

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING

Tuesday, April 13, 2004

2:00 p.m. – 5:00 p.m.

National Press Club

Ballroom

Washington, DC

AGENDA

- I. OPENING OF MEETING** *Nancy J. Wong*, U.S. Department of Homeland Security (DHS)/Designated Federal Officer, NIAC
- II. ROLL CALL OF MEMBERS** NIAC Staff
- III. OPENING REMARKS**
- Lt. Gen. Frank Libutti (USMC, ret.)*, Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security;
- Gen. John A. Gordon (USAF, ret.)*, Assistant to the President and Homeland Security Advisor, Homeland Security Council;
- Richard K. Davidson*, Chairman, President & CEO, Union Pacific Corporation; Chairman, NIAC; *Erle A Nye*, Chairman of the Board of TXU Corp; newly appointed Chairman, NIAC; **Passing of the Gavel**; and
- John T. Chambers*, President & CEO, Cisco Systems, Inc.; Vice Chairman, NIAC
- IV. STATUS REPORTS ON PENDING INITIATIVES:**
- A. HARDENING THE INTERNET** *George H. Conrades*, Chairman & CEO, Akamai Technologies; NIAC Member

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

Meeting Minutes and Briefing Materials for April 13, 2004 Meeting

Page 2

- | | |
|--|--|
| B. PRIORITIZATION OF CYBER VULNERABILITIES | <i>Martin G. McGuinn, Chairman & CEO, Mellon Financial Corporation; NIAC Member</i> |
| C. COMMON VULNERABILITY SCORING SYSTEM | <i>Vice Chairman Chambers; and John W. Thompson, Chairman & CEO, Symantec Corporation; NIAC Member</i> |
| D. EVALUATION AND ENHANCEMENT OF INFORMATION SHARING AND ANALYSIS | <i>Thomas E. Noonan, Chairman, President & CEO, Internet Security Systems, Inc; NIAC Member</i> |
| V. FINAL REPORT AND DISCUSSION ON GOVERNMENT INTERVENTION / BEST PRACTICES FOR ENHANCING SECURITY OF CRITICAL INFRASTRUCTURE INDUSTRIES | <i>Karen Katen, President, Pfizer Global Pharmaceuticals and Exec. V.P., Pfizer Inc.; NIAC Member</i> |
| VI. ADOPTION OF NIAC RECOMMENDATIONS | NIAC Members |
| VII. UPDATES | |
| A. NSTAC | <i>Dr. Vance D. Coffman, Chairman & CEO, Lockheed Martin; Chairman, NSTAC</i>
<i>F. Duane Ackerman, Chairman & CEO, Bell South; Vice Chairman NSTAC</i> |
| B. NATIONAL CYBER SECURITY DIVISION | <i>Amit Yoran, Director, National Cyber Security Division</i> |
| C. HSPD 7 BRIEFING | <i>Ken Stroech, Chief of Staff for Infrastructure Protection</i> |
| VIII. NEW BUSINESS | <i>Chairman Nye; NIAC Members</i> |
| IX. ADJOURNMENT | |

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON

Chairman Davidson; Vice Chairman Chambers; Mr. Berkeley; Mr. Conrades; Ms. Katen; Mr. Dunham; Gen. Edmonds; Chief Gallegos; Ms. Grayson; Mr. Martinez; Mr. McGuinn; Mr. Noonan; Mr. Nye; Mr. Thompson; and Ms. Ware

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL

Mr. Barrett; Mr. Carty; Ms. Marsh;

STAFF DESIGNEES ATTENDING ON BEHALF OF ABSENT NIAC MEMBERS:

Rob Clyde (for Mr. Thompson); John Puckett (for Mr. Holliday); Howard Schmidt (for Mr. Webb); Ed Ternan (for Mr. Hernandez); Jonathan White (for Ms. Katen).

STAFF DESIGNEES MONITORING PROCEEDINGS VIA CONFERENCE CALL ON BEHALF OF ABSENT NIAC MEMBERS:

Tom Lockwood (for Governor Ehrlich); Sgt. Paul Morrell (for Commissioner Kelly);

MEMBERS ABSENT:

Dr. Rose.

OTHER DIGNITARIES PRESENT:

U.S. Government: Mr. Robert E. Coyle, Acting Legal Advisor for Ethics, the Department of Homeland Security; Gen. John A Gordon, Assistant to the President and Homeland Security Advisor, Homeland Security Council; The Honorable Frank Libutti, Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection; Mr. Ken Stroech, Chief of Staff for Infrastructure Protection, the Department of Homeland Security; 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

The meeting was called to order and formally opened by Ms. Nancy J. Wong, Designated Federal Officer for the NIAC. Ms. Wong welcomed attendees to the eighth meeting of the NIAC and the second meeting of year 2004, including Chairman Davidson, Vice Chairman Chambers, newly appointed Chairman Nye, Under Secretary Libutti, Mr. Jim Caverly representing Under Secretary Liscouski, all other NIAC members and their staffs, the many other federal representatives, and the members of the press and public. Ms. Wong reminded participants that

the meeting is open to the public and, therefore, care should be exercised when discussing potentially sensitive information.

II. ROLL CALL

Ms. Nancy Wong called roll.

Ms. Wong said the Council approved two sets of recommendations during the January meeting, an Interdependencies Risk Assessment and the second on Vulnerability Disclosures as they relate to information systems. Those reports and recommendations have been transmitted to the President and are currently under review by the White House. They are available for viewing on the DHS website.

The NIAC has five more issues to report on. In addition, this meeting will include a briefing by Dr. Vance Coffman, the Chairman of the National Telecommunications Advisory Council; Amit Yoran, Director for National Cyber Security Division; and Mr. Kenneth Stroech, Chief of Staff for Infrastructure Protection Office who will provide a briefing on the Homeland Security Presidential Directive 7 and the progress of the National Critical Infrastructure Protection Plan. .

Ms. Wong introduced Undersecretary Libutti who introduced Gen. Gordon, and he made the following remarks on behalf of the Department and this directorate.

III. OPENING REMARKS

Lt. Gen. Frank Libutti (USMC, ret.), Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security;

Gen. John A. Gordon (USAF, ret.), Assistant to the President and Homeland Security Advisor, Homeland Security Council;

*Richard K. Davidson, Chairman, President & CEO, Union Pacific Corporation; Chairman, NIAC; Erle A Nye, Chairman of the Board of TXU Corp; newly appointed Chairman, NIAC; **Passing of the Gavel**; and*

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

Under Secretary Libutti thanked Ms. Wong and said it was an honor for him to introduce his dear friend, Gen. John A. Gordon. The Under Secretary said the General is an assistant to the President and advisor to the Homeland Security Council at the White House. He said that this is a critically important job. He said Gen. Gordon is both a visionary and a forward-thinker in the area of counter terrorism.

Gen. Gordon thanked Under Secretary Libutti and all the attendees for coming to Washington. He told the audience the President understands the value the members bring to Washington. He said that the members operate the cyber systems that are the backbone of commerce, industry, science, and education in America and are in many ways the embodiment of the private and public partnership that must form the cornerstone of Cyber Security. Gen. Gordon said the President counts on the NIAC to provide real, direct, and actionable advice and recommendations to improve Cyber Security. He thanked the Council for the last two reports, Vulnerability Disclosures and Cross-Sector Interdependencies Risk Assessment, which were submitted during the January meeting. He said the Vulnerability Disclosure report contained real, actionable recommendations supporting the development of common vulnerability management architecture. The Interdependencies Risk Assessment validated the need to support the organizational structures behind Critical Infrastructure Protection to strengthen Sector Coordinators and Information Sharing and Analysis Centers (ISACs). The Homeland Security Council and DHS are looking at these recommendations very hard. Gen. Gordon said it is in this spirit that he looks forward to the new reports and recommendations from today's meeting.

