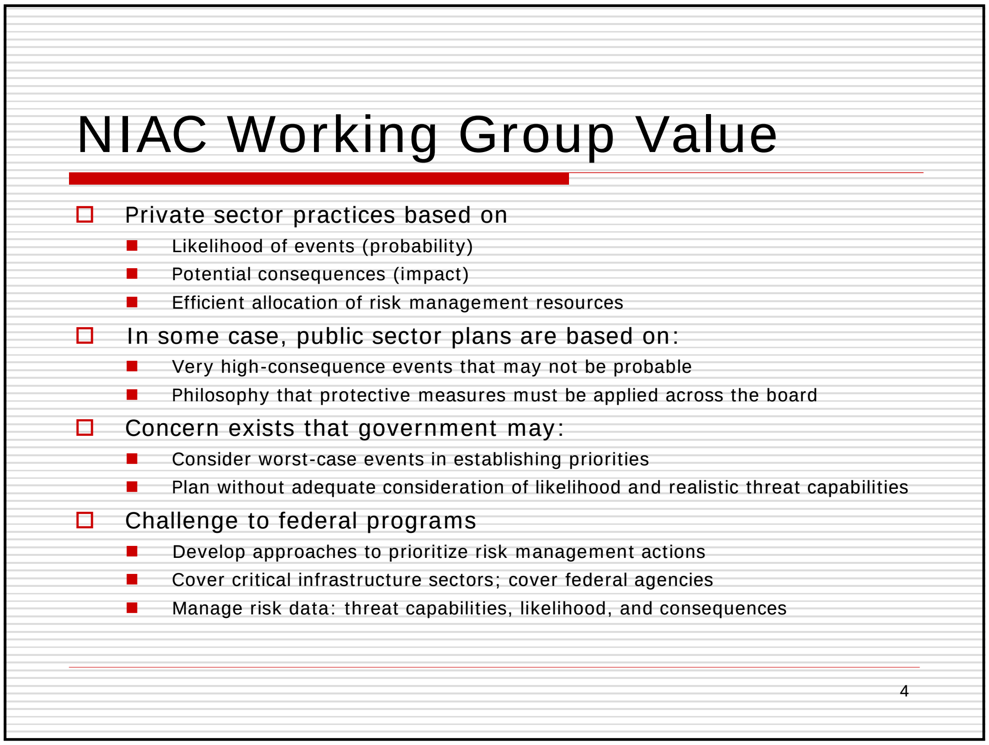
- NIAC Question
- NIAC Working Group Value
- Working Group Focus
- Outcomes
- Next steps
- Timeline



NIAC Question

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

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



NIAC Working Group Value

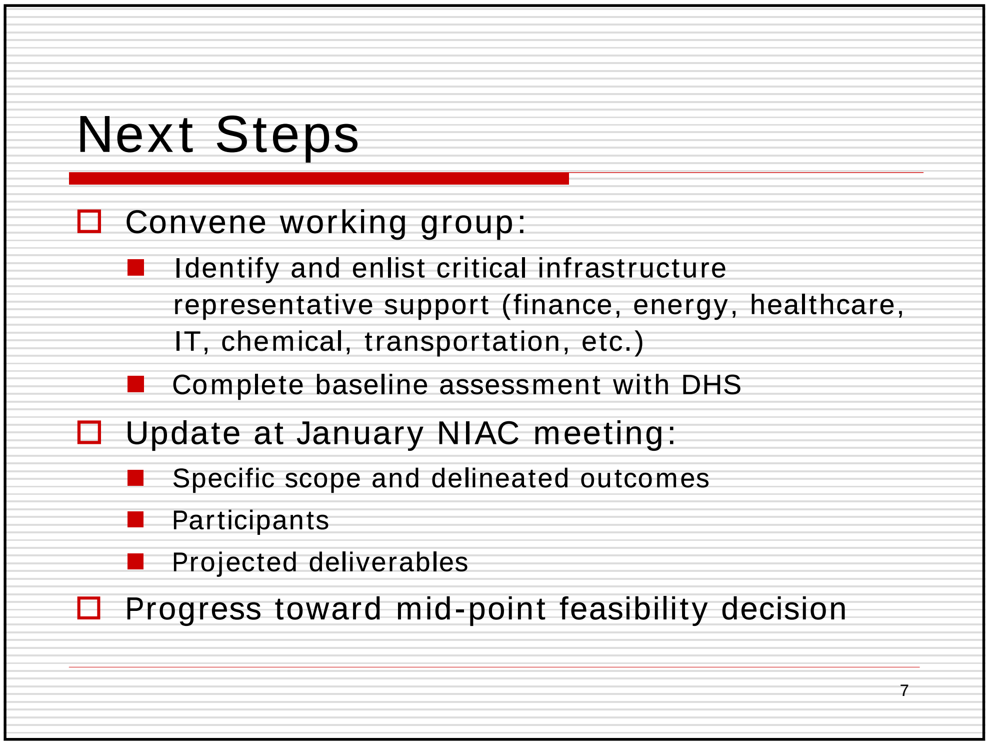
- □ Private sector practices based on
  - Likelihood of events (probability)
  - Potential consequences (impact)
  - Efficient allocation of risk management resources
- □ In some case, public sector plans are based on:
  - Very high-consequence events that may not be probable
  - Philosophy that protective measures must be applied across the board
- □ Concern exists that government may:
  - Consider worst-case events in establishing priorities
  - Plan without adequate consideration of likelihood and realistic threat capabilities
- □ Challenge to federal programs
  - Develop approaches to prioritize risk management actions
  - Cover critical infrastructure sectors; cover federal agencies
  - Manage risk data: threat capabilities, likelihood, and consequences

Working Group Focus

- □ Work group will:
  - Assess existing government risk management methodologies, practices, philosophies, and decision models
  - Identify differences/commonalities between public and private sector goals
  - Compare state of government risk management efforts against private sector risk management efforts
  - Identify focus areas covered by private sector uncovered or not fully matured in government methodologies or practices
  - Capture risk management trade-offs that differ between private and public sector models
  - Produce a deliverable of value

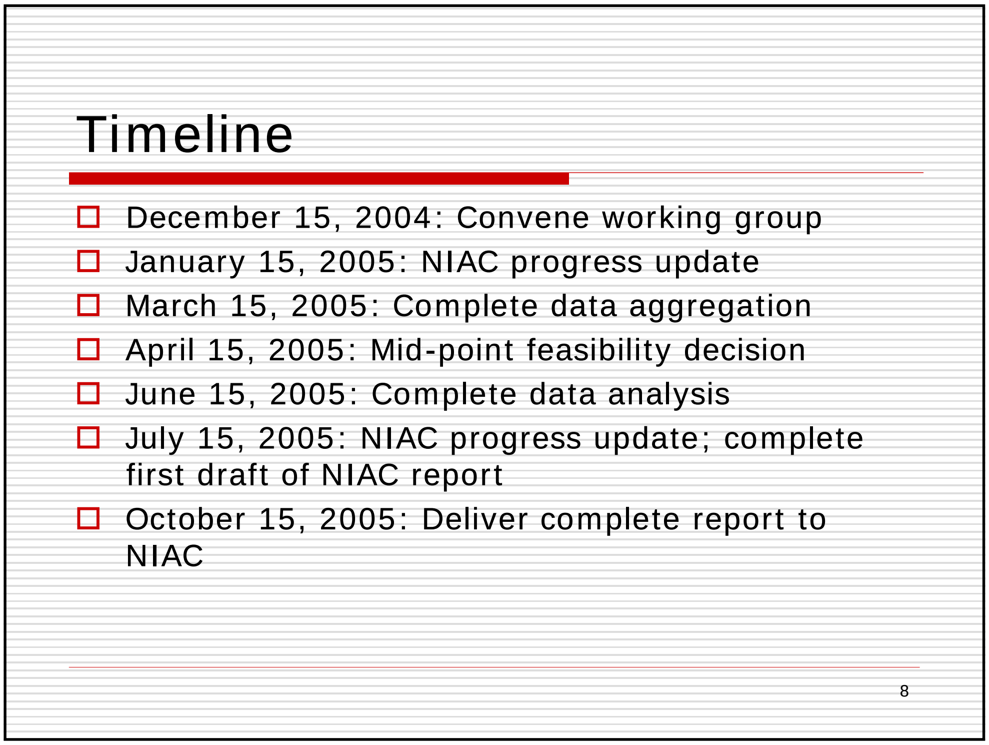
Outcomes

- □ Specific outcome dependent upon multiple variables
- □ Deliverables may include:
  - Recommendations to modify risk management focal points, methodology, or philosophy
  - Recommendations to adopt a risk management scoring system
  - Recommendations to tailor existing risk management practices to more efficiently allocate resources
- □ Mid-point decision to identify whether existing methodologies are sufficient; whether advancement of risk management body of knowledge feasible within context of Working Group scope



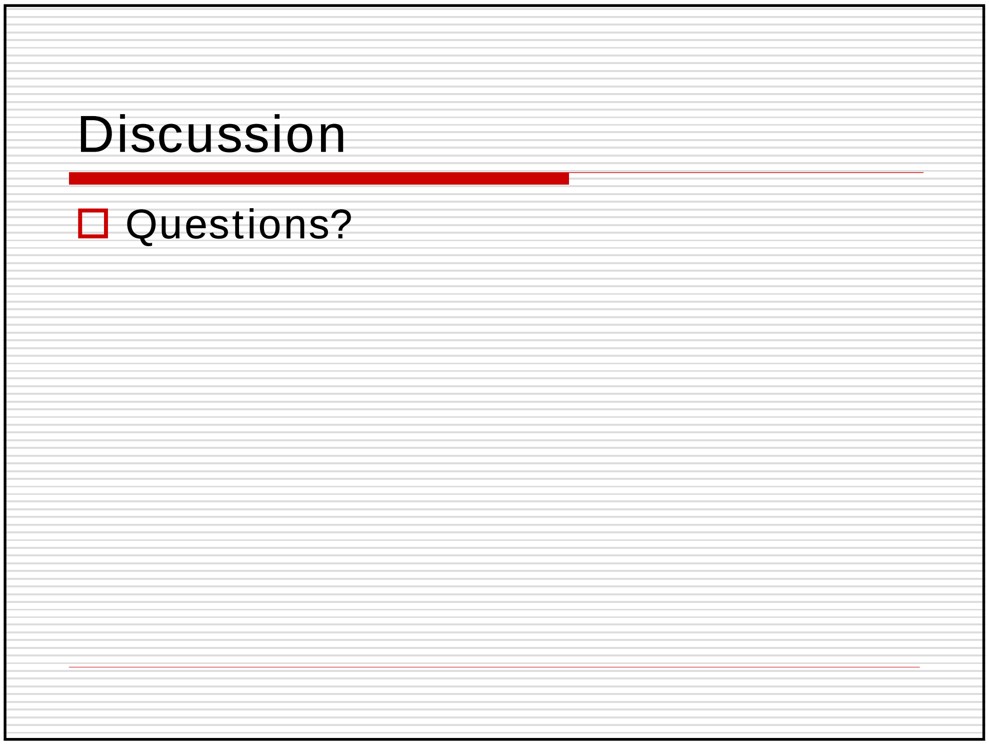
Next Steps

- □ Convene working group:
  - ■ Identify and enlist critical infrastructure representative support (finance, energy, healthcare, IT, chemical, transportation, etc.)
  - ■ Complete baseline assessment with DHS
- □ Update at January NIAC meeting:
  - ■ Specific scope and delineated outcomes
  - ■ Participants
  - ■ Projected deliverables
- □ Progress toward mid-point feasibility decision



Timeline

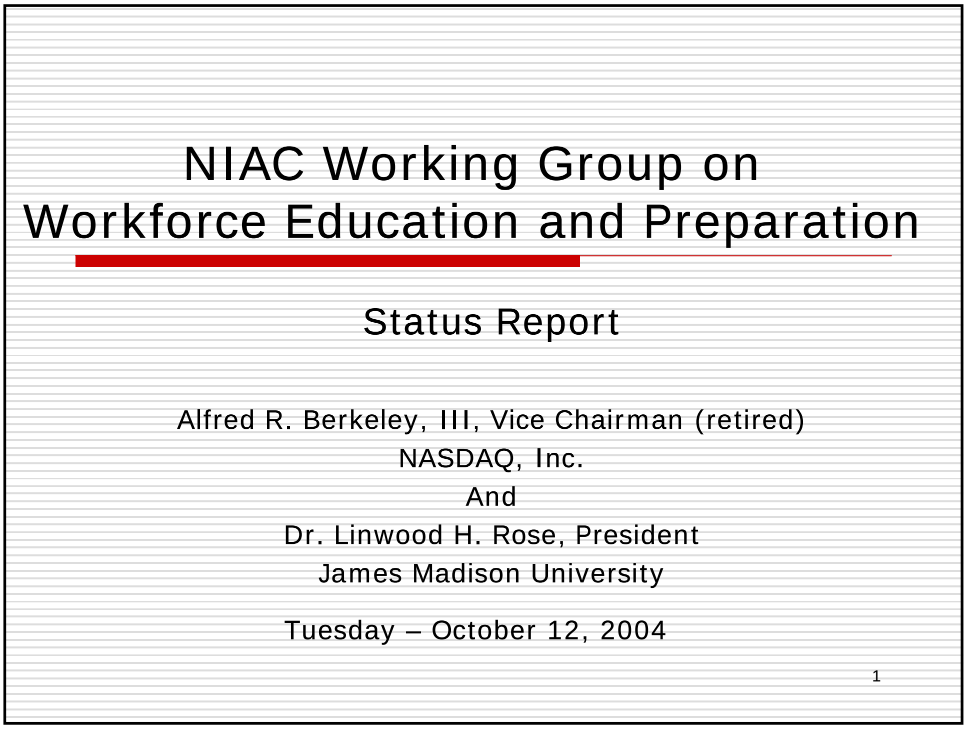
- □ December 15, 2004: Convene working group
- □ January 15, 2005: NIAC progress update
- □ March 15, 2005: Complete data aggregation
- □ April 15, 2005: Mid-point feasibility decision
- □ June 15, 2005: Complete data analysis
- □ July 15, 2005: NIAC progress update; complete first draft of NIAC report
- □ October 15, 2005: Deliver complete report to NIAC



Discussion

- □ Questions?