Gen. Gordon went on to say that the NIAC is a great group. The key to its effectiveness, other than the leadership of Chairman Davidson and Vice Chairman Chambers, is that the members actually do most of the work themselves—something unusual on advisory panels. The Homeland Security Council and the Department of Homeland Security truly benefit from the knowledge, experience, and leadership of some of the most senior members of American business leadership and state and local government. This is recognized, valued, and appreciated.

Gen. Gordon then offered special thanks for Chairman Davidson's effective leadership for the last two and a half years and thanked him for remaining as an active member.

Gen. Gordon thanked Erle Nye in advance for taking over the Chair of the NIAC, for his commitment, and for the contributions he will be making. He acknowledged business partnerships can be tough and private/public partnerships can be even more difficult. The Council, under Mr. Nye's leadership, will have an important role in keeping this partnership healthy, balanced, and productive. Gen. Gordon then turned the floor over to Chairman Davidson.

Chairman Davidson thanked Gen. Gordon for his comments and said that serving as chairman of this group had been quite an interesting experience. He said he is not a "techie" by nature but has had great support from Rick Holmes in his organization and even more importantly, support from the other members of the Council composing a cross section of great companies in the United States. He said the Council has really been a blue-ribbon group and the members are thankful for their support staff as well. The Council has made a number of very important recommendations to the President of the United States-- most of the Council members feel this is an honor. The Council has covered a wide range of subject matter—the President himself posed several questions to be addressed by the council. He said that it had been an exciting period and that he had enjoyed his tenure as Chairman. He also thanked Vice Chairman Chambers for his role with the NIAC. Chairman Davidson said he was pleased to be turning the gavel over to Mr. Nye. He passed the gavel over to Mr. Nye.

Incoming Chairman Nye thanked Mr. Davidson for his comments and contributions to the Council. He noted Mr. Davidson's leadership, enthusiasm, and guidance has been tremendous. He said leadership is reflected in the quality of the work of the Council, which produced two reports in the last meeting. The reports have been transmitted to the White House and the department and have been very well received. Chairman Nye said he had received word that the administration is impressed with the work the Council is producing. He acknowledged there is a lot more to do. Nonetheless, he told the Council to take courage from the reception their work has received and to maintain the pace Chairman Davidson set. Chairman Nye turned the floor over to Under Secretary Libutti to provide his remarks.

Under Secretary Libutti thanked the Council for their work and offered to stay and answer questions or hear comments he would take back to IAIP and DHS to work aggressively. He expressed best wishes from Secretary Ridge and thanked Chairman Davidson, Mr. Nye, and Vice Chairman Chambers for their leadership. He thanked the Council for their invaluable work over the last year. Under Secretary Libutti said the Council's contributions have proven effective in various situations including Cross Section Interdependencies and Risk Assessment Guidelines. He cited the final report and recommendations on the Vulnerability Disclosure Framework Report and Best Practices for Government Intervention to Enhance Security of the Nation's Critical Infrastructure as examples. The Under Secretary said the Council's studies and recommendations have illuminated various issues for DHS. He stressed it has been a challenging year protecting the nation, standing up the organization, and developing strategic policy that will affect us all in the coming years, especially, in the area of protecting our critical infrastructure. The Council is extremely instrumental in assuring infrastructure security decisions are not made in a vacuum. Important decisions must incorporate all elements involved within the public and private sectors. This Council lends a unique and vital perspective to the process of how critical infrastructure decisions are made and implemented. Private industry, state and local government are the front lines in defending our critical infrastructures. The Council's expertise and judgment are highly regarded and its recommendations carry substantial weight.

He said the formation of IAIP has created a unique, integrated capability to not only map the current threat picture against the nation's vulnerabilities, but also assess the risk of a terrorist attack based upon preventative and protective measures already in place. The IAIP team is enabling the government to move from a reactive posture in the homeland security business to one of risk management and mitigation.

He cited the following as examples:

- Coordination of operation Liberty Shield and the rapid enhancement of security at more than 145 national sites and assets,
- Implementation of the wireless priority service to ensure the continuity of cellular networks nationwide,
- Continuation of improvements in the Homeland Security Advisory System,
- Establishment of the National Cyber Security Division, and
- Formally executing the Protective Critical Infrastructure Information Program.

Even with these accomplishments, he stressed there is much more to be done. The United States remains at risk, and critical infrastructure will remain one of the top priority targets for terrorists

desiring to destroy the U.S., its infrastructure, economy, and people. The Government continues to work towards implementing the National Response Plan and the National Infrastructure Protection Plan for Critical Infrastructure—the latter being coordinated through the Infrastructure Protection Office. That office will unveil implementation steps for a national Critical Infrastructure Protection (CIP) program as required by Homeland Security Presidential Directive 7. Both of these national plans are basic roadmaps for CIP. Under Secretary Libutti said he is pleased about the substantial progress being made and looks forward to working with the Council over the next year.

He also praised outgoing Chairman Davidson, saying he wanted to recognize his extraordinary leadership and service to the country. He said the nation is a much safer place as a result of Chairman Davidson's work. Under Secretary Libutti said he was happy to learn Chairman Davidson was planning to stay on as a member of the Council. He then recognized and thanked incoming Chairman Nye by wishing him the best of luck and telling him he has the department's full support. He offered to take questions from the Council.

Chairman Nye asked if anyone had questions for Under Secretary Libutti.

Vice Chairman Chambers requested Under Secretary Libutti inform the NIAC if he would rather see them apply their resources to other areas. He said they needed a regular check and balance in terms of what the Council's priorities are, and making sure they are accomplishing the goals set forth for them. He also said he wanted the NIAC to make a difference and requested Under Secretary Libutti's guidance, which he said would not offend Council members.

Under Secretary Libutti said the Council was on track and productive. The goal now is to implement the Council's findings, particularly across the infrastructure industry overall. He stressed that IAIP works with other members of the federal government, particularly in terms of the intelligence sharing piece, and by extension sharing information from the Council, and with industry overall. He stated his top two priorities were information sharing and infrastructure protection.

Chairman Nye thanked Under Secretary Libutti and asked if anyone on the phone or on the Council had a question or comment for him. There were no questions. He asked Vice Chairman Chambers if he had any comments.

Vice Chairman Chambers said that in only a year and a half, Chairman Davidson created an environment where the CEO's, along with the support of their staffs, truly got involved. He added it is important that the Council not lose that talent. For example, he said if you think about George Conrades, Marty McGuinn, Margaret Grayson, John Thompson or Tom Noonan, you see CEO's get involved in every weekly session of their study groups; that's what really distinguishes the Council in terms of making it as effective as possible.

Chairman Nye thanked Under Secretary Libutti and offered the podium to Vice Chairman Chambers.

Vice Chairman Chambers said he hoped the CEOs and their staffs continued to stay as involved with the Council as they have since its inception. He warned that the Council should limit recommendations for regulations to when there is actually a problem. He welcomed Chairman Nye to his new, challenging role and congratulated Ms. Katen and her key staff leads for taking on the role of regulation. He said he looks forward to the final report today and that the Evaluation and Enhancement of Information Sharing report from Mr. Noonan's working group was also important. While not final, he said the group is making good progress on information sharing in private industry and government. Vice Chairman Chambers then thanked members of NSTAC for joining the meeting of the Council today.