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

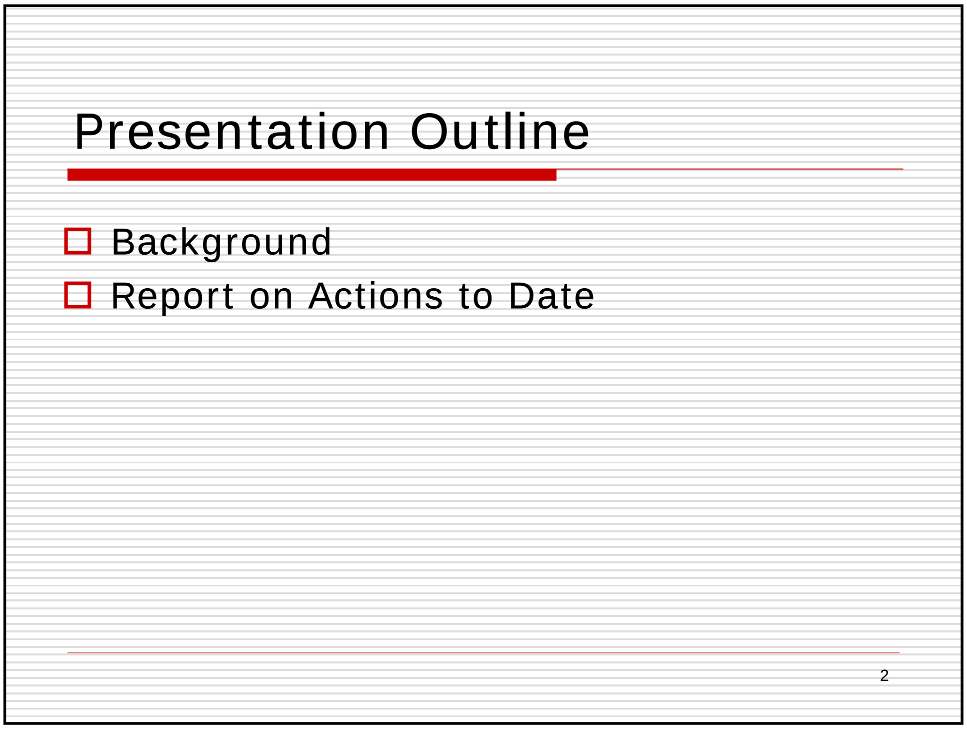


NIAC Working Group on Workforce Education and Preparation

Status Report

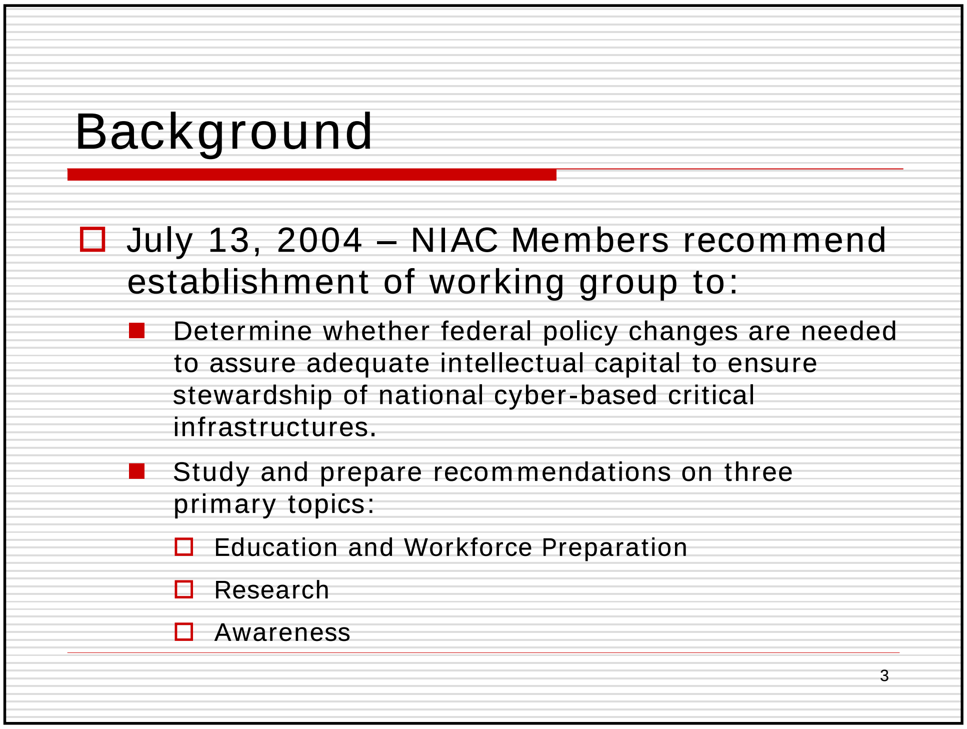
Alfred R. Berkeley, III, Vice Chairman (retired)
NASDAQ, Inc.
And
Dr. Linwood H. Rose, President
James Madison University

Tuesday – October 12, 2004



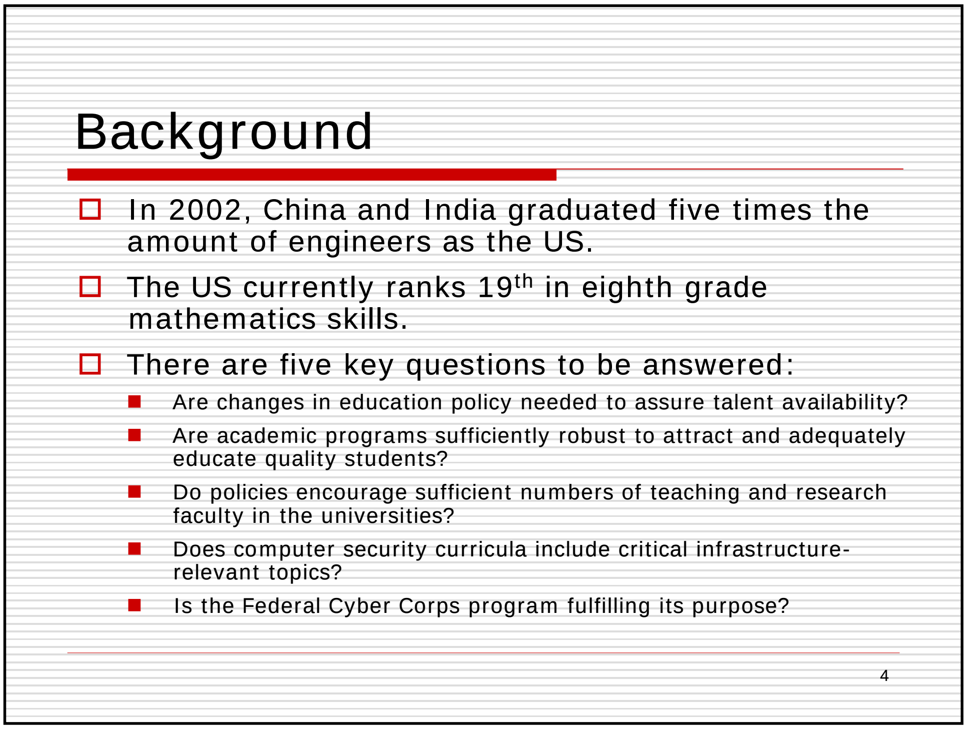
Presentation Outline

- □ Background
- □ Report on Actions to Date



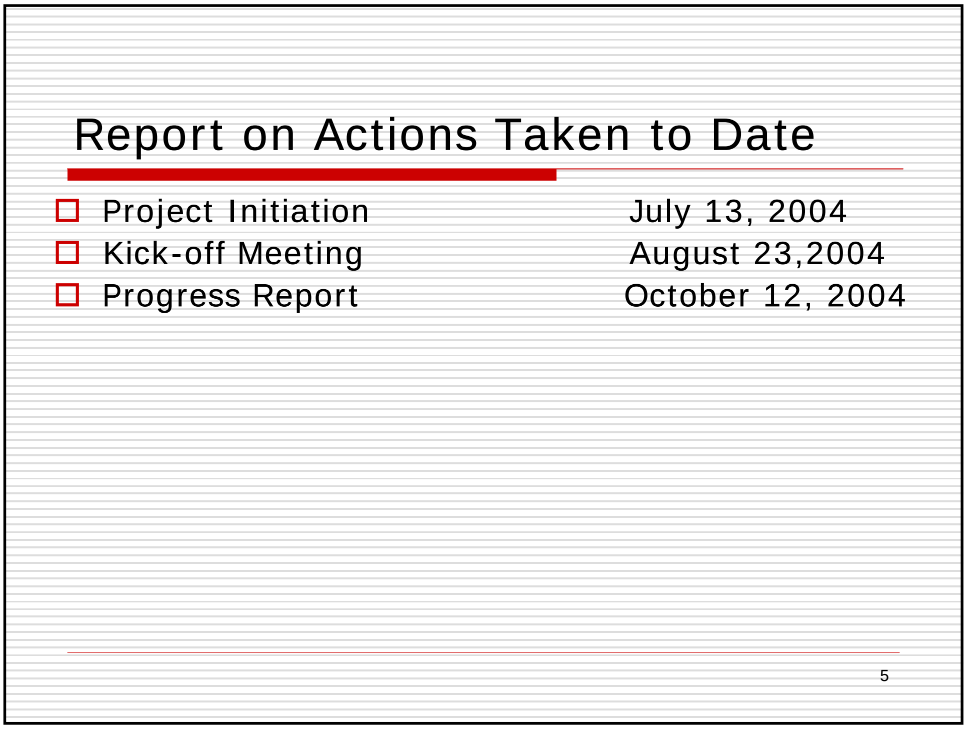
Background

- July 13, 2004 – NIAC Members recommend establishment of working group to:
  - Determine whether federal policy changes are needed to assure adequate intellectual capital to ensure stewardship of national cyber-based critical infrastructures.
  - Study and prepare recommendations on three primary topics:
    - Education and Workforce Preparation
    - Research
    - Awareness



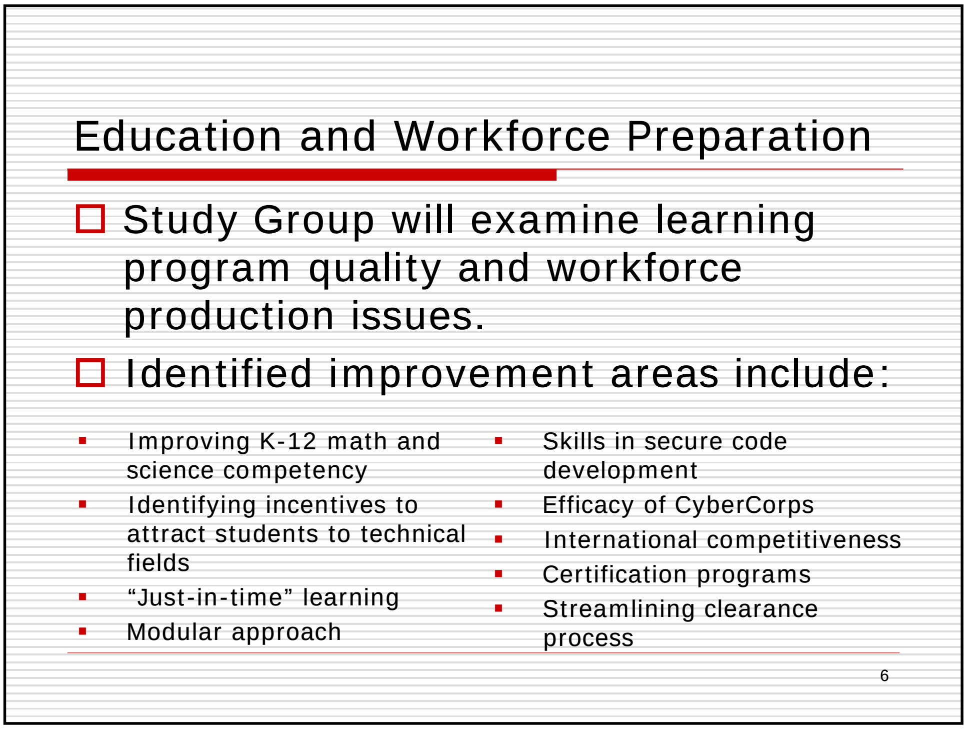
Background

- In 2002, China and India graduated five times the amount of engineers as the US.
- The US currently ranks 19th in eighth grade mathematics skills.
- There are five key questions to be answered:
  - Are changes in education policy needed to assure talent availability?
  - Are academic programs sufficiently robust to attract and adequately educate quality students?
  - Do policies encourage sufficient numbers of teaching and research faculty in the universities?
  - Does computer security curricula include critical infrastructure-relevant topics?
  - Is the Federal Cyber Corps program fulfilling its purpose?



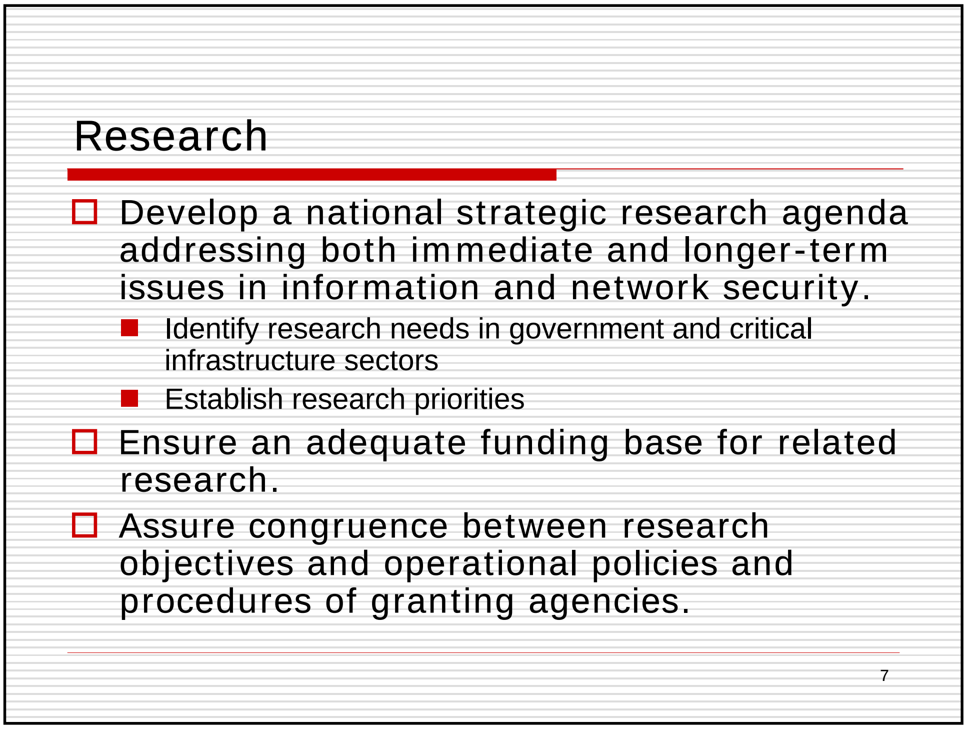
Report on Actions Taken to Date

□ Project Initiation	July 13, 2004
□ Kick-off Meeting	August 23,2004
□ Progress Report	October 12, 2004



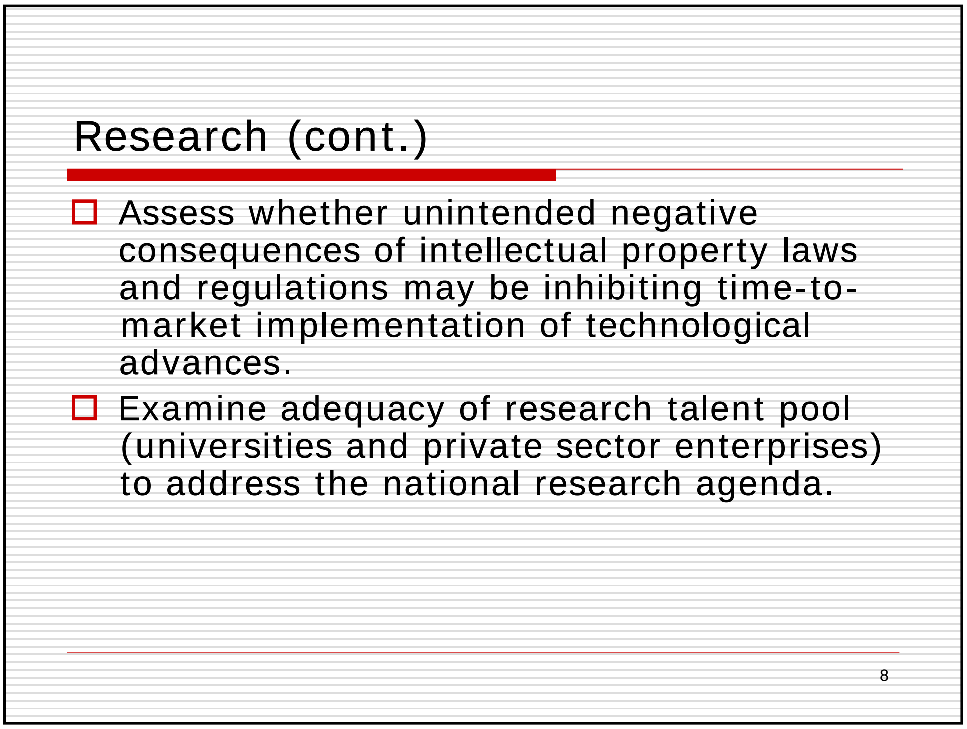
Education and Workforce Preparation

- □ Study Group will examine learning program quality and workforce production issues.
- □ Identified improvement areas include:
  - Improving K-12 math and science competency
  - Identifying incentives to attract students to technical fields
  - "Just-in-time" learning
  - Modular approach
  - Skills in secure code development
  - Efficacy of CyberCorps
  - International competitiveness
  - Certification programs
  - Streamlining clearance process



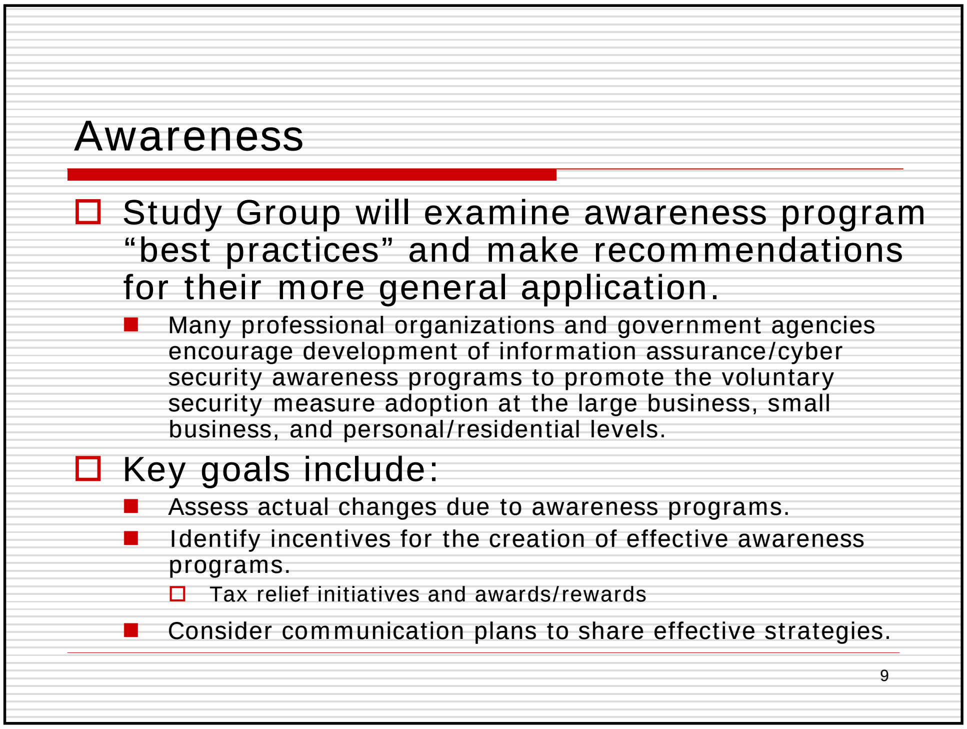
Research

- □ Develop a national strategic research agenda addressing both immediate and longer-term issues in information and network security.
  - Identify research needs in government and critical infrastructure sectors
  - Establish research priorities
- □ Ensure an adequate funding base for related research.
- □ Assure congruence between research objectives and operational policies and procedures of granting agencies.