Chairman Nye took the podium and called for a motion to approve the minutes from the January 13, 2004 meeting. Mr. McGuinn made the motion and Mr. Noonan seconded it. He asked if there were further discussion about the minutes. There were none and he recommended approval of the minutes. The motion carried and the Council approved the minutes.

Chairman Nye turned the floor over to George Conrades to discuss the effort of his working group's report on Hardening of the Internet.

IV. STATUS REPORTS ON PENDING INITIATIVES:

- | | |
|--|--|
| A. HARDENING THE INTERNET | <i>George H. Conrades, Chairman & CEO, Akamai Technologies; NIAC Member</i> |
| B. PRIORITIZATION OF CYBER VULNERABILITIES | <i>Martin G. McGuinn, Chairman & CEO, Mellon Financial Corporation; NIAC Member</i> |
| C. COMMON VULNERABILITY SCORING SYSTEM | <i>Vice Chairman Chambers; and John W. Thompson, Chairman & CEO, Symantec Corporation; NIAC Member</i> |
| D. EVALUATION AND ENHANCEMENT OF INFORMATION SHARING AND ANALYSIS | <i>Thomas E. Noonan, Chairman, President & CEO, Internet Security Systems, Inc; NIAC Member</i> |

Hardening the Internet

Mr. Conrades thanked the Chairman and briefed the Council on the working group's progress. He said the working group is off to a good start and has agreed on the scope, which is no small task. The study group holds conference calls every Tuesday and the work has been divided into two sub-tasks. One is protecting the infrastructure itself, and the other is addressing the customer environment, which could affect the infrastructure. He said they are finding that private entities and government entities are already providing best practices and recommendations, which have been proving helpful. The study group plans to draw upon these recommendations, reinforcing as broad a consensus as possible on solid recommendations. The task ahead of the working group is to make policy recommendations to the NIAC underscoring and educating about issues relevant to the vulnerabilities of the Internet, and the good things that could be done

to protect it. Mr. Conrades introduced Mr. Andy Ellis to report on the progress of the study group, supporting the working group in more detail.

Mr. Ellis thanked Mr. Conrades and the NIAC and said the study group's mission has been to develop guidance based on the best practices that have already been laid out for Internet systems management. The study group divided the practices into two categories: those addressing how to implement best practices and increase the likelihood of their adoption and those addressing new technology areas where there is room for improvement. Much of the infrastructure environment lies strictly in the hands of the private sector. As a result, any policy recommendations the Council makes will need to take that into account. The study group has found best practices are normally aimed at small and medium players in a location. The large enterprises, whether on the network side or from a customer environment perspective, generally follow most of the best practices. The study group is trying to understand why more people don't follow best practices. The information is there to address root causes. Mr. Ellis said because some best practices take a long time to be adopted, it is important to continually improve on them, targeting larger enterprises and larger players with room for improvement. Also, the study group will look at new technologies while there is still time to improve methods. For example, the cost of investing in new systems is frequently a barrier to adopting any new technology.

The study group determined there are two types of attacks that present risks to the national infrastructure. The first are those attacks going against pieces of the infrastructure, which could take the infrastructure out of commission. The second are attacks that take advantage of the infrastructure and its weaknesses to seize control of some information asset. The study group looked at the Border Gateway Protocol (BGP), the underlying routing fabric for the Internet; the Domain Name Servers (DNS), which provide translation from human readable names into Internet Protocol (IP) addresses; and Distributed Denial of Service attacks, which either use or are directed at the infrastructure.

The study group identified three possible ways to secure the infrastructure today. The first is to have small and medium sized enterprises rely on best practices of securing individual network elements. The second is to educate users to have hardened passwords and secure systems by implementing processes to ensure only certified configurations, and hardened systems are deployed into the field. Third, it is important to secure methods administrators use to actually control the backbone of the infrastructure itself.

The study group also identified some technical areas that warrant consideration—prefix and package filtering. These are methods of ensuring only legitimate traffic can pass across the Internet itself. This ensures one network is not sending traffic belonging to another network-- a common tactic used in cyber attacks.

Mr. Ellis said the study group has explored the development of routing registries—methods of determining which network is allowed to send traffic from given Internet Protocol address ranges. After the study group looked at the various secure BGP protocols to increase the reliability in the underlying Internet infrastructure itself, it found many operational management issues needing to be addressed that might require global implementation.

Mr. Ellis said a major target for cyber attacks are non-enterprise end users or customer environments--small and medium businesses or individual home users not necessarily implementing good security practices, such as patch levels or firewalls, in their environments. While no individual machine represents a critical asset, many machines together can be used as a weapon against the Internet itself. He said best practices need to center around individual participation and education. The study group is beginning to explore public education and awareness, and potential incentives to encourage the acquisition of security tools to protect those systems.

There is a range of approaches to incentives: 1) the negative incentives such as regulation of private sector companies, which requires compliance with some standard; 2) neutral incentives, which means the government would only do business with certified vendors who had secure enterprises themselves; and 3) positive incentives, which are ways to convince companies to adopt best practices because it is in their best interest.

The study group's next step is to identify elements of guidance based on the published public recommendations and existing practices. He concluded his remarks by saying the study group has begun to draft and review a report for the Council's working group.

Chairman Nye asked if there were any questions for Mr. Conrades or Mr. Ellis.

Gen. Gordon thanked Mr. Conrades and Mr. Ellis for the discussions and asked if the meeting of the Task Force for Corporate Governance held the day earlier would fit into the study group's ideas about best practices.

Mr. Conrades said the discussions from Task Force for Corporate Governance fits independently in the study group's weekly discussions in thinking about the corporate environment, customer environment and best practices. He said with the increased importance of the audit function for information security, there would be a way to incorporate the thought that best practices relative to enterprise security would also be relevant against cyber attacks.

Gen. Gordon said that information from this task force seemed like an excellent avenue to tie both the enterprise and the non-enterprise side together. He said there might be some things that can be done to encourage small businesses. He stated that it is still hard for even knowledgeable users to buy a new computer with a wireless Internet and make it operational quickly. Somewhere along the line, the industry has to make it one step easier for even a reasonably knowledgeable small user to be able to rapidly use new computers without having to read overly confusing manuals.

Vice Chairman Chambers stated the report was solid. The study group needs to consider how reinforcing best business practices can be done for both enterprise users and service providers. Vice Chairman Chambers asserted that operationally relevant practices in an enterprise environment are not necessarily relevant in a service provider environment. He said the working group should consider a recommendation around government funding in research to develop key concepts appropriate to both hardening the Internet and relevant to the service provider

environment. Vice Chairman Chambers stated that with a relatively minor amount of funding, outstanding results can be achieved.

Chairman Nye said it was an excellent idea.

Mr. Conrades agreed and said he appreciated Vice Chairman Chambers bringing up the service provider environment because it's apparent from the group's work on the task force and the study group, that the major service providers are extremely sensitive to this issue and have every interest in protecting and safeguarding the Internet. They are very conscious of the best practices because they are implementing them all.

Gen. Edmonds added the Council should look at the Internet in layers rather than as a total entity. If the working group focuses on large Internet service providers constructing the first line of enterprise architecture defense, it may be easier to get smaller businesses to follow suit.