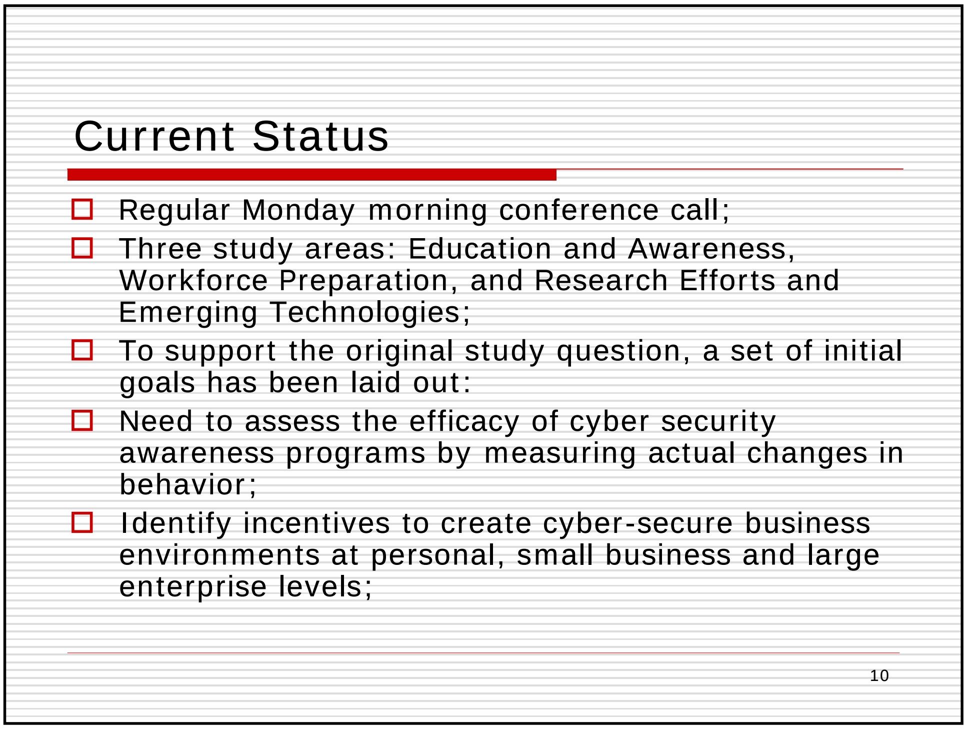
Research (cont.)

- □ Assess whether unintended negative consequences of intellectual property laws and regulations may be inhibiting time-to-market implementation of technological advances.
- □ Examine adequacy of research talent pool (universities and private sector enterprises) to address the national research agenda.



Awareness

- Study Group will examine awareness program “best practices” and make recommendations for their more general application.
  - Many professional organizations and government agencies encourage development of information assurance/cyber security awareness programs to promote the voluntary security measure adoption at the large business, small business, and personal/residential levels.
- Key goals include:
  - Assess actual changes due to awareness programs.
  - Identify incentives for the creation of effective awareness programs.
    - Tax relief initiatives and awards/rewards
  - Consider communication plans to share effective strategies.



Current Status

- Regular Monday morning conference call;
- Three study areas: Education and Awareness, Workforce Preparation, and Research Efforts and Emerging Technologies;
- To support the original study question, a set of initial goals has been laid out:
- Need to assess the efficacy of cyber security awareness programs by measuring actual changes in behavior;
- Identify incentives to create cyber-secure business environments at personal, small business and large enterprise levels;

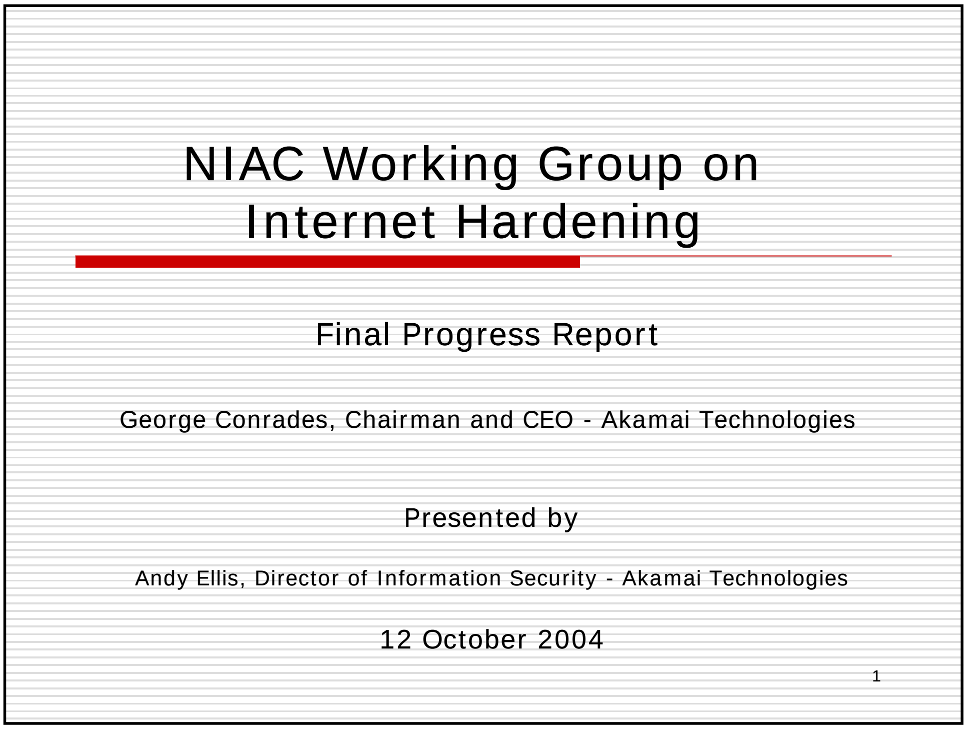
Current Status (cont.)

- □ Identify incentives to recruit professionals into cyber security in business, government and education;
- □ Create a process for college and university students to begin the security clearance process at the beginning of the senior year to avoid delays in hiring upon graduation;
- □ Identify research interests of sector leaders of research products, i.e. patents that are not transferred to the marketplace;

Current Status (cont.)

- □ Curriculum building: encourage a modular approach to curriculum building as well as pre-testing to identify learning needs of individuals prior to enrollment;
- □ Group predicts study duration could be three quarters;
- □ Group will rely on DHS support to provide information on existing initiatives in this area;
- □ Next step is to provide a report scope to NIAC Members for review and approval at the October 12 NIAC meeting.

ATTACHMENT D:
Final Report on Hardening the Internet



NIAC Working Group on Internet Hardening

Final Progress Report

George Conrades, Chairman and CEO - Akamai Technologies

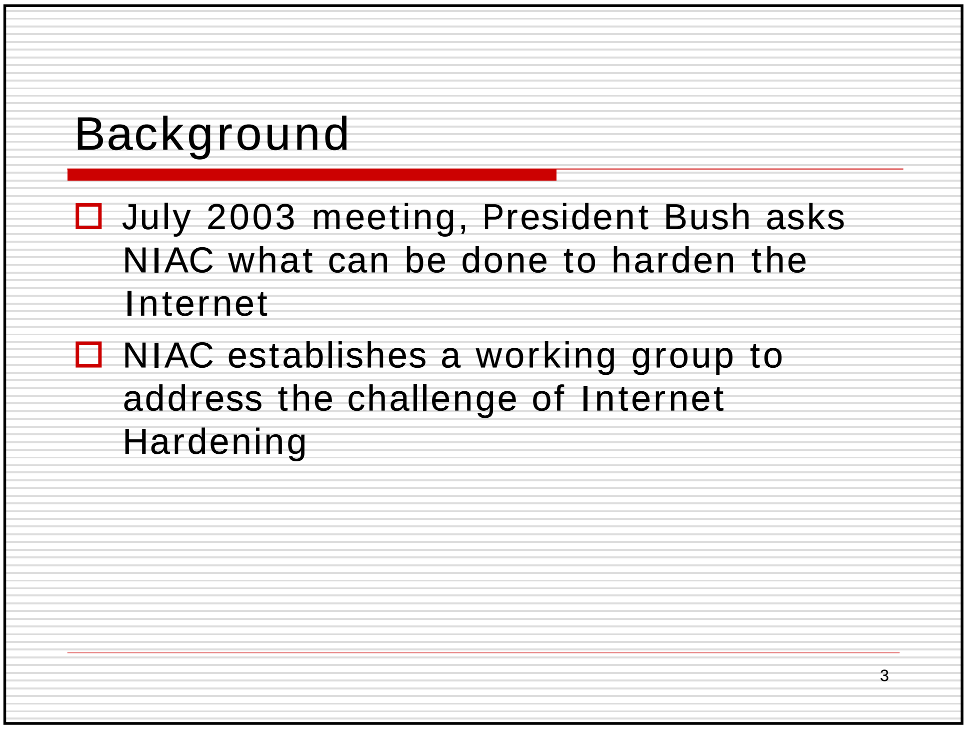
Presented by

Andy Ellis, Director of Information Security - Akamai Technologies

12 October 2004

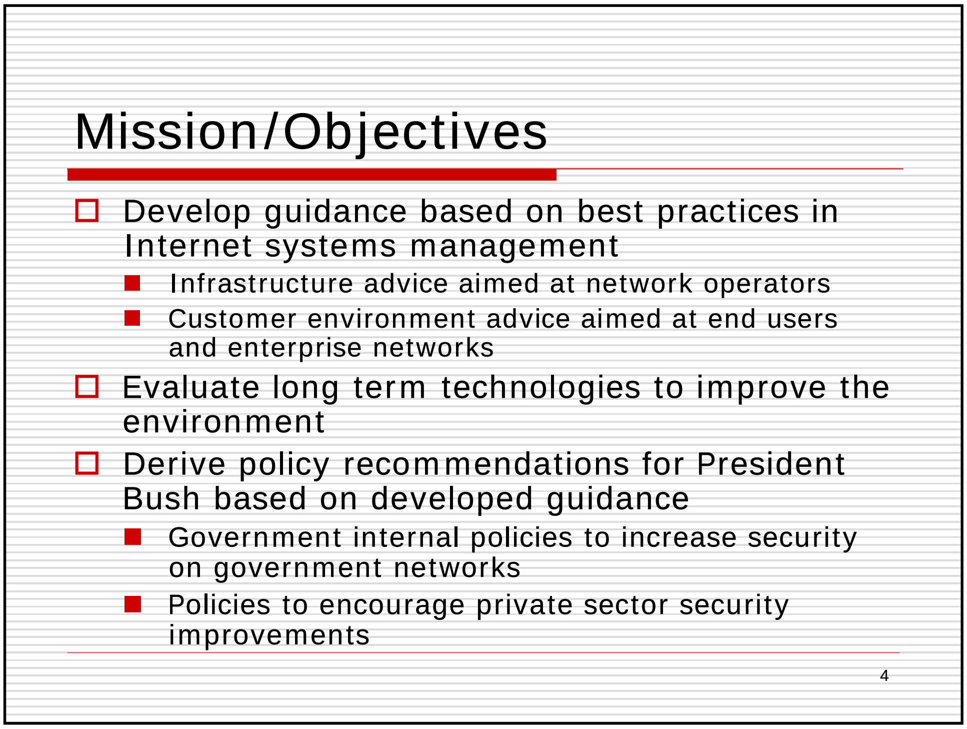
Agenda

- Background
- Methodology
- Challenges
- Recommendation Areas
- Recommendations



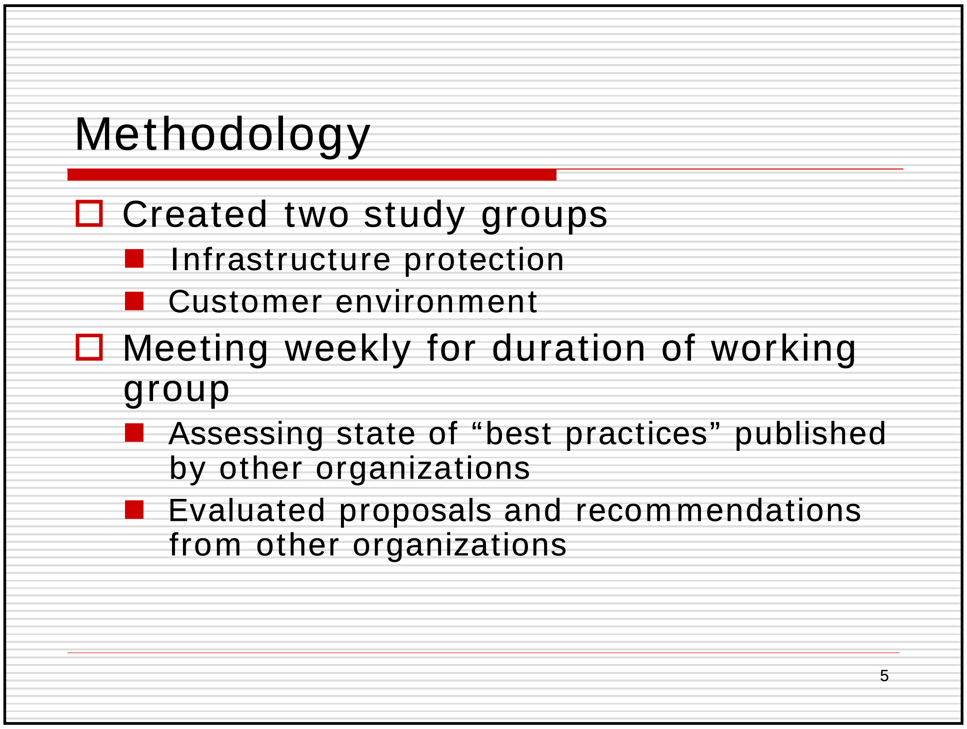
Background

- □ July 2003 meeting, President Bush asks NIAC what can be done to harden the Internet
- □ NIAC establishes a working group to address the challenge of Internet Hardening



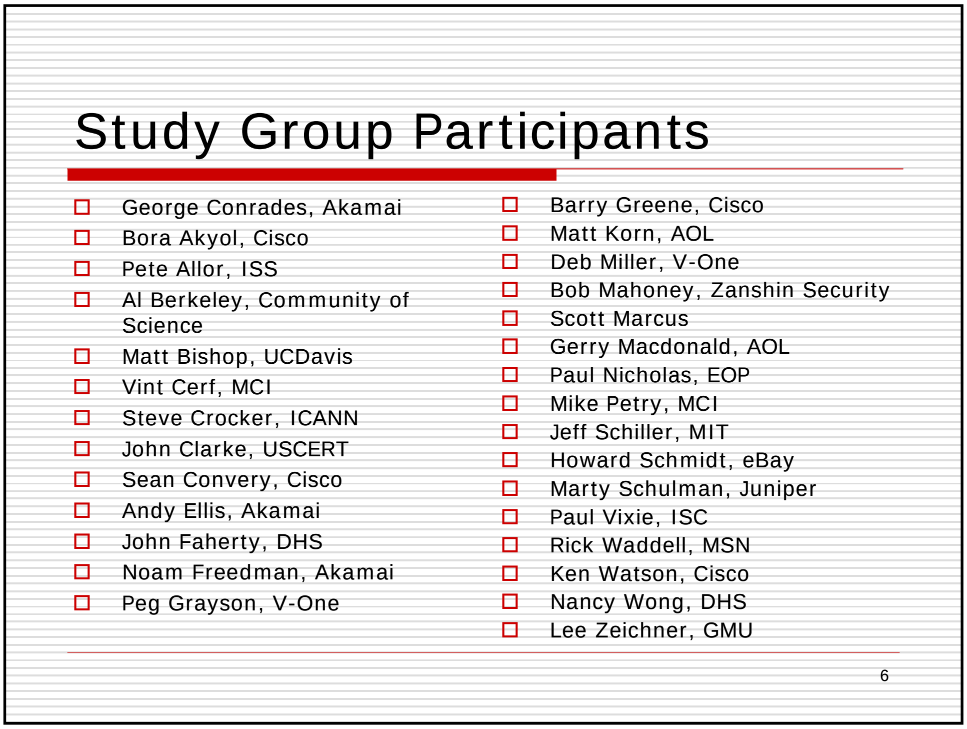
Mission/Objectives

- □ Develop guidance based on best practices in Internet systems management
  - ■ Infrastructure advice aimed at network operators
  - ■ Customer environment advice aimed at end users and enterprise networks
- □ Evaluate long term technologies to improve the environment
- □ Derive policy recommendations for President Bush based on developed guidance
  - ■ Government internal policies to increase security on government networks
  - ■ Policies to encourage private sector security improvements



Methodology

- □ Created two study groups
  - ■ Infrastructure protection
  - ■ Customer environment
- □ Meeting weekly for duration of working group
  - ■ Assessing state of “best practices” published by other organizations
  - ■ Evaluated proposals and recommendations from other organizations



Study Group Participants

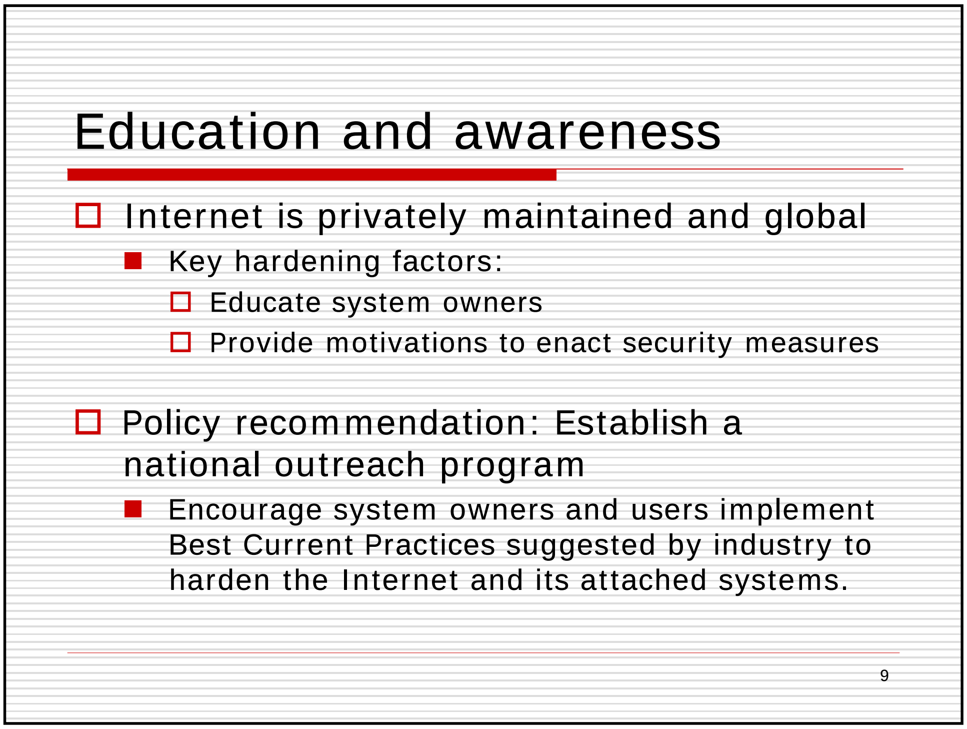
- □ George Conrades, Akamai
- □ Bora Akyol, Cisco
- □ Pete Allor, ISS
- □ Al Berkeley, Community of Science
- □ Matt Bishop, UCDavis
- □ Vint Cerf, MCI
- □ Steve Crocker, ICANN
- □ John Clarke, USCERT
- □ Sean Convery, Cisco
- □ Andy Ellis, Akamai
- □ John Faherty, DHS
- □ Noam Freedman, Akamai
- □ Peg Grayson, V-One
- □ Barry Greene, Cisco
- □ Matt Korn, AOL
- □ Deb Miller, V-One
- □ Bob Mahoney, Zanshin Security
- □ Scott Marcus
- □ Gerry Macdonald, AOL
- □ Paul Nicholas, EOP
- □ Mike Petry, MCI
- □ Jeff Schiller, MIT
- □ Howard Schmidt, eBay
- □ Marty Schulman, Juniper
- □ Paul Vixie, ISC
- □ Rick Waddell, MSN
- □ Ken Watson, Cisco
- □ Nancy Wong, DHS
- □ Lee Zeichner, GMU

Challenges

- Distributed Denial of Service
  - The availability of easily compromised computers on the Internet provides attackers with potent weapons against Internet-connected systems
- Infrastructure Protocol Security
  - Technologies not designed to prevent false control messages, but Best Current Practices sufficient for now
  - For the long term, moving to more secure protocols may be required

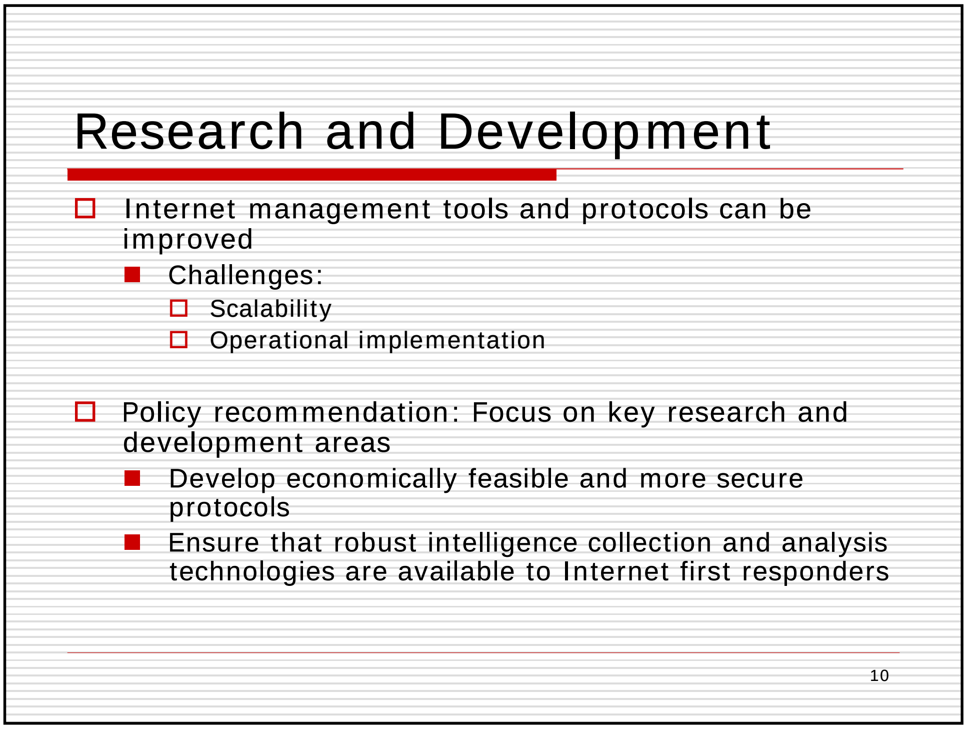
Recommendation Areas

- Education and awareness
  - End-user system security
  - Corporate security
- Research
  - New technologies
  - Investigation of secure protocol versions
- Empowerment
  - ISPs to act against aggressors
  - Law enforcement to focus on attackers



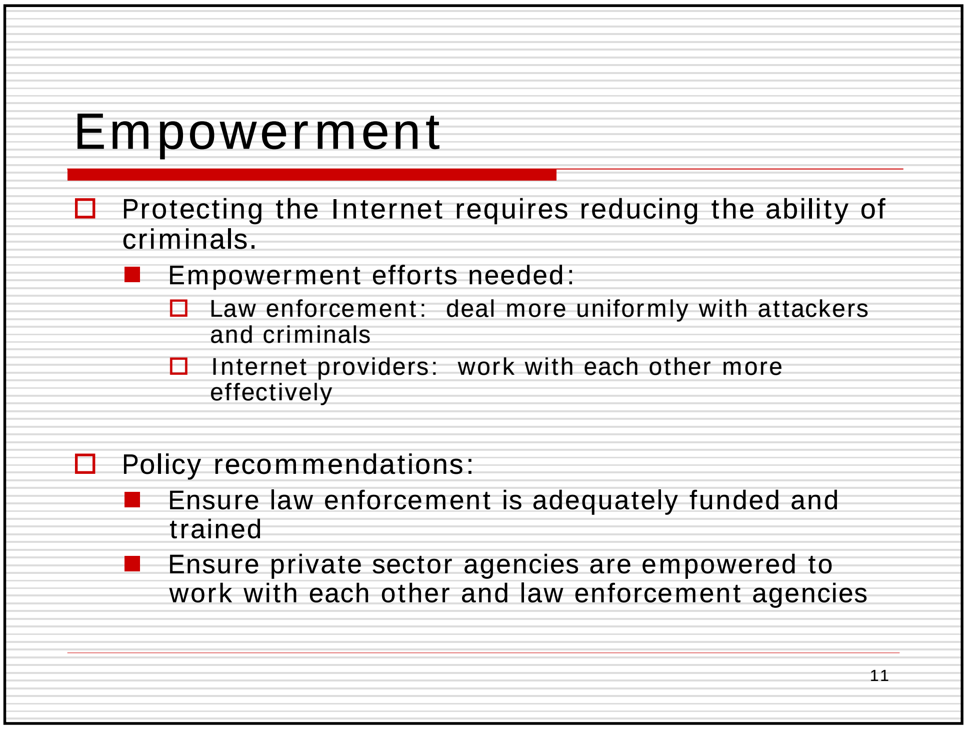
Education and awareness

- □ Internet is privately maintained and global
  - ■ Key hardening factors:
    - □ Educate system owners
    - □ Provide motivations to enact security measures
- □ Policy recommendation: Establish a national outreach program
  - ■ Encourage system owners and users implement Best Current Practices suggested by industry to harden the Internet and its attached systems.



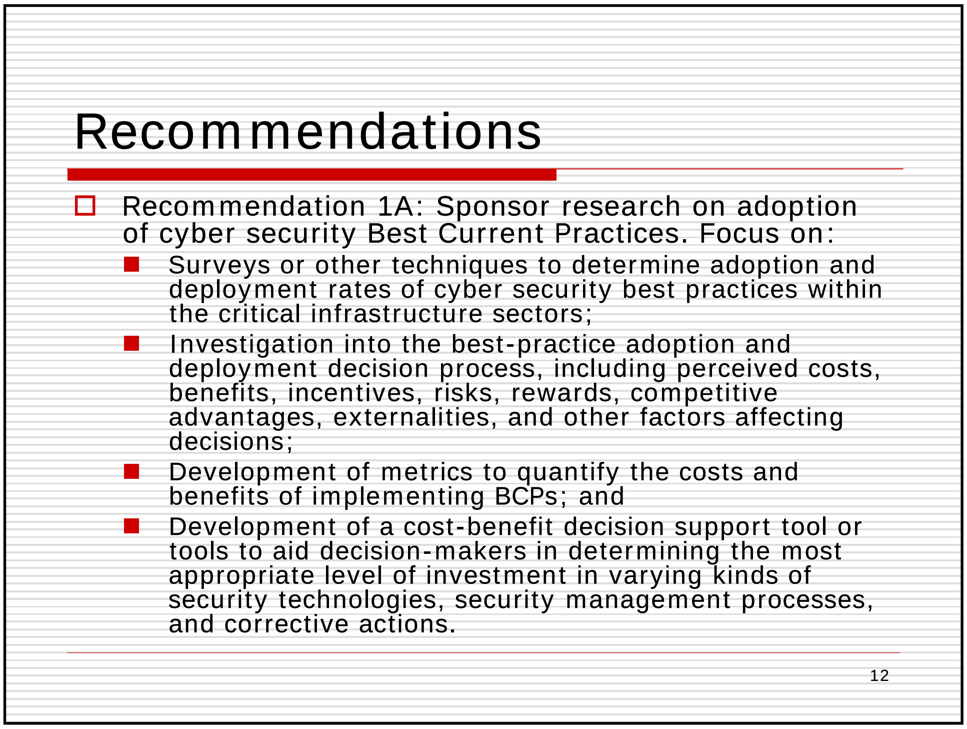
Research and Development

- □ Internet management tools and protocols can be improved
  - ■ Challenges:
    - □ Scalability
    - □ Operational implementation
- □ Policy recommendation: Focus on key research and development areas
  - ■ Develop economically feasible and more secure protocols
  - ■ Ensure that robust intelligence collection and analysis technologies are available to Internet first responders



Empowerment

- Protecting the Internet requires reducing the ability of criminals.
  - Empowerment efforts needed:
    - Law enforcement: deal more uniformly with attackers and criminals
    - Internet providers: work with each other more effectively
- Policy recommendations:
  - Ensure law enforcement is adequately funded and trained
  - Ensure private sector agencies are empowered to work with each other and law enforcement agencies