Vice Chairman Chambers agreed and said that was why the Council needs service provider representation. He said all these problems are more inter-related than first realized and having them here, as part of the committee, would add a lot of value, and make the Council better because of it.

Chairman Nye asked if there were further comments.

Mr. Conrades accepted what Gen. Edmonds said and added that if Gen. Edmonds' remarks were suggesting a cascading approach for implementing best practices, the Council should consider investigating this possibility.

Chairman Nye thanked the working group for the update and turned the meeting to Mr. McGuinn and his working group.

Prioritization of Cyber Vulnerabilities

Mr. McGuinn introduced Ms. Vismor, his colleague from Mellon, and began the status update on the Prioritization of Cyber Vulnerabilities Working Group. He stated that prioritization of cyber vulnerabilities is an especially relevant topic to the financial services sector. He said the prevalence of cyber security incidents has escalated both the risk and cost to the financial services industry. Internet viruses and worms are becoming increasingly virulent and expensive. As an example of these trends, he used the 2003 "Slammer" worm—when it began infecting machines, it was the fastest spreading worm in history. It was soon eclipsed by the succession of viruses like "My Doom" and "Netsky." Carnegie Mellon University recently reported that over 114,000 computer virus attacks and computer breaches in 2003 resulted in more than \$140 billion in damages worldwide. The Banking Industry Technology Secretariat (BITS), a financial services industry group, has estimated the cost of addressing software vulnerabilities within our sector alone is approaching \$1 billion annually. While he said numbers seem high, they are in fact limited to preventive costs and infrastructure repair costs. They do not include the actual loss of business as a result of the attacks, which is really the focus of this study group.

Mr. McGuinn said the status update would provide information on what has been accomplished on this topic since the January meeting of the NIAC. He said he would briefly review the purpose of the working group. The group is attempting to rank the impact that cyber attacks might have on various sectors—the task is in response to a question originally posed by President Bush in a July 2002 meeting with the NIAC. Mr. McGuinn noted that a number of initiatives are currently underway relating to this topic. For example, the study group discovered the Department of Justice’s Bureau of Justice Statistics results of a survey examining cyber crime in 2001. Of the 198 companies that responded, 74% reported being victims of cyber crime. Nearly 66% of these companies had been victimized by a computer virus at least once, 25% had experienced denial of service attacks, and 20% reported their computer systems had been vandalized or sabotaged. Results of the survey did not, however, specifically address these problems on a sector-by-sector basis. Mr. McGuinn commented that this survey was of a pilot group, but there are plans for a refined version of the survey to be sent out to 36,000 companies. This survey will examine the impact of computer security incidents in terms of down time, cost to recover, and other monetary losses. Mr. McGuinn said the working group will recommend to the Council that there needs to be more collaboration with the Bureau of Justice to ensure the addition of sector-specific questions on the final survey.

Mr. McGuinn turned the meeting over to Ms. Vismor to provide an update on the actions taken by the study group supporting the working group.

Ms. Vismor said that while the study group believes the Department of Justice survey will help validate the group’s findings, the group thinks it is still worthwhile to continue its own initiatives originally defined at the January meeting. The study group’s analysis will enable cataloging the primary functional uses of the Internet by sector, assess the business impact of a cyber incident on the sectors, and consider the implications on national security in emergency preparedness. Once complete, the study group will then be able to rank which sectors are the most vulnerable to a cyber attack. Ms. Vismor said that, unlike the Bureau of Justice, the study group would address a much smaller targeted audience. There will be a good representation across all the critical sectors. Activities to date have included a briefing from Cisco on their efforts to develop best practices for the implementation of the Border Gateway Protocol (BGP). BGP is one of the core routing protocols for the Internet. The analysis was technical in nature, but the conclusion was if best practices were followed in deploying BGP routers, chances of exploiting this piece of infrastructure could be significantly reduced. The study group then developed a draft survey cataloging the uses of cyberspace and the economic impacts.

Ms. Vismor thanked Tim Zoph, Healthcare Sector Coordinator, who took a sample survey and had members of the healthcare sector validate the study group’s approach. The study group then received a briefing from Scott Borg, senior research fellow at Dartmouth University, with a number of innovative ideas and concepts. Within the past two weeks, the study group has also collaborated with Mona Rantella from the Department of Justice. Ms. Rantella worked extensively on the Bureau of Justice’s statistic survey and has provided the study group with valuable insight into the survey process. The model proposed by Scott Borg really helped to shift the focus from an event’s technical vulnerabilities to its economic consequences. The first example Ms. Vismor used was technical exploits—these are incidents tracked by the Computer Emergency Readiness Team (CERT). The second example represents system confidentiality—

ensuring both systems availability and integrity. The third example, the Borg Model, asserts that business flow can be interrupted so that business operations stop. Data may be corrupted, false, or the system itself may become unreliable. Ms. Vismor said that the fourth example is that actual data could become public over the Internet, making users afraid or unwilling to use the system. For example, a denial of service attack compromises system availability and interrupts data flows.

Ms. Vismor said the amount of risk in cyberspace is a product of three things:

- Who is coordinating the cyber attacks?
- What vulnerabilities can these attacks exploit?
- What is the overall business impact?

In terms of the survey content, the study group is asking the participants to identify their three key information systems that are running over the network. The study group also looked for key economic data, revenue, and efficiencies from these systems. There are also questions around potential impacts to emergency preparedness, national security, and dependencies on other critical infrastructures. For each key system, participants are asked to consider business interruptions:

- What would be the effect if the interruption were over a three-day period or over a week?
- What would happen if false data were inserted into a system?
- How long would it take to determine that false data was inserted?
- What would the customer impact be?
- Are there alternate systems?
- If the current system were no longer considered trustworthy or reliable, what would the cost be to switch to the alternate system?
- What alternatives will customers have to switch to another system?
- How effective will a new system be and at what cost?

The study group plans to send out the survey within the next two weeks and to begin analyzing the results by June. Ms. Vismor thanked the study group participants, with a special thanks to Scott Borg, Mona Rantella and Ken Watson.

Chairman Nye thanked Mr. McGuinn and Ms. Vismor and asked if there were any questions or comments.

Chief Gallegos said the survey didn't seem to lend itself towards information from government entities regarding the impact of cyber vulnerabilities on their own operations, from traffic signals to sewer systems. He asked if government entities were going to be included or if there is an assumption that what goes on in business will carry over to government agencies.

Ms. Vismor said that government entities are one of the critical infrastructures. The Defense Industrial Base is a specific example.

Chief Gallegos said he would like to see further exploration of overall government impact. He said that government entities are impacted across the board, from traffic signals to sewer systems

to almost total operations in large cities. Small cities also rely on these types of network capabilities and they need to be surveyed.

Mr. McGuinn and Ms. Vismor said that the study group would consider this.

Vice Chairman Chambers congratulated the working group and said they were examining realistic situations that have the potential to affect every industry from government to enterprise to small business. He said that once the study group determined the impact of cyber vulnerabilities, the study group could give sector-specific pointers on what industries can do differently. Vice Chairman Chambers said that the Prioritization of Cyber Vulnerabilities was a complex task and applauded the way it is being approached.

Chairman Nye thanked Mr. McGuinn and Ms. Vismor and turned the floor over to Vice Chairman Chambers and Mr. Thompson to present the update on Vulnerabilities Scoring System.