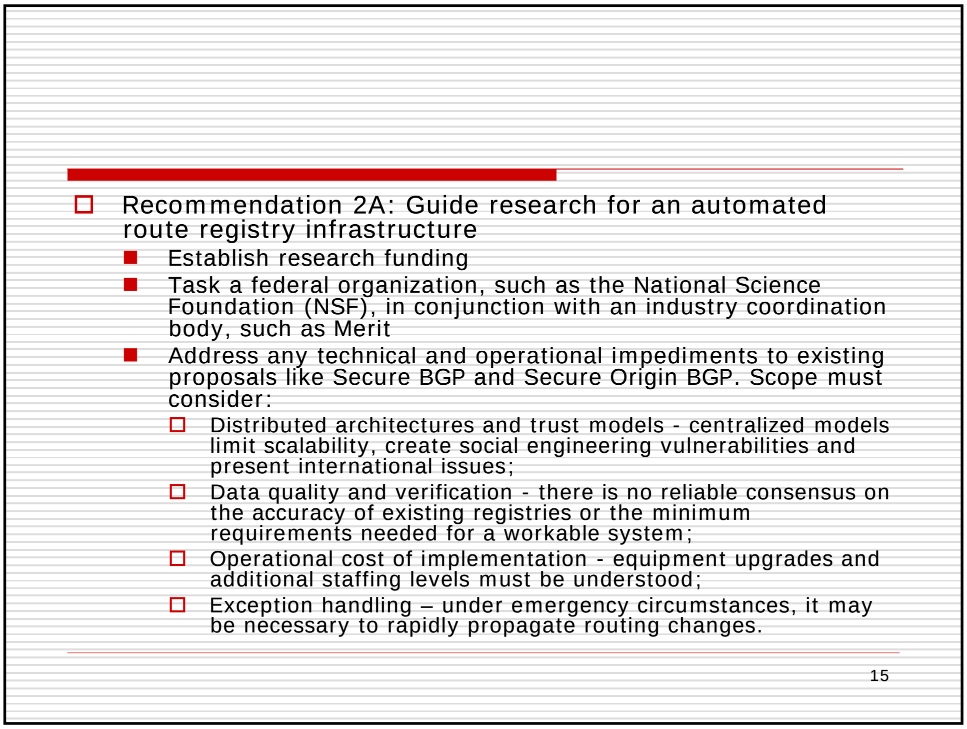


Recommendations

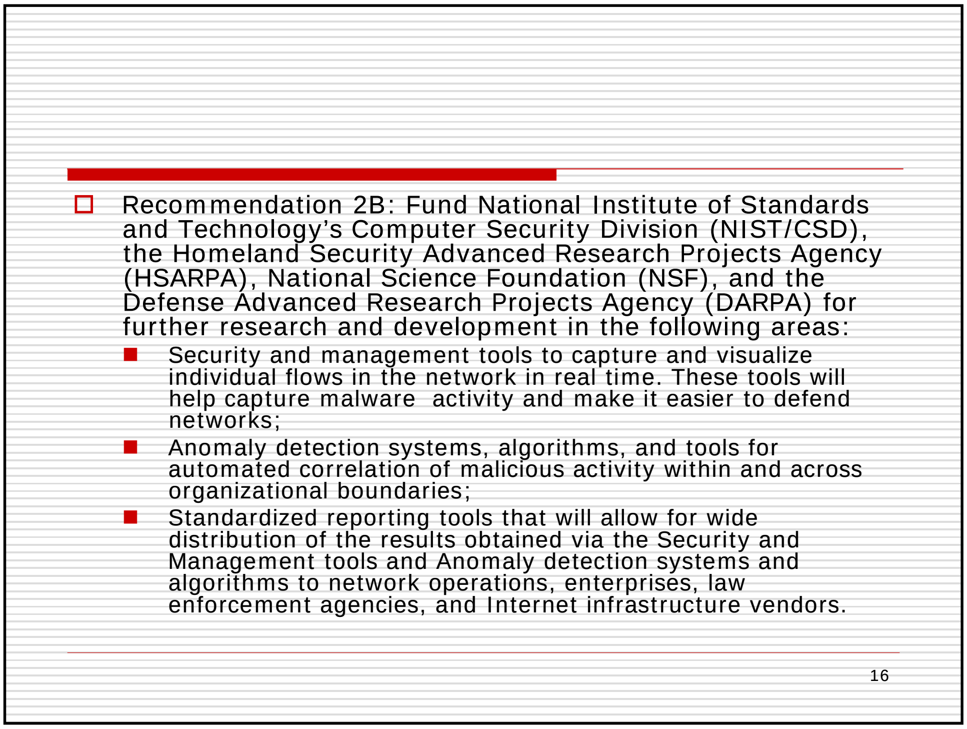
- Recommendation 1A: Sponsor research on adoption of cyber security Best Current Practices. Focus on:
  - Surveys or other techniques to determine adoption and deployment rates of cyber security best practices within the critical infrastructure sectors;
  - Investigation into the best-practice adoption and deployment decision process, including perceived costs, benefits, incentives, risks, rewards, competitive advantages, externalities, and other factors affecting decisions;
  - Development of metrics to quantify the costs and benefits of implementing BCPs; and
  - Development of a cost-benefit decision support tool or tools to aid decision-makers in determining the most appropriate level of investment in varying kinds of security technologies, security management processes, and corrective actions.

- Recommendation 1B: Recommend route and packet filtering as an important security best practice.
  - Refer to the Internet best practice, Request For Comment (RFC) 2267, adopted by the Internet Engineering Task Force (IETF)
- Recommendation 1C: Initiate partnership programs to increase American public awareness of computer security best practices.
  - Include close coordination with industry consortia
  - DHS hire a professional marketing firm to conduct a targeted campaign to help ensure security, promote awareness, and use nationally-sponsored commercials or events.
- Recommendation 1D: Publish guidelines and documentation on Secure Software Development Lifecycles.
  - Include representatives from leading software vendors and academics who teach software development
  - Sponsor a research project to develop metrics to determine the effectiveness of the adoption of the Secure Software Development Lifecycle
    - Should be conducted by a combination of a professional research firm, an academic institution, and the National Institute of Standards and Technology (NIST).

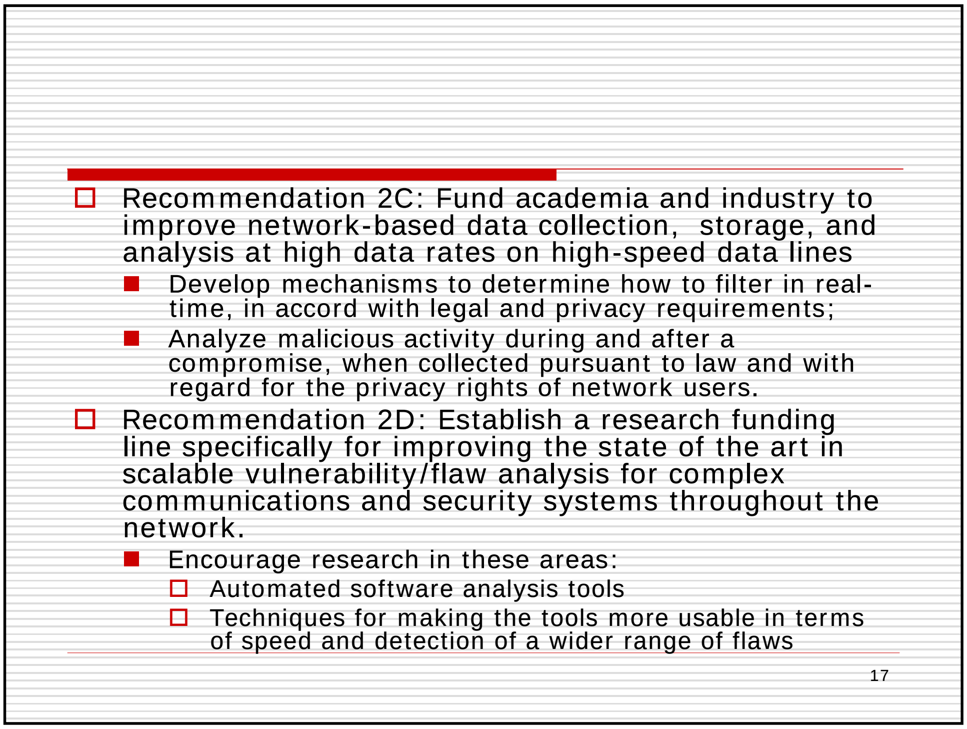
- Recommendation 1E: Provide and promote education to boards of companies and universities around IT security policy, oversight and governance.
  - Partner with groups like the Institute for Internal Auditors (IIA), Financial Executives International (FEI), and the National Association of Corporate Directors (NACD)
  - Provide information on voluntary standards available to organizations that wish to benchmark their security programs against industry best practices
  - Champion stronger cyber security policies and best practices
  - Promote cyber security policy and practice education through Federal agencies to contractors and government organizations that initiate procurements
  - Evaluate funding a “Mentor-Protégé” program where large government prime contractors adopt smaller companies to help educate and implement appropriate security policies and practices.



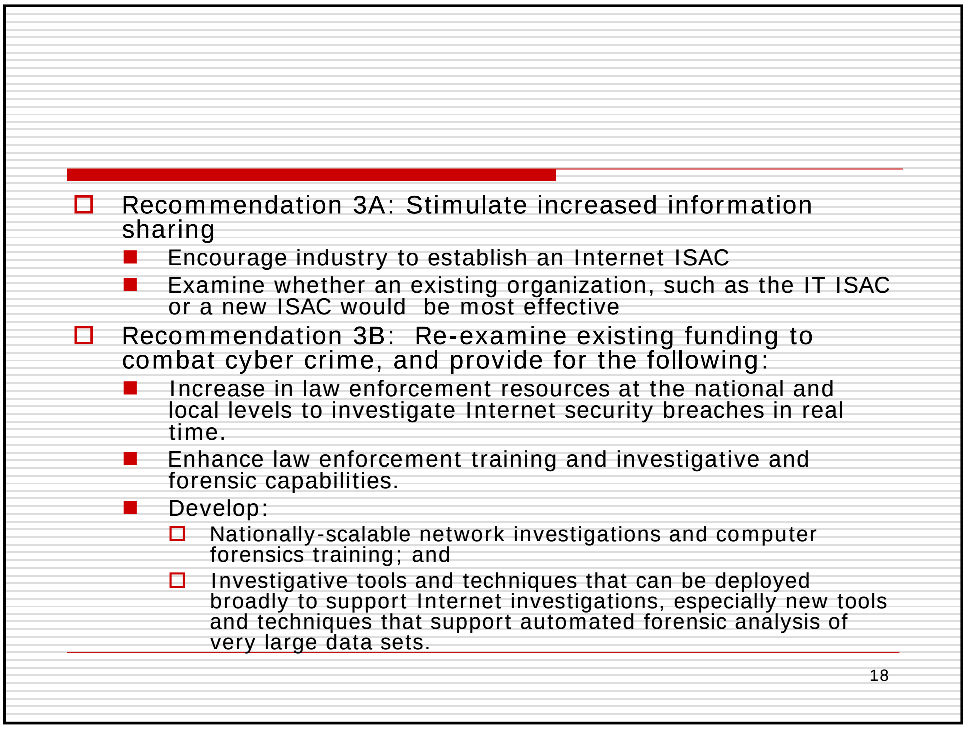
- Recommendation 2A: Guide research for an automated route registry infrastructure
  - Establish research funding
  - Task a federal organization, such as the National Science Foundation (NSF), in conjunction with an industry coordination body, such as Merit
  - Address any technical and operational impediments to existing proposals like Secure BGP and Secure Origin BGP. Scope must consider:
    - Distributed architectures and trust models - centralized models limit scalability, create social engineering vulnerabilities and present international issues;
    - Data quality and verification - there is no reliable consensus on the accuracy of existing registries or the minimum requirements needed for a workable system;
    - Operational cost of implementation - equipment upgrades and additional staffing levels must be understood;
    - Exception handling – under emergency circumstances, it may be necessary to rapidly propagate routing changes.



- Recommendation 2B: Fund National Institute of Standards and Technology's Computer Security Division (NIST/CSD), the Homeland Security Advanced Research Projects Agency (HSARPA), National Science Foundation (NSF), and the Defense Advanced Research Projects Agency (DARPA) for further research and development in the following areas:
  - Security and management tools to capture and visualize individual flows in the network in real time. These tools will help capture malware activity and make it easier to defend networks;
  - Anomaly detection systems, algorithms, and tools for automated correlation of malicious activity within and across organizational boundaries;
  - Standardized reporting tools that will allow for wide distribution of the results obtained via the Security and Management tools and Anomaly detection systems and algorithms to network operations, enterprises, law enforcement agencies, and Internet infrastructure vendors.



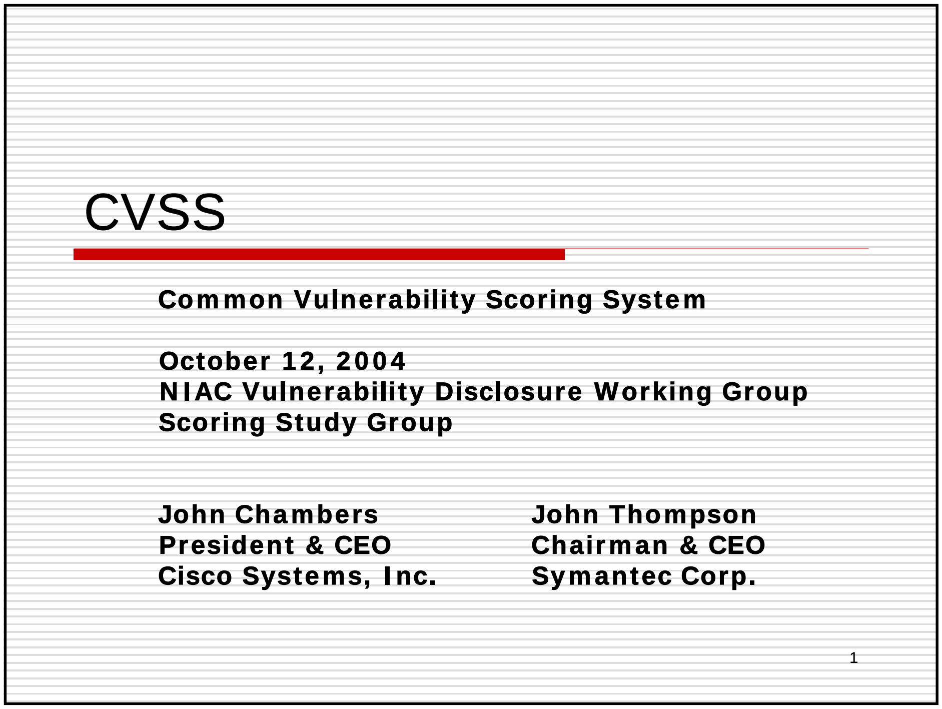
- Recommendation 2C: Fund academia and industry to improve network-based data collection, storage, and analysis at high data rates on high-speed data lines
  - Develop mechanisms to determine how to filter in real-time, in accord with legal and privacy requirements;
  - Analyze malicious activity during and after a compromise, when collected pursuant to law and with regard for the privacy rights of network users.
- Recommendation 2D: Establish a research funding line specifically for improving the state of the art in scalable vulnerability/flaw analysis for complex communications and security systems throughout the network.
  - Encourage research in these areas:
    - Automated software analysis tools
    - Techniques for making the tools more usable in terms of speed and detection of a wider range of flaws



- Recommendation 3A: Stimulate increased information sharing
  - Encourage industry to establish an Internet ISAC
  - Examine whether an existing organization, such as the IT ISAC or a new ISAC would be most effective
- Recommendation 3B: Re-examine existing funding to combat cyber crime, and provide for the following:
  - Increase in law enforcement resources at the national and local levels to investigate Internet security breaches in real time.
  - Enhance law enforcement training and investigative and forensic capabilities.
  - Develop:
    - Nationally-scalable network investigations and computer forensics training; and
    - Investigative tools and techniques that can be deployed broadly to support Internet investigations, especially new tools and techniques that support automated forensic analysis of very large data sets.

ATTACHMENT E:

Final Report on the Common Vulnerability Scoring System



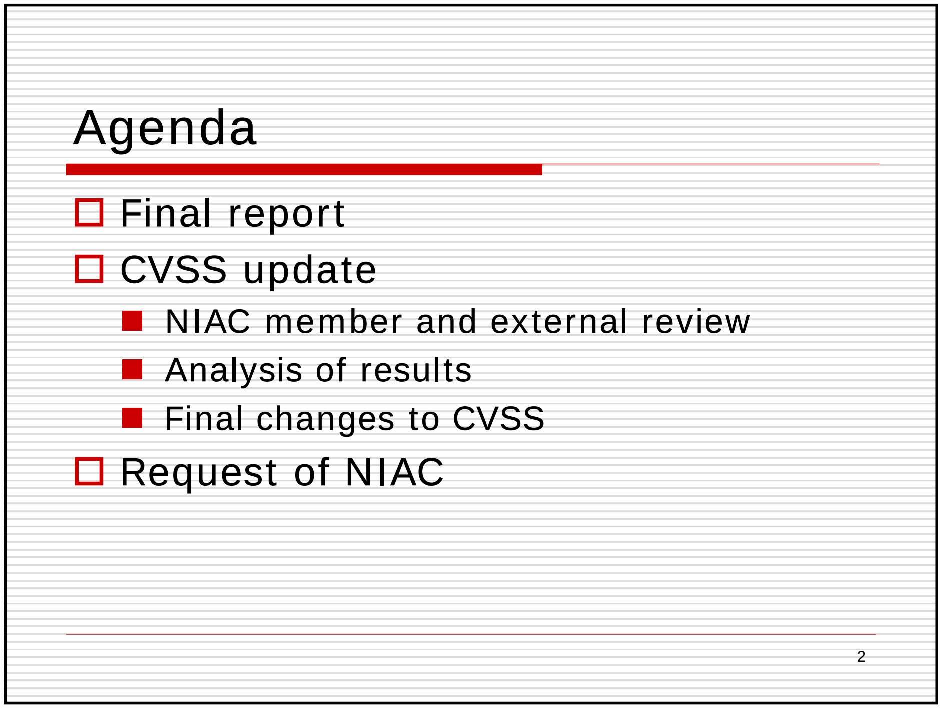
CVSS

Common Vulnerability Scoring System

October 12, 2004
NIAC Vulnerability Disclosure Working Group
Scoring Study Group

John Chambers
President & CEO
Cisco Systems, Inc.

John Thompson
Chairman & CEO
Symantec Corp.



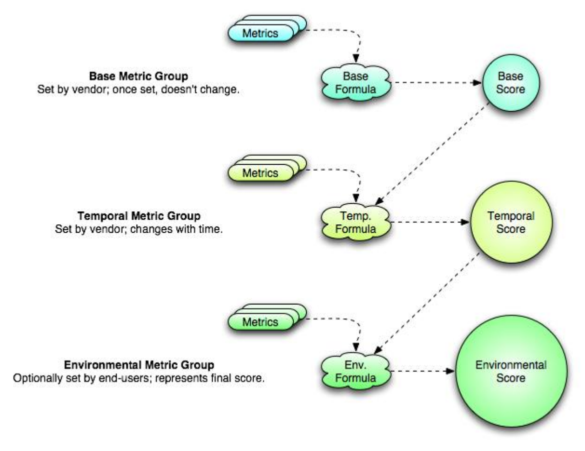
Agenda

- Final report
- CVSS update
  - NIAC member and external review
  - Analysis of results
  - Final changes to CVSS
- Request of NIAC

CVSS Final Draft Report

- Represents *initial* methodology
- Incorporates changes from NIAC member evaluation testing and external review
- CVSS development team will remain available for training & assistance
- CVSS needs home for future updates

The CVSS



Metrics

Base Formula

Base Score

Base Metric Group
Set by vendor; once set, doesn't change.

Metrics

Temp. Formula

Temporal Score

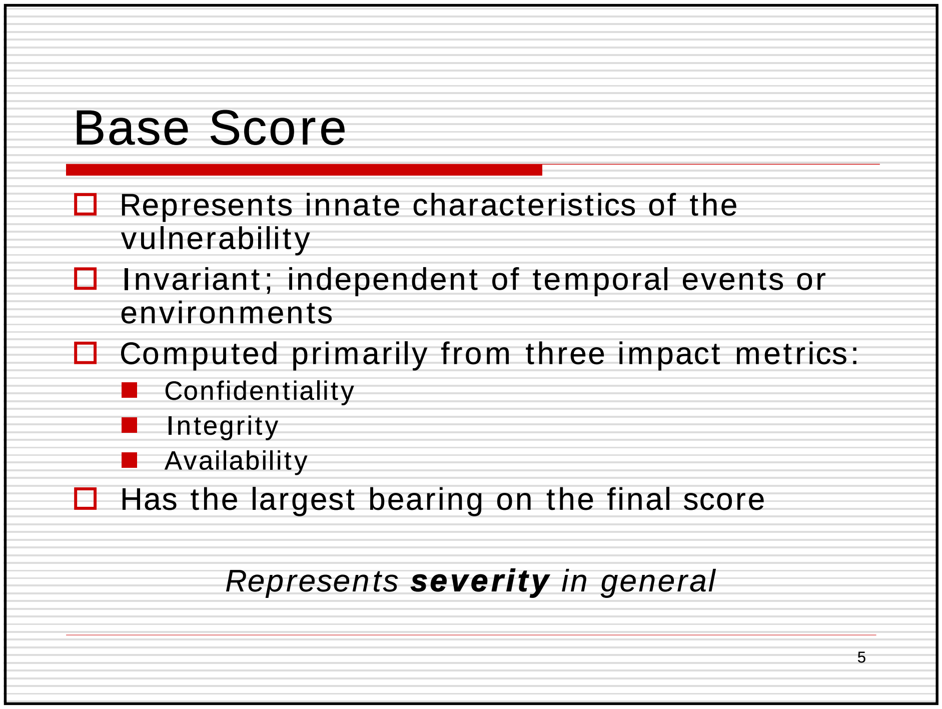
Temporal Metric Group
Set by vendor; changes with time.

Metrics

Env. Formula

Environmental Score

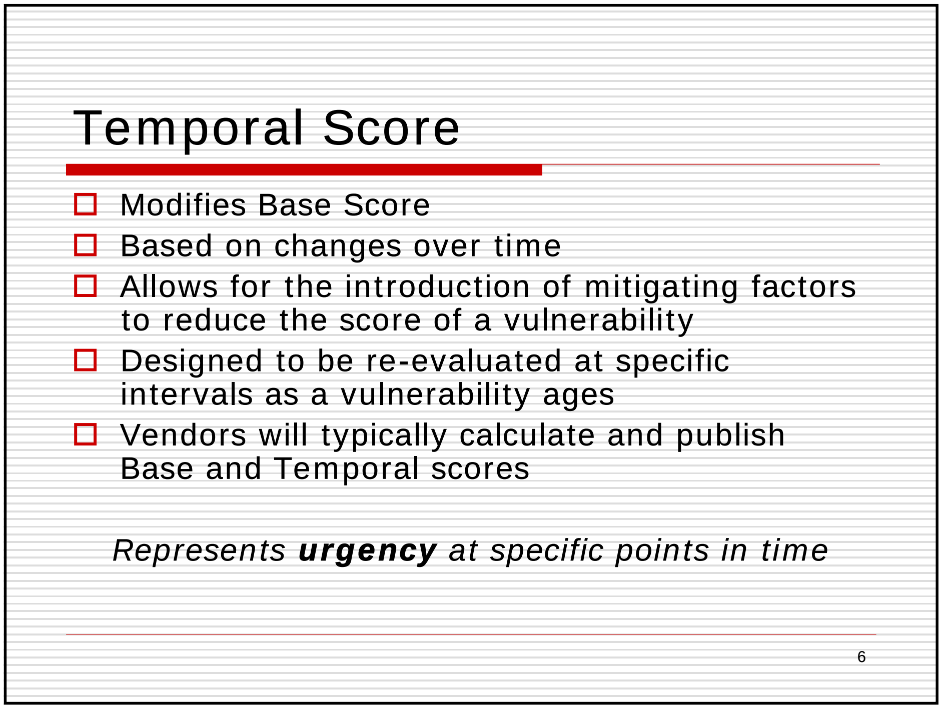
Environmental Metric Group
Optionally set by end-users; represents final score.



Base Score

- □ Represents innate characteristics of the vulnerability
- □ Invariant; independent of temporal events or environments
- □ Computed primarily from three impact metrics:
  - ■ Confidentiality
  - ■ Integrity
  - ■ Availability
- □ Has the largest bearing on the final score

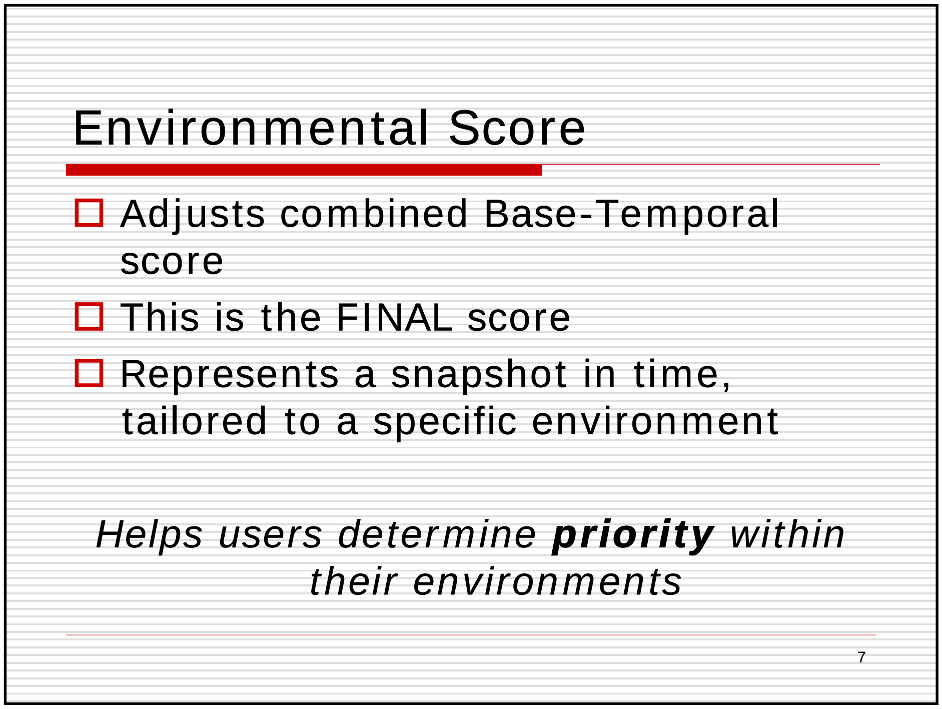
*Represents **severity** in general*



Temporal Score

- □ Modifies Base Score
- □ Based on changes over time
- □ Allows for the introduction of mitigating factors to reduce the score of a vulnerability
- □ Designed to be re-evaluated at specific intervals as a vulnerability ages
- □ Vendors will typically calculate and publish Base and Temporal scores

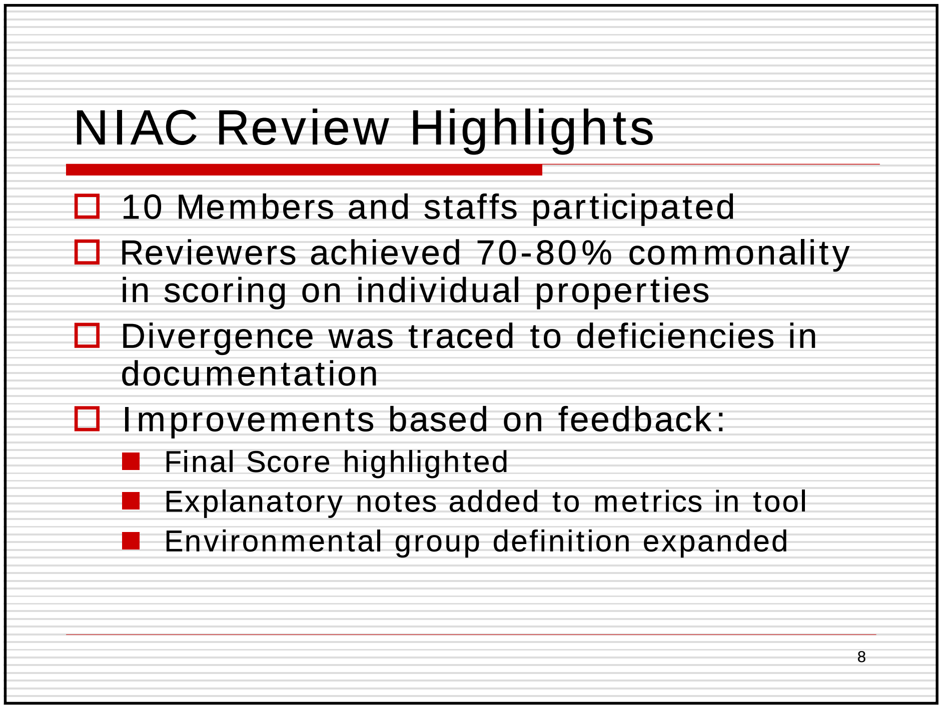
*Represents **urgency** at specific points in time*



Environmental Score

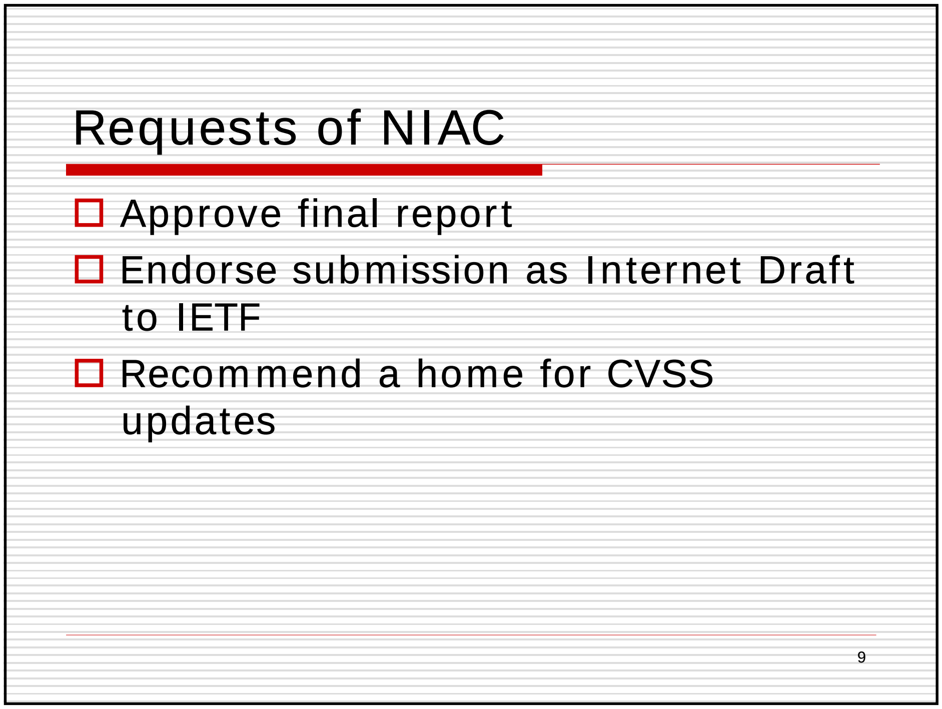
- □ Adjusts combined Base-Temporal score
- □ This is the FINAL score
- □ Represents a snapshot in time, tailored to a specific environment

*Helps users determine **priority** within their environments*



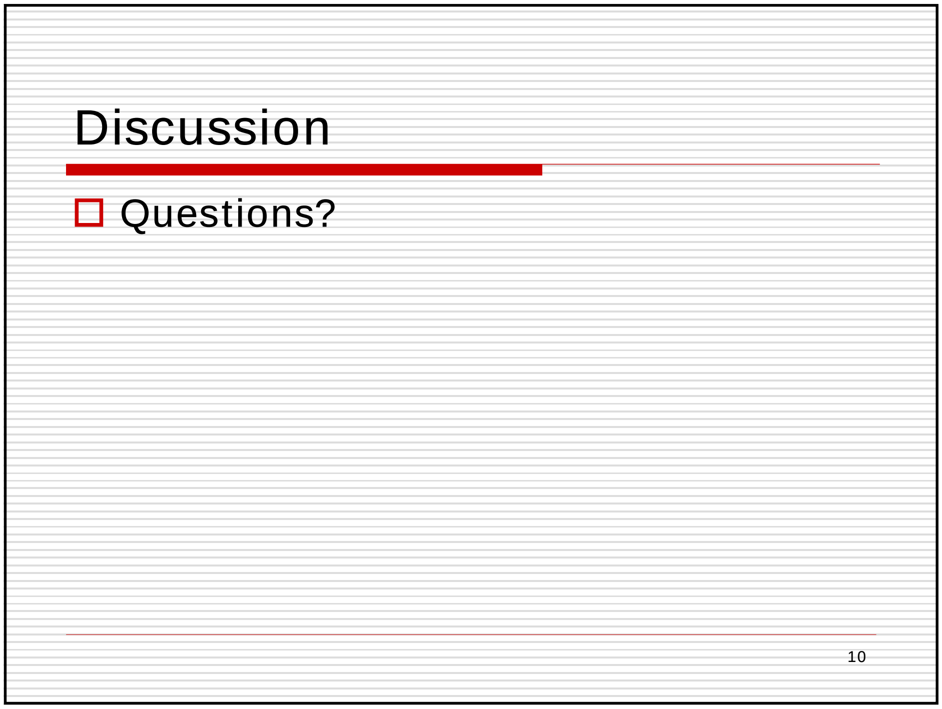
NIAC Review Highlights

- □ 10 Members and staffs participated
- □ Reviewers achieved 70-80% commonality in scoring on individual properties
- □ Divergence was traced to deficiencies in documentation
- □ Improvements based on feedback:
  - ■ Final Score highlighted
  - ■ Explanatory notes added to metrics in tool
  - ■ Environmental group definition expanded



Requests of NIAC

- □ Approve final report
- □ Endorse submission as Internet Draft to IETF
- □ Recommend a home for CVSS updates



Discussion

- □ Questions?