Common Vulnerability Scoring System

Vice Chairman Chambers thanked Chairman Nye and began by saying the working group realized early on that there are a great many vulnerability scoring systems out there. Mr. Chambers thanked Mr. Thompson and Ken Watson, and Rob Clyde from Symantec for the work that has been done so far for this report. He said the study group supporting the working group is about 75% of the way complete and plan to have it wrapped up by the next meeting in July with the final report. Vice Chairman Chambers said this supports the Vulnerability Disclosure Guidelines, which were presented to the President on March 13. Vice Chairman Chambers introduced Ken Watson to provide the Council with an update.

Mr. Watson said the goal of the status report was to provide background, reiterate the scope of the effort, provide current status, and give a glimpse of the proposed framework. He said the study group believes it can finish this effort by the July 13 meeting of the NIAC. Mr. Watson asserted the need for this effort was identified as the Council's working group worked through the vulnerability disclosure guidelines. The Vulnerability Disclosure Working Group tested existing scoring methodologies and found very different results for the same threats. He stated since the guidelines support common processes to manage vulnerabilities, a common way to approach scoring or ranking is required--the purpose is to develop a general method for ranking the threat of vulnerabilities to information systems. Mr. Watson said the term "information systems" is used in its broadest sense so the rating system can be applied to application software, server software, hardware, standards, and protocols. The ultimate purpose of the work is to: 1) support a common understanding of the vulnerabilities that constitute risk; 2) to define a common process for converting those characteristics into a single threat rating; and 3) to provide a common language for communicating that risk.

Mr. Watson said the working group would recommend the creation of a Common Vulnerability Scoring System (CVSS) to the NIAC. He said the study group thinks this will develop a common framework for evaluating vulnerabilities. The group developed a simple, modular approach so it can be consistently used in different environments. The framework does not replace the disclosure decisions—he said stakeholders were intended to use the previously published guidelines. The proposed CVSS defines metrics, which are common to almost all

security vulnerabilities. Severity ratings for vulnerabilities can be derived from metrics using the process. A metric can fall into one of three groups:

- ❑ **Base Metrics:** Constant and relevant at any time in any operational environment and that are applicable to every organization and don't change over time,
- ❑ **Temporal Metrics:** Change over time, but are independent of environments,
- ❑ **Environmental Metrics:** Specific to an organization's implementation of effective technologies.

Mr. Watson said if there were a vulnerability specific to a particular operating system, an individual using a different operating system would have a lower score. If that operating system were exclusive in that environment, scores would be significantly higher; this is the base temporal metric and an environment metric.

He said the development of the CVSS is about 75% complete. The metrics have been defined in a draft document, and the study group is finalizing rating formulas and weights. The study group continues to develop the process for generating a single score from all three elements and documentation of all the guidelines. The group still needs to develop a process for producing a single score from all three elements as well as documentation of all guidelines. Testing has not yet started, but will begin once the final draft of the formula and process is completed. Several organizations and security experts will be included in the testing process. Technical representatives of those organizations, which generally have scoring methodologies, have been consulted including Cisco, Symantec, Internet Security Systems (ISS), Microsoft, CERT CC at Carnegie Mellon, and others. Technical representation came from DHS and EBay for the study group. The study group's intention is for the scoring system to be used not only by the security committee, but also by infrastructure owners and operators.

Mr. Watson said there are many factors to consider when assessing vulnerability severity. The study group has included 14 different metrics. These factors include a vulnerability's impact on the affected system, the system's accessibility to attackers, the attack's complexity, and the ability of patches. The study group attempted to make these metrics as generic as possible so they are applicable to all vulnerabilities.

Mr. Watson said the scoring process should be progressive. Base scores should be calculated at the moment of vulnerability analysis or discovery. Temporal modules set at the outset would be used to adjust the base score as temporal metrics change; for example, when a patch is available or an exploit is published. Environmental modules are meant for organizations implementing this process for task prioritization within their own environments. He said final ratings with temporal environmental modules represent the threat of a vulnerability at a specific point in time and within a specific environment. Base metrics include constant characteristics, which include items like excess vectors, authentication requirements, access complexities, impacts on confidentiality, integrity, availability, and the requirements of an exploit.

Temporal metrics include exploit complexities in greater detail, remediation complexity, and confidence. Environment characteristics include target distribution:

- ❑ How populous is the target technology in an environment?

- What is the potential for casualties?
- What is the potential for financial loss?
- What is the potential for physical loss in the environment?

Mr. Watson stated the metrics are not equally weighted and careful thought has gone into each metric's influence on the overall score. The temporal formula will be applied to the initial base score, followed by the environmental formula to generate a single score for a particular time and a particular environment.

Mr. Watson turned the podium over to Mr. Clyde to discuss next steps and timelines.

Mr. Clyde thanked Mr. Watson and said that several organizations will be involved in test runs determining systems usability. This usability measurement is in terms of cyber vulnerability characteristics generalities and the ability of process implementers to assign meaningful values to metrics. The ratings' usefulness will be determined through comparison of related vulnerabilities against each other and against subjective practical risk perception by experts as well as through comparison with ratings produced by other threat-rating systems. After testing is completed, the participants' feedback will be evaluated. These evaluations will allow for detailed process guideline development for assigning metric values, including examples from the testing process. These guidelines are meant to aid in the CVSS implementation. Mr. Clyde concluded his remarks and returned the podium to Chairman Nye.

Chairman Nye thanked the working group and asked if there were any questions.

Mr. Conrades asked how the working group envisioned the use of CVSS from a stakeholder point of view and what that value would be.

Mr. Watson said it would depend on the environment and the user operating the system. Presently, those scoring vulnerabilities for writing virus signatures, assessing trends like CERT at Carnegie Mellon, or developing software patches have their own scoring system. There is no common understanding around threat severity, so the purpose of the report is to develop common language. For example, Mr. Watson said for the users and infrastructure environment the CVSS could prioritize remedies in one environment, but still speak the same language as the vendors and security community.

Chairman Nye asked if there were other questions.

Mr. Berkeley asked if there was any effort to rank the importance of the industry's implementation of the scoring system.

Mr. Watson responded that the study group had not gone in that direction as it is examining specific characteristics understood by those handling information structure vulnerabilities on a daily basis. He added the Prioritization of Cyber Vulnerabilities Working Group is looking at broader sector implementations.

Chairman Nye asked if there were additional questions.

Mr. Dunham said the working group should also consider the petroleum industry along with the electricity structure. Mr. Dunham said he had discussed it with Mr. Davidson previously, and offered to volunteer someone from ConocoPhillips to represent the petroleum industry.

Chairman Nye thanked Mr. Dunham and asked if there were any other questions.

Ms. Ware said she sees a great deal of potential in the interaction between industry and government in developing a sophisticated common vulnerability scoring system that could interface with portions of the Best Practices for Regulatory Guidance report. The CVSS may aid in measuring or quantifying the point where the government and private sector need to come together over critically vulnerable infrastructures.

Chairman Nye thanked Mr. Watson and the rest of working group, and said they have made excellent progress. He commended Vice Chairman Chambers for the work thus far.

He then called on Mr. Noonan to discuss the progress of the Evaluation and Enhancement of Information Sharing and Analysis working group.

Evaluation and Enhancement of Information Sharing and Analysis

Mr. Noonan thanked Chairman Nye and the members of the NIAC and said he appreciated the opportunity to provide the final report on the Working Group for the Evaluation and Enhancement of Information Sharing and Analysis.

Mr. Noonan said he thinks the NIAC agrees that the defense of our nation and critical infrastructures depends upon complex and interdependent infrastructures in both the public and private sectors. The private sector controls a vast majority of critical infrastructure and many of these industry sectors heeded the call of Presidential Decision Directive (PDD-63) that established the Information Sharing and Analysis Centers (ISACs) to proactively manage risk in industry. He said that he was going to address methodology findings and proposed recommendations as the process moves from draft form to final.

The current project analyzes the current environment for information sharing and analysis across critical industry sectors and proposes recommendations regarding enhancements, increased effectiveness, and broader influence across industry sectors. The working group did not initially realize the size of the undertaking, but has made great strides.

The study group wanted to leverage existing information and analysis; especially from the body of work produced by the Information Sharing and Analysis Center (ISAC) Council. The ISAC Council has shared a lot of its studies and analysis to the DHS already.

Mr. Noonan said Ms. Wong has been very helpful in reviewing General Accounting Office reports and other reports on critical infrastructure information sharing and identifying funding options and incentives. Mr. Noonan said the study group focused on four attributes the group

wanted to analyze in each industry sector--particularly business models for sharing and analyzing information.

Mr. Noonan said from the inception of the task, there have been significant positive changes in the landscape affecting information sharing. First, DHS released HSPD 7 and 8 in December 2003 through the White House, superceding PDD-63. These drove recommended policy changes for a number of things including ISACs. Mr. Noonan said while DHS underwent significant staffing and procedural developments, the private sector ISACs formed the ISAC Council and, as a result, many ISACs have undergone market-driven restructuring.

Mr. Noonan said the study group's first finding is that there are manifest information sharing differences between cyber and physical infrastructures. While most ISACs are coordinated along industry lines, there are great commonalities in cyber infrastructure and great distinctions within physical infrastructure. Mr. Noonan said information sharing has many levels and there is no single definition of information sharing. Some of this information is based on strategic value focusing on the threat and its potential to harm critical functions, including sector infrastructures. Operational information is passed quite freely among ISACs and information is focused on critical infrastructure sectors and how they support systems providing services to a large number of people or support the economy in defense of the nation. There are also levels of tactical information sharing with both physical and cyber attributes around first responder incidents. Mr. Noonan said over the past few months, the study group discovered many organizations had differing opinions around the scope of information sharing covered but there were universal concerns around vulnerability information. Mr. Noonan said cyber components of information sharing are not universal across sectors but common vulnerability definitions emerged:

- ❑ Attack vectors are exploits usually written to take advantage of a vulnerability,
- ❑ Threats are who will attack a system,
- ❑ Incidents are when a system is attacked and compromised by an exploit,
- ❑ Best practices are the ability to proactively alleviate the threat with early warning systems providing mass communication.

Mr. Noonan asserted that there were two private sector levels clearly evident in the working group's findings: 1) critical infrastructures and 2) non-aligned businesses. He said a challenge for the ISACs is the delivery of information to the private sector from a critical infrastructure. As a result, the working group intends to propose a specific recommendation to address this fact. In critical infrastructure sectors, some of the key industries can be reached quickly and efficiently, but for industry as a whole, there are many thousands of businesses that are unreachable. He continued, saying some ISACs are communicating with DHS and its lead agencies, which is great progress, but other ISACs are at very different maturity levels.

Mr. Noonan stated that four major issues have been identified by the study group, and that the group will have specific recommendations for the definitions, roles, and responsibilities of the ISACs and sector coordinators. He further stated that the roles and responsibilities of the ISACs and sector coordinators are not well understood and have not been universally adopted by the federal government. He said definitions are necessary and participants must be more clearly defined. Current business models for most ISACs have strengths and weaknesses around the flow of analysis and information to its members. There is a lack of understanding and reliance

on the unique sector research and analytical capabilities. He said a majority of the research is being done in the private sector to advance their business capabilities. The private sector operates over 80% of the infrastructure and consequently has a grasp on regular occurrences. But private sector analysis growth is focused primarily on sector vulnerabilities and enabling the ISAC to provide refined analysis over raw data. There must be a better understanding of the government's requirements for analysis and products. The study group suggested an ISAC maturity model, which has been used and identified within the ISAC Council and can be a great metric. The ability to actually drive performance through metrics begins at capabilities maturity level one and moving through level five. The capabilities are based on analysis, coordination, communication, and response time. Moving at level five signifies anticipatory risk mitigation mode as opposed to a "react-and-hope" mode. The working group will propose four specific recommendations:

1. Clarify roles for ISACs and sector coordinators,
2. Information sharing and analysis should be centralized in each sector,
3. Dissemination, sharing and communication of information on both cyber threats and physical threats; in most cases, these mechanisms are stood up, but they still need to be driven forward.
4. Sector coordinators should develop policy and sector-wide vulnerability analysis for risk mitigation. Progress is being made on this already.

The working group proposed recommendations included:

- Joint work with the private sector to further refine the role and responsibilities of the sector coordinator, which came through HSPD7,
- Refine the relationship of the coordinator to the ISAC,
- Enhance private sector ISAC reach through funding of infrastructure enhancements,
- Create a two-tier information mode by incorporating private sector analysis and focus with government's reach in communication for general alerts,
- Provide for a timely flow of private sector information to the government.

Mr. Noonan then recognized the work of Wells Fargo, EDS, Cisco, Symantec, V-One, North American Electricity Reliability Council (NERC), Securities Industry Automation Corporation (SIAC), DuPont, and Intercon Security Systems. Mr. Noonan said his report will be circulating in final draft form and he would work with Ms. Wong to draft a transmission letter from the Council to the President by the July meeting. He concluded his remarks and asked if there were questions.

Chairman Nye said this was an extremely complex and detailed report, and the Council owes Mr. Noonan a thorough review of his work. He asked if there were any questions. There were no questions.

Chairman Nye thanked Mr. Noonan and urged members to review the report once it is submitted and provide the working group with thoughts. Chairman Nye then called for a 10-minute break.

When the meeting resumed, Chairman Nye called on Ms. Ware to present the final report on Government Intervention/Best Practices For Enhancing Security of Critical Infrastructure Industries.

**V. FINAL REPORT AND DISCUSSION ON *Karen Katen*, President, Pfizer
GOVERNMENT INTERVENTION / BEST Global Pharmaceuticals and Exec. V.P.,
PRACTICES FOR ENHANCING SECURITY Pfizer Inc.; NIAC Member
OF CRITICAL INFRASTRUCTURE
INDUSTRIES**

Ms. Ware, substituting for Ms. Katen, thanked Chairman Nye and introduced the final draft report on Best Practices for Government Intervention and Enhancing the Security of Critical Infrastructures. The NIAC chose to refine the definition of government regulation to government intervention. She said the group had been working on the report since summer 2003, evaluating issues related to the topic. The working group broke its work down into three phases: 1) surveying the Council members, 2) collecting data across many companies and several sectors, and, 3) conducting an in-depth look at four sectors with very different characteristics: Chemicals, Financial Services, Information Technology, and Water. Ms. Ware said the working group deliberations produced the following seven recommendations:

1. When considering the power that market forces can exert on ensuring the critical infrastructure security, the working group concluded that security would be most efficiently improved where market forces are free to operate.
2. If market forces prove unable to operate efficiently and quickly, government should consider intervention, but only when: 1) a clear characterization of the potential harm resulting from an attack is; and 2) a better understanding is developed of the role that market forces exert in promoting an improved, sector-wide security posture across the sector. He also noted that, in the case of 1), this is a very good example of where the vulnerability scoring system may be useful.
3. When government does consider intervention, a deep understanding of sector dynamics is needed for intervention to be effective. Given the extensive differences within and across the critical sectors, any proposed intervention must be designed and enforced at an appropriate level and through the most effective agency or agencies. The working group proposes:
 - Discussions between DHS and industry to guide recommendations, and
 - A significant degree of analysis completed at the sector level before any specific policy recommendations are made,
4. Since companies have recognized the risk and are already responding to the threat through market and mechanisms, before intervening the government should consider the pace at which sector-level activities are occurring within the infrastructure.
5. Government actions that least distort the market are best. Before reaching a conclusion that market intervention will be beneficial, government should consider whether market forces will work over time, whether the sector will be able to establish mechanisms to increase security, and whether intervention can achieve its desired goals without causing any subsequent negative consequences.
6. A common framework can be used to guide discussions between the government and sectors on the role of market intervention. At a tactical level, the working group's assessment of whether there is need for intervention found eight valuable screening questions by providing a common language for the discussion,

7. When intervention is planned, identified best practices should be considered. The study has suggested some conditions under which government involvement is most likely to provide a beneficial effect.

Ms. Ware then asked Jonathan White, Ms. Katen's representative for the study group, to describe the process through which these conclusions were reached.

Mr. White thanked Ms. Ware and offered sincere regrets on behalf of Ms. Katen for her absence. He also thanked the study group and recognized Bruce Larson of American Water, Glenn Rust of Sterling Bank, Beth Turner of DuPont, and Ken Watson and Adam Golodner of Cisco Systems for their extensive, valued and as yet, unrecognized contributions to the report.

Mr. White said in support of the recommendations, he was going to run through the group's charter and how the report met its goals. He asked the NIAC to review the supporting material and pay close attention to the process used to realize the final report.

He began reviewing the original charter presented to the working group and said it was necessary for the NIAC to be clear on two scope issues in the work. The first is the term "infrastructure", which the study group found very ambiguous, because there is so much convergence between physical and information infrastructure, two tightly interdependent domains. Secondly, the study group recognized the breadth of possible tools government can use to encourage and enhance security posture. These include, but are not limited to, supporting innovation, encouraging diffusion of best practices, offering tax credits, sponsoring research and development, and educating the public. Mr. White stated that regulation is simply one of many possible responses to a perceived need.

Mr. White asserted that, to encourage a more sustained and effective security posture, the recommendations focus on four issues:

- Understanding market dynamics on how sectors really operate,
- Defining how government should interact with industry,
- Creating a framework for scoping discussions with sectors,
- Identifying best practices for government to refer to when considering intervention.

He said the group would like to describe how these tools and processes lead to sector-specific views for each sector. To develop these tools and framework, the study group first surveyed the NIAC members for their views of market and government support and security. The study group then reviewed existing studies on government efforts and conducted a number of in-depth interviews across many critical infrastructure sectors, to develop a broad view of security issues. From this data, the study group has constructed a framework for analysis and discussion. Lastly, the validity of this framework has been tested extensively in four sectors with thorough stakeholder input across sectors ensuring that they remain fully informed. The report does not recommend government intervention at this time, and does not believe that it is required in any particular arena.

Mr. White said the first recommendation is the role of market forces. The study group's initial survey of NIAC members showed extremely strong support for market-oriented approaches to this issue. Roughly 66% of the NIAC were in favor of market-based solutions, and subsequent

discussion and review has led to this conclusion. He said where market forces are free to operate, they prove to be the most efficient and efficacious vehicle to enhance critical infrastructure security. This conclusion was not obvious from the start. Most members of the study group operate and thrive in highly regulated industries and were adamant that well-constructed regulations acted to strengthen their industry in the national interest. Nonetheless, the support, in principal, for a primarily market-driven approach, was unanimous. Where members might differ in their own position, they still recognized that conditions for efficient market operations were not in place for them. Consequently, the study group also agreed that if market forces proved unable to operate efficiently or the pace of change is too slow, government should consider intervention. The intervention, however, should only be after potential harm has been well characterized and the roles of market forces within the sector are fully understood.

Mr. White said the second recommendation requires a deep understanding of sector dynamics for effective intervention. Within sectors and sub-sectors, difference in industry structure, market forces, and regulations play out in very subtle ways. For example, the water sector is composed of local, independent monopolies with weak market forces--a stark difference to financial services, which is an inter-connected and competitive sector with strong market forces and mature existing regulatory structures. No single set of rules will effectively apply to both sectors. Moreover, in the sector labeled financial services, banking institutions, structures, and interconnected networks regulated at the federal and even super national levels operate differently than insurance companies. Sectors are not homogeneous and market forces play out through these differences. He asserted that cultivating diversity within and across sectors, any proposed intervention must be designed and enforced at the appropriate level. The study group believes discussion should initially take place between DHS and industry sectors to guide future recommendations. A significant degree of analysis is needed before specific policy recommendations are made or enforced through appropriate oversight agencies.

Thirdly, Mr. White continued, customers already recognize how their critical assets could be damaged by malicious intent and companies are responding effectively through competition and cooperation to address threats. In addition, some industry groups, such as the American Chemistry Council, have published mandatory security guidelines for their sector's members. Across these sectors, different forms of oversight exist that provide an obligation to conduct activities such as vulnerability assessments; meeting outcomes goals, such as recovery times; or taking specific steps, such as setting up physical fencing around facilities. Sector-led activities have been found to be effective in augmenting market forces driving security. The strength of these enforcement mechanisms can vary significantly leading to a spectrum of responses. He also said in one financial services poll, existing regulation already drives security behavior effectively, and many participants see this regulation as pivotal in securing the system and excluding weak players from participation. At the other extreme, in information technology, little intervention exists, and the participants feel if customers are in a position to switch products and services in a competitive environment, market forces will eliminate non-performing suppliers. These organizations and sector dynamics are the results of changing pace as a sector matures.

Mr. White said it is important to note what conditions warrant the consideration of direct intervention. This decision requires prudent judgment and assessment to the appropriate degree

of risk exposure based on the pace of market activity and the impact of failure. Mr. White spoke first about the impact. Although all NIAC sectors are deemed critical, there are differences in potential impact. The catastrophic failure we saw in the electricity industry last year, where one failure impacted multiple industries and the damage to key payment systems such as a major Federal Reserve district bank, can significantly have more impact than damage to a small regional bank. The study group spent a considerable amount of time discussing the distinction between tragic and catastrophic events. It can be hard to separate events threatening national security and the economy from those that do not, but where sector or sub-sector members are critical nodes for the system, they clearly need to meet required security standards. This judgment call depends on the attack impact on an individual player, the spillover impact on other players, and the impact of damage of one sector upon another. If this severity warrants a response, what should it be? He said given the power of market forces, before backing market intervention, one should consider whether market forces would work over an acceptable timeframe. Making this assessment requires deep understanding of both industry-specific issues and system interdependencies. Some sectors may be able to establish their own mechanism to increase security-- if they can achieve wide participation and consensus-driven recommendations, it may obviate the need for government intervention.

Mr. White stated the government should consider whether the sector would be able to establish mechanisms to increase security. In sectors with diverse types and sizes of firms, government actions may be warranted. The American Chemistry Council represents most of the U.S. productive capacity for chemicals, encompasses a small percentage of facilities, and is calling for federal regulation to require chemical facilities to take these actions.

Finally, he said there might be a perceived need for government intervention in some sectors. The NIAC needs to consider whether this can be successfully applied. Regarding issues like safety, bank regulation has achieved its desired effects without causing negative consequences. Members of the financial sector were adamant that the securities act and subsequent regulations are widely held examples of good legislation, which have added transparency and improved the operation of market forces in that sector. It is seen as a pillar for the stability for the nation's financial services sector. In mature sectors, particularly those with a history of successfully evolving responses to threats, effective public/private partnerships and regulated processes may be suitable to facilitate the desired security enhancements within the sector. Within immature sectors, with rapidly evolving business models, the government needs to carefully determine whether regulation can achieve its intent without causing severe negative consequences such as stifling innovation. To be clear, he said, regulation in information technology and the Internet may blunt innovation resulting in less consumer choice, economy, and security. The study group found no case for government intervention in this sector, and believes regulation of the Internet is unwise, because market forces will continue to drive adoption and innovation. There are many examples of well-intentioned regulation that is crude and costly. Mr. White said it's important to remember the existence of market failure does not guarantee that government can provide a better solution.

Mr. White discussed the framework that was described by Ms. Ware in her opening statements. The study group used this to provide a common language describing the power of market forces to coordinate sector activity and provide critical infrastructure protection. The study group's

decision process is a useful lesson providing a microcosm example of the challenges the NIAC will face reaching consensus on these issues. At the start of the study, members held diametrically opposed views on the need for market intervention in their sectors. To resolve the issue, study group members first needed to move away from entrenched positions and towards a common understanding. From these discussions, the following eight questions emerged, forming a basis from which insights were developed on sector dynamics, a rich discussion on the effects of government insight, and oversight on industry participants. They include:

1. Are there network interdependencies?
2. Does security drive customer switching?
3. Is voluntary sector activity occurring?
4. Can the sector exert peer pressure?
5. Do attacks occur frequently?
6. Could attacks cause catastrophic injury or major economic damage?
7. Is industry profitable enough to invest?
8. Is there sufficient expertise to execute a plan?

Mr. White repeated themes that Ms. Katen had reported on during prior Council meetings, but the themes have reappeared time and again. First, in group discussions with participants, there was an emphasis on the need for government and industry to develop plans and drive towards outcomes in concert. If government fails to collaborate and build on the work of early adopters, this will provide a disincentive to companies taking timely remediation.

Secondly, Mr. White said the study group believes the recommendations should be gradually implemented to allow industry to prepare and spread out capital investments and allow agencies time to mobilize staff. Alignment of legislation at the federal, state, and local levels created jurisdictional issues causing confusion. Security should also be considered in all regulations put forth in other areas because they may enhance and diminish the effectiveness of security activities documented in the report. There should also be a flexibility to evolve or retire interventions in proposed changing circumstances. Mr. White concluded his remarks and turned the podium back to Ms. Ware.

Ms. Ware thanked Mr. White and the study group.

Chairman Nye thanked Ms. Ware and Mr. White. He said the report is up for consideration for passage by the NIAC. He said the report was a subject of internal discussion and debate and he believed the conflicts have been balanced very well. Chairman Nye said he would like to hear from the members of the Council.

**VI. ADOPTION OF NIAC
RECOMMENDATIONS**

NIAC Members

Mr. Berkeley said it was obvious a tremendous amount of work went into the report and made a motion to accept the report, Mr. Martinez seconded it.

Chairman Nye asked one more time if there was need for further discussion or comments.

Vice Chairman Chambers said all the topics covered during the meeting demonstrated a world-class effort. He said the Best Practices report was probably the most controversial of them all and wanted to congratulate the group for moving past what would have been a very easy theoretical discussion to say what could be done. He said the working group recognized such practices had to vary by sector and it was important to understand what those differences are. He added that the report was one of the best examples of what the Council has done on one of its hardest topics, and offered congratulations.

Chairman Nye asked if there were additional comments.

Chairman Nye said they had a first and a second motion, and called for a voice vote. He said all in favor of adopting the report; please say, "Aye."

The Council responded, "Aye."

Chairman Nye said all opposed say, "Nay". The motion carried unanimously.

He congratulated Ms. Ware and Mr. White. He thanked them for their excellent work and said it will add credibility to the Council and is appreciated.

Chairman Nye said that completes NIAC business. The Council has other updates, one of them being from the National Security Telecommunications Advisory Committee (NSTAC).

Chairman Nye then introduced Dr. Vance Coffman to provide an update on NSTAC activities.

VII. UPDATES

A. NSTAC

*Dr. Vance D. Coffman, Chairman & CEO,
Lockheed Martin; Chairman, NSTAC*

*F. Duane Ackerman, Chairman & CEO, Bell South;
Vice Chairman NSTAC*

Dr. Coffman thanked Chairman Nye and announced Mr. F. Duane Ackerman, the current vice chairman of NSTAC, would be taking over the chairmanship in May because that will be the beginning of the 27th NSTAC cycle. He said he would update the NIAC on the NSTAC's activities since July 2003, when he last addressed the Council. He would also let the Council know about upcoming meetings occurring in the near future.

Dr. Coffman noted NSTAC has provided the President with advice and recommendations on critical national security and emergency preparedness in telecommunications matters for more than twenty years and has been referred to, by some in government, as a model of industry and government cooperation.

The NSTAC is now in the last months of its 26th cycle, which runs from May 1, 2003 to May 19, 2004. Dr. Coffman said he would update the NIAC on the status of NSTAC's task forces and working groups during this cycle.

The Financial Services Task Force explored the physical aspects of the financial services sector's concerns around resiliency and redundancy capabilities of telecommunications infrastructure supporting financial services' mission-critical activities. This collaborative effort between the financial services and telecommunications sectors resulted in an outstanding draft report to the President. The report found the following:

- Comprehensive business continuity planning and practices are essential,
- National security and emergency preparedness functions should acquire the highest levels of telecommunications resiliency assurances available. The continuity of the payment, clearing, and settlement processes of the financial services sectors is critical to the overall economic security of the nation, and
- Public policy options are needed to stimulate investments. From a public policy perspective, appropriate mechanisms to stimulate market investments would enhance the National Security Emergency Preparedness (NSEP) telecommunications resiliency and should be identified.

The Satellite Task Force produced a report identifying 22 findings and highlights the need for the government to improve the management of its commercial satellite communications or SATCOM activities. The report provides three overarching recommendations to the President regarding:

- Developing national policy for the provisioning of management of commercial SATCOM services integral to the NSEP communications activities,
- Providing funding to support the implementation of a commercial SATCOM NSEP improvement program, principally an internal government activity similar in nature to the National Coordinating Center (NCC) of the National Communications System,
- Appointing commercial satellite service providers and associations to represent the SATCOM industry on the NSTAC itself.

The Trusted Access Task Force is examining various government and private sector models for background check processes for access to critical facilities. Government participation with the group has included personnel from the General Services Administration, the Transportation Security Administration, the Nuclear Regulatory Commission and others.

Last October, the Legislative and Regulatory Task Force sent a letter to the President advising him on national security policies and regulatory issues that conflict with the NSEP missions. The legislative and regulatory task force also recently produced a report on various information sharing under the Critical Infrastructure Information Act of 2002.

Dr. Coffman noted that he was interested in the NIAC's Evaluation and Enhancement of Information Sharing and Analysis Working Group and added that NSTAC will be willing to contribute