ATTACHMENT G:
Final Report and Discussion on the Prioritization of Cyber Vulnerabilities

NIAC Working Group on Prioritization of Cyber Vulnerabilities

Working Group Update

Martin G. McGuinn, Chairman & CEO
Mellon Financial Corporation

Tuesday – October 12, 2004

An example of a recent attack:

J.S.Scob Trojan Horse

- □ Internet Storm center receives reports of a new virus (June 20-04)
- □ ***J.S. Scob*** Trojan horse infected over 630 web servers
  - ■ Kelley Blue Book car pricing service
  - ■ Minerva Health (online financial services for the health care)
- □ Consumers using sites unknowingly had software downloaded to their own machines which recorded keystrokes
  - ■ Credit card numbers and passwords
  - ■ Information sent back to hackers
- □ Suspects are Russian virus group, the HangUP team
  - ■ FBI and Scotland Yard investigating
- □ Current anti-virus products would not detect malicious code.
- □ ISPs blocked customers access to the Russian web site launching attack

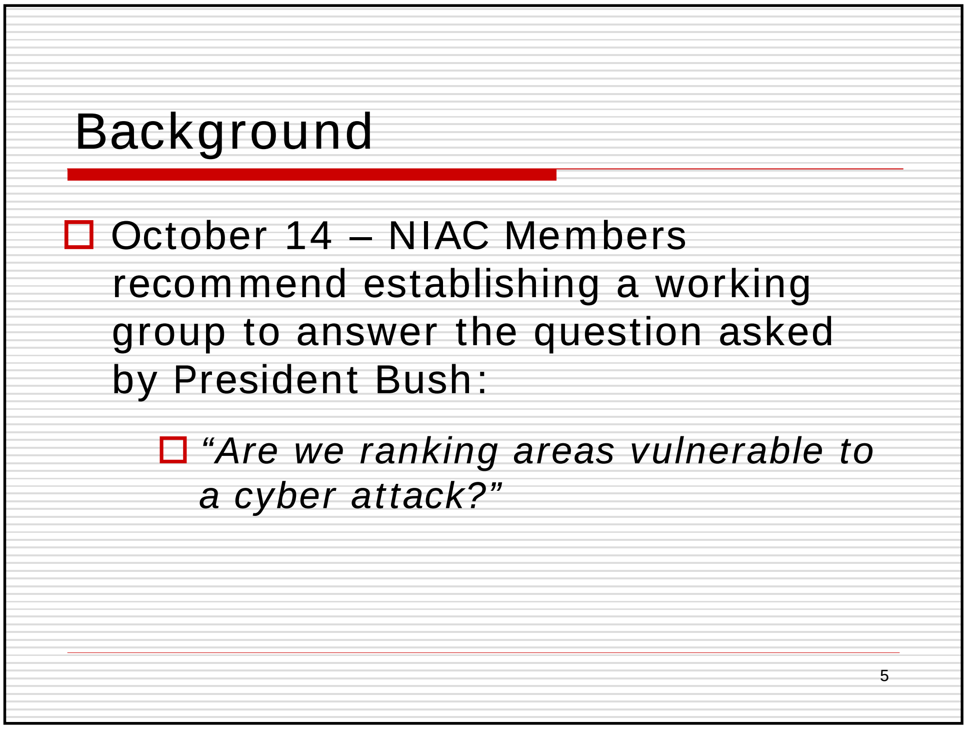
Source: Computer – September 2004

Study Group Participants

- Susan Vismor - Mellon Financial Corp., Study Group Chair
- Bruce Larsen – American Water
- Chris Terzich - Wells Fargo & Company
- Ken Watson - Cisco Systems, Inc.
- Teresa C. Lindsey - BITS
- Dan Bart - TIA
- David Thompson - TIA
- Lou Leffler - North American Electric Power
- Tim Zoph - Northwestern Memorial Hospital
- Scott Borg - Institute for Security Technology Studies, Dartmouth College
- Nancy Wong - DHS
- Leslie Burchett - DHS
- Gail Kaufmann - DHS
- Brett Lambo - DHS
- Tran Trang - DHS, National Cyber Security Division

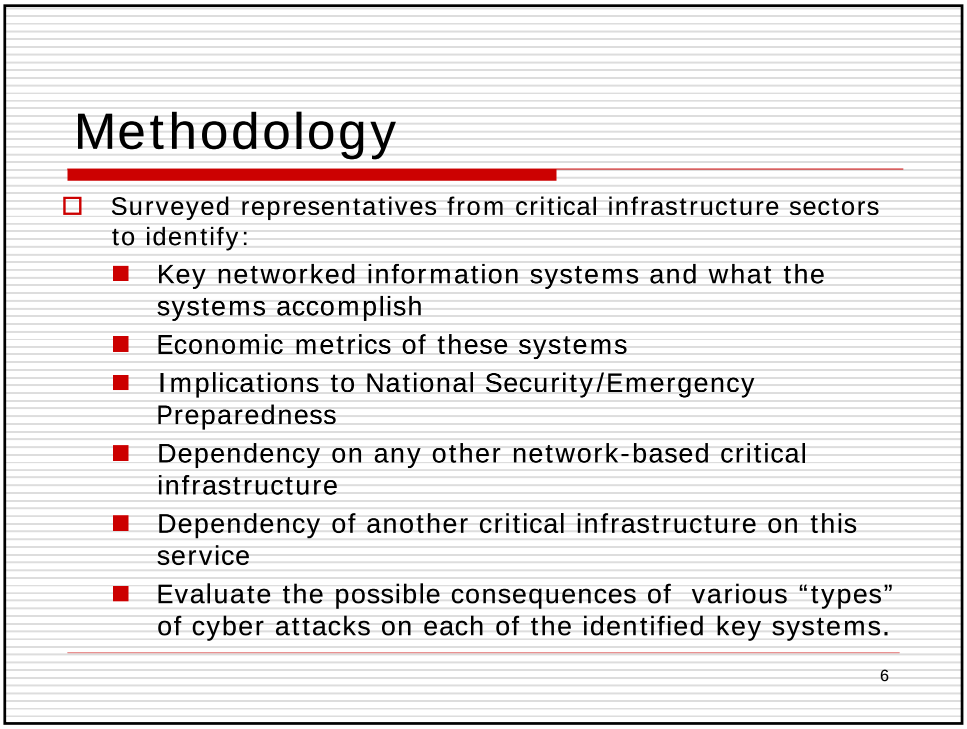
Presentation Outline

- □ Background
- □ Methodology
- □ Key Findings
- □ Proposed Recommendations



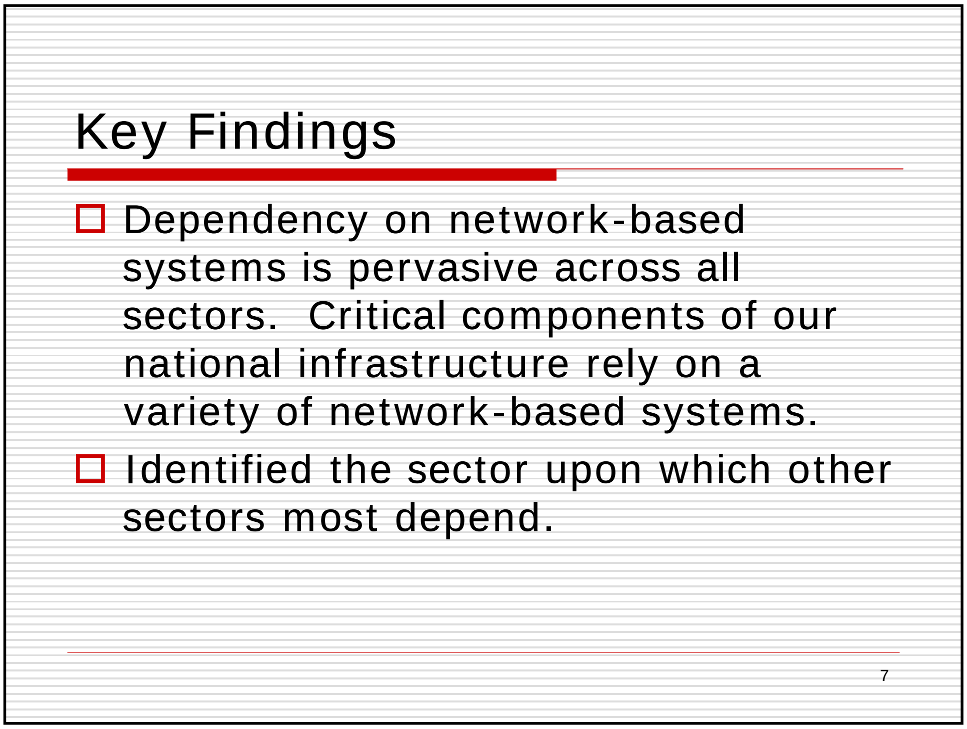
Background

- October 14 – NIAC Members recommend establishing a working group to answer the question asked by President Bush:
  - *“Are we ranking areas vulnerable to a cyber attack?”*



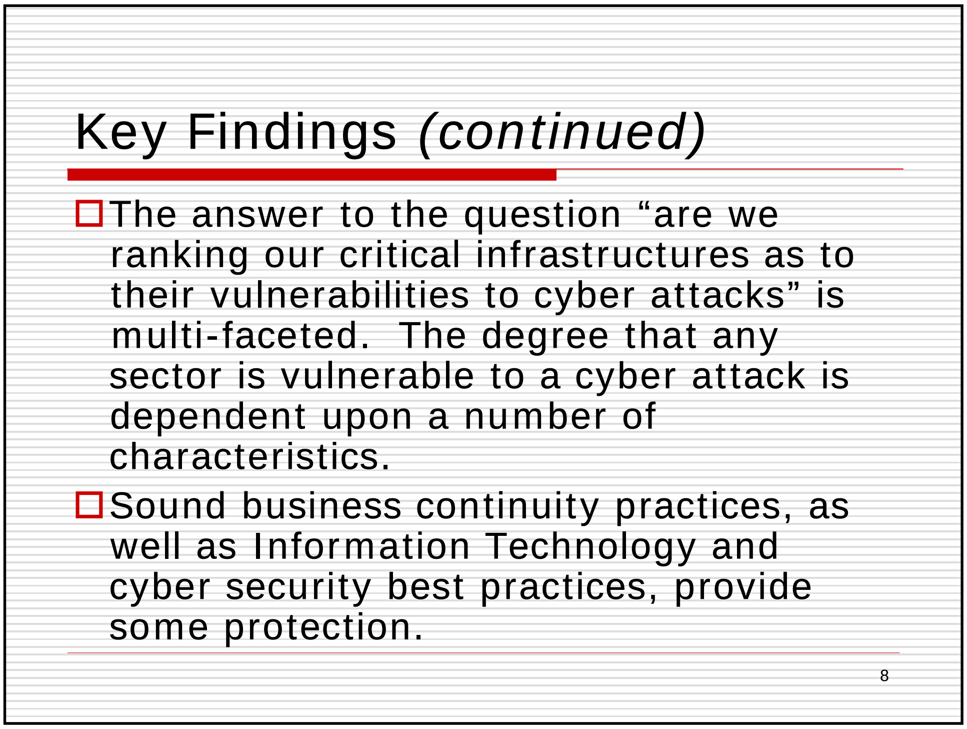
Methodology

- Surveyed representatives from critical infrastructure sectors to identify:
  - Key networked information systems and what the systems accomplish
  - Economic metrics of these systems
  - Implications to National Security/Emergency Preparedness
  - Dependency on any other network-based critical infrastructure
  - Dependency of another critical infrastructure on this service
  - Evaluate the possible consequences of various “types” of cyber attacks on each of the identified key systems.



Key Findings

- Dependency on network-based systems is pervasive across all sectors. Critical components of our national infrastructure rely on a variety of network-based systems.
- Identified the sector upon which other sectors most depend.



Key Findings *(continued)*

- The answer to the question “are we ranking our critical infrastructures as to their vulnerabilities to cyber attacks” is multi-faceted. The degree that any sector is vulnerable to a cyber attack is dependent upon a number of characteristics.
- Sound business continuity practices, as well as Information Technology and cyber security best practices, provide some protection.

Key Finding 1

- □ Dependency on network-based systems is pervasive across all sectors. Critical components of our national infrastructure rely on a variety of network-based systems.
  - A sample of critical systems identified in the survey were reviewed.

Public Example: Slammer

- □ 15,000 high-speed servers
- □ 55 million meaningless database server requests
- □ 75,000 victims in 15 minutes:
  - Major airline reservation system shuts down
  - One of the nation’s largest banks had customers that could not withdraw money from its 13,000 ATMs
  - Shut down Emergency 911 dispatcher in suburban Washington
  - 300,000 cable modems went dark in Portugal
  - South Korea web access shut down
  - 27 million people lost cell phone or internet service
  - Five of the Internet’s 13 root name servers succumbed to the squall of packets

Total cost from lost revenue was estimated at more than $1 billion

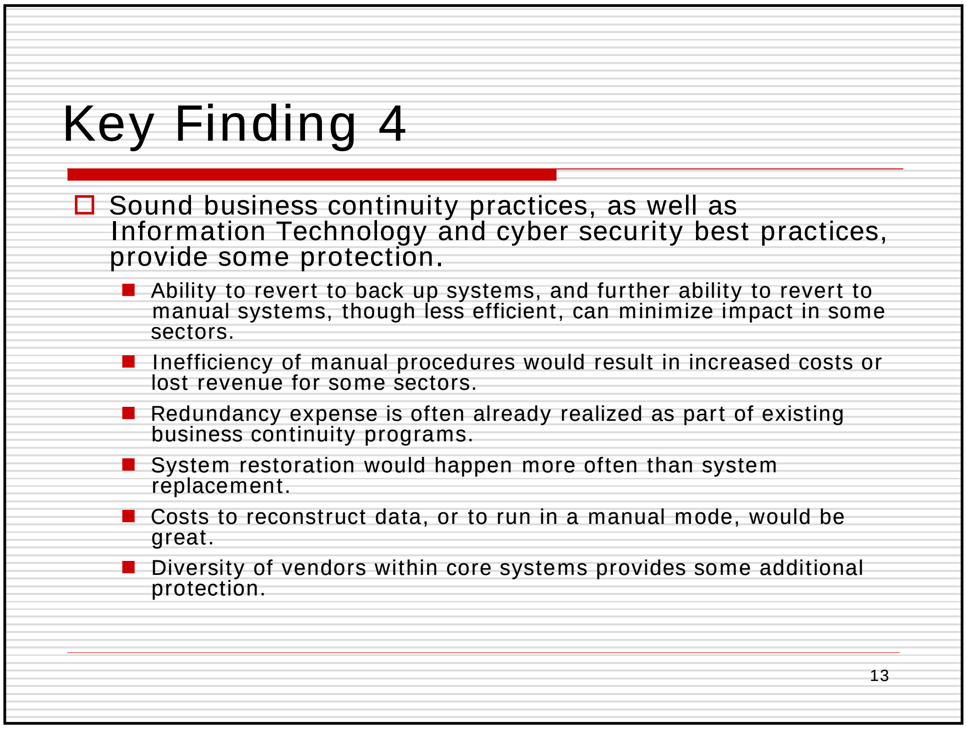
Key Finding 2

"Which sector are you most dependent upon?"

- Identified the sector upon which other sectors most depend.
  - Ranking was provided based on survey responses.

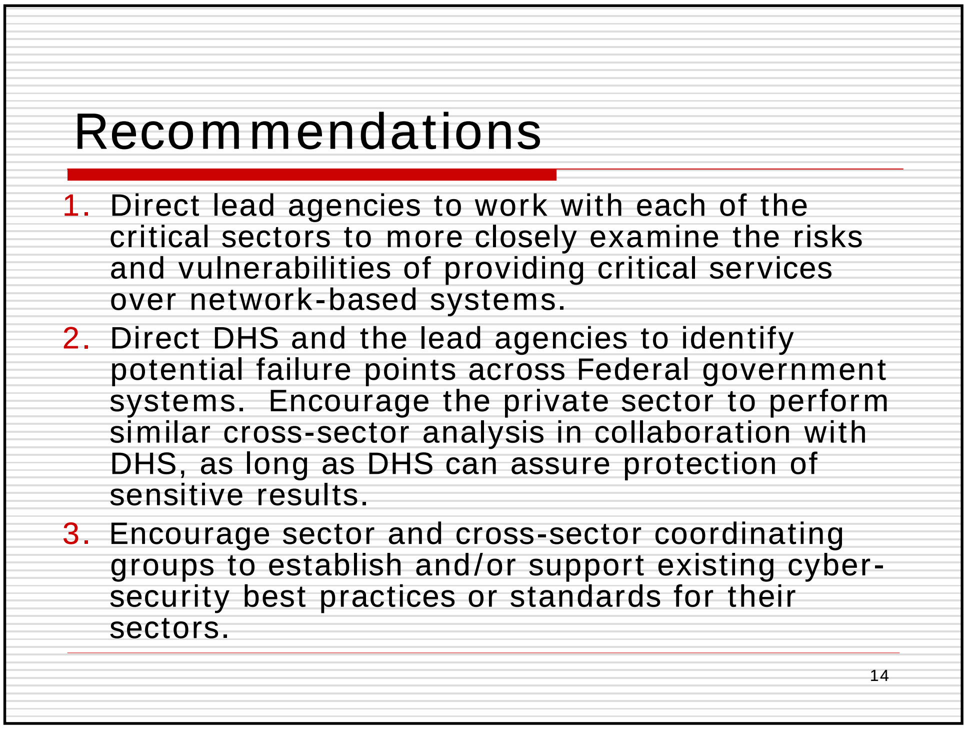
Key Finding 3

- The answer to the question "are we ranking our critical infrastructures as to their vulnerability to cyber attacks" is multi-faceted.
  - The degree that any sector is vulnerable to a cyber attack is dependent upon a number of characteristics:
    - Type of attack
    - Scope of the impact
    - Time of the attack
    - Duration of outage



Key Finding 4

- Sound business continuity practices, as well as Information Technology and cyber security best practices, provide some protection.
  - Ability to revert to back up systems, and further ability to revert to manual systems, though less efficient, can minimize impact in some sectors.
  - Inefficiency of manual procedures would result in increased costs or lost revenue for some sectors.
  - Redundancy expense is often already realized as part of existing business continuity programs.
  - System restoration would happen more often than system replacement.
  - Costs to reconstruct data, or to run in a manual mode, would be great.
  - Diversity of vendors within core systems provides some additional protection.



Recommendations

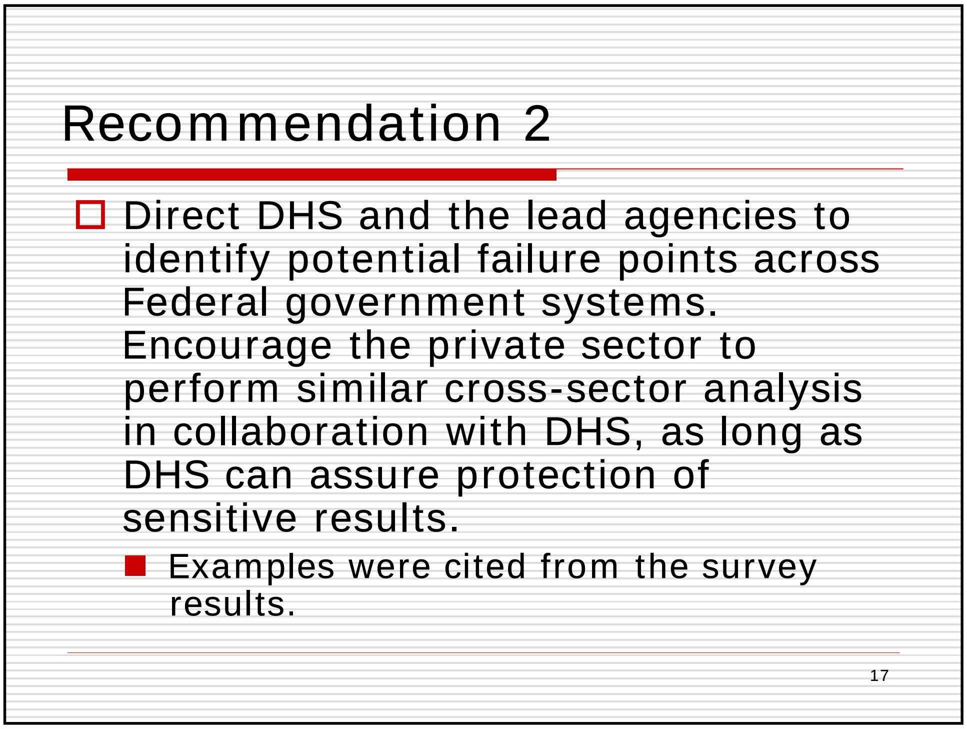
1. Direct lead agencies to work with each of the critical sectors to more closely examine the risks and vulnerabilities of providing critical services over network-based systems.
2. Direct DHS and the lead agencies to identify potential failure points across Federal government systems. Encourage the private sector to perform similar cross-sector analysis in collaboration with DHS, as long as DHS can assure protection of sensitive results.
3. Encourage sector and cross-sector coordinating groups to establish and/or support existing cyber-security best practices or standards for their sectors.

Recommendations *(Continued)*

4. Direct DHS to sponsor cross-sector activities to promote a better understanding of the cross sector vulnerability impacts of a cyber attack.
5. Direct Federal agencies to include cyber attack scenarios and protective measures in their disaster recovery planning. Encourage sector coordinating groups to include cyber attacks in scenarios to address in disaster recovery planning.
6. Encourage law enforcement to prosecute cyber criminals and identity thieves, as well as publicize efforts to do so.
7. Promote awareness of cyber security best practices at the corporate, government, small business, university, and individual levels.

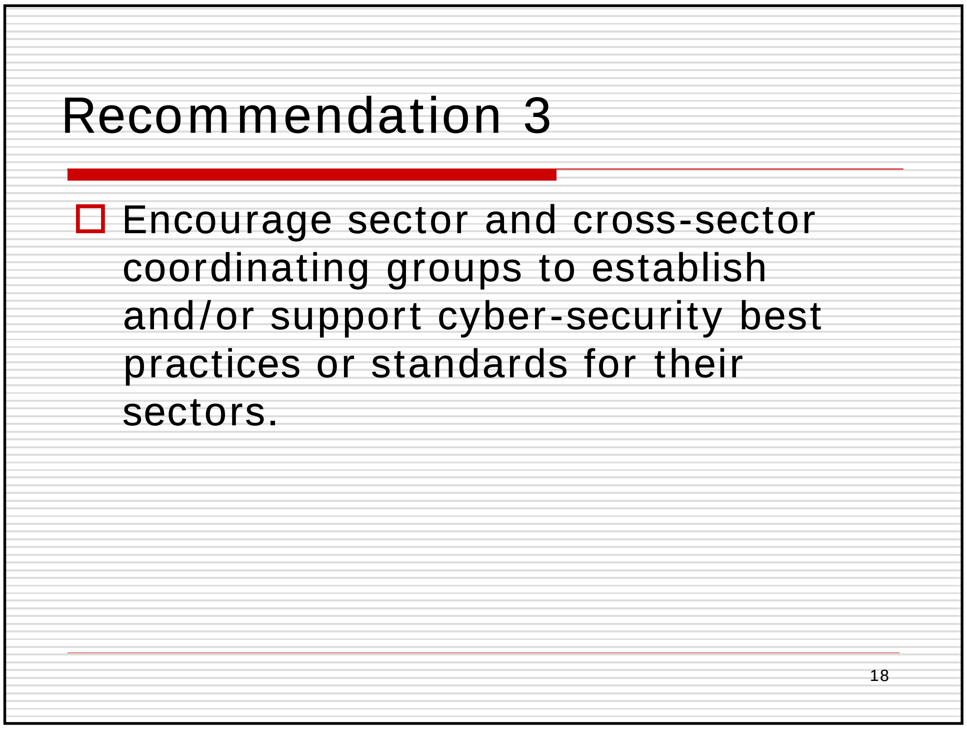
Recommendation 1

- Direct lead agencies to work with each of the critical sectors to more closely examine the risks and vulnerabilities of providing critical services over network-based systems.
  - Survey data revealed that some sectors may be more vulnerable than others to certain types of attacks.
  - Lead agencies should work with the sectors to understand these types of vulnerabilities.



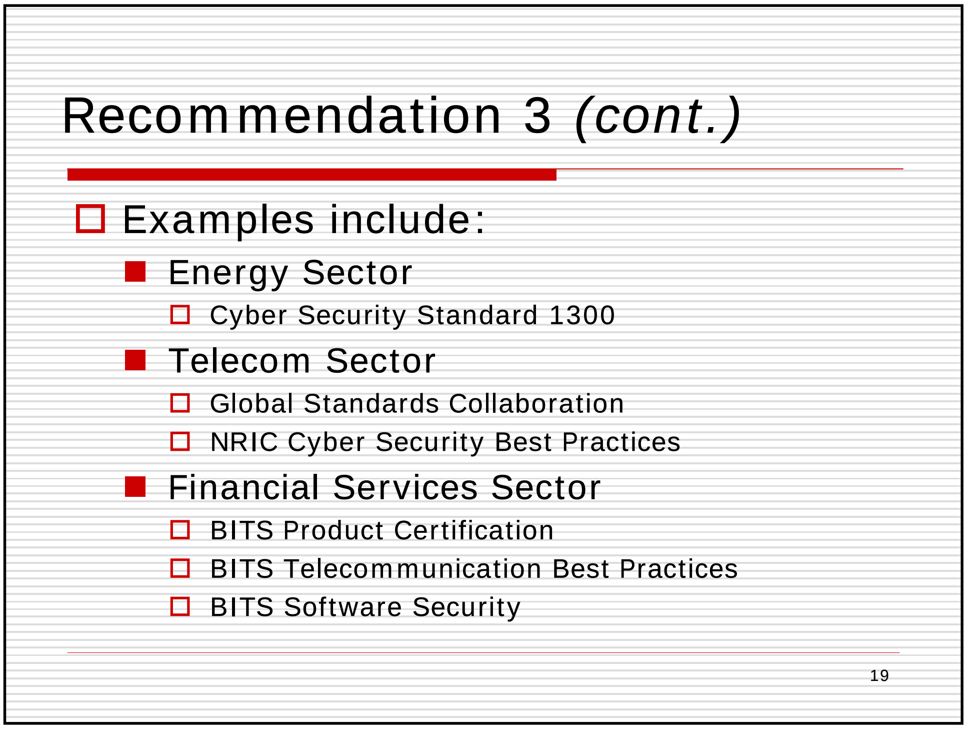
Recommendation 2

- 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, as long as DHS can assure protection of sensitive results.
  - Examples were cited from the survey results.



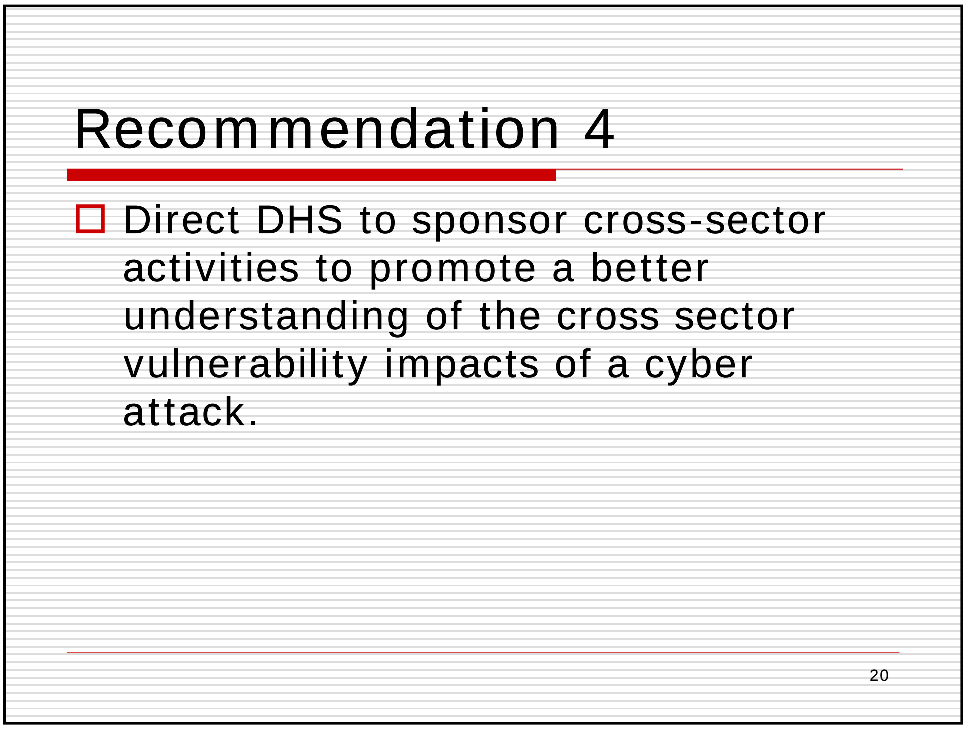
Recommendation 3

- Encourage sector and cross-sector coordinating groups to establish and/or support cyber-security best practices or standards for their sectors.



Recommendation 3 *(cont.)*

- Examples include:
  - Energy Sector
    - Cyber Security Standard 1300
  - Telecom Sector
    - Global Standards Collaboration
    - NRIC Cyber Security Best Practices
  - Financial Services Sector
    - BITS Product Certification
    - BITS Telecommunication Best Practices
    - BITS Software Security



Recommendation 4

- Direct DHS to sponsor cross-sector activities to promote a better understanding of the cross sector vulnerability impacts of a cyber attack.

Recommendation 4 *(cont.)*

Example:

- BITS Critical Infrastructure Forum, “Strengthening Resiliency of the Telecommunications and Energy Sectors.”
  - □ More than 100 executives from the financial services, telecommunications, energy, and chemical sectors attended.
  - □ Senior officials from Treasury, DHS and Federal Reserve Board participated.
  - □ Discussed critical issues related to interdependencies among these sectors and developed an agenda to address them.

Recommendation 5

□ Direct Federal agencies to include cyber attacks in scenarios and protective measures in their disaster recovery planning. Encourage sector coordinating groups to include cyber attack scenarios and protective

Recommendation 5 *(cont.)*

- How many .gov and .mil sites were hacked in 100 days?

1. Administrative Office of US Courts
2. Army NE Region Civilian Personnel Operations Center
3. Army Signal Center
4. Washington, DC
5. Defense Automated Printing Service
6. DISA Information Center
7. DOI US Bureau of Reclamation
8. DOI US Bureau of Land Management
9. Energy Sandia National Labs
10. Federal Maritime Commission
11. Government Printing Office
12. Multistate Tax Commission
13. NASA #2 Technical Info, et Propulsion
14. … 37

From August to November, 2000, SANS Institute reported that 37 sites were defaced in 100 days. By Spring of 2001, one site a day was reported defaced.

NASA implemented an effective program that reduced vulnerabilities from 1.3 per machine to fewer than 7 vulnerabilities per 1,000 systems.

Recommendation 6

- Encourage law enforcement to prosecute cyber criminals and identity thieves, as well as publicize efforts to do so.

Recommendation 6 *(cont.)*

- Successful capture requires collaboration across organizations and national boundaries, as well as acute technical skills by the investigators:
  - 22 year old Welsh web designer infected 33,000 computers in 42 countries with 3 viruses
  - 18 year old Exeter student hacked into 17 US Department of Energy’s Fermi National Accelerator Labs web sites
  - 18 year old high school student in Germany responsible for the Sasser virus
- Motive for cyber attacks appears to shifting away from a leisure activity to an opportunity to make money

Recommendation 7

- Promote awareness of cyber security best practices at the corporate, government, small business, university, and individual levels.
- NASA example
- NRIC Best Practices
  - Slammer:
    - Originated in Asia at 12:30 am Jan 25 – 03
    - Patch was available in July 2002
    - Did not affect sites that used general Best Practice concept of “turn it off if not needed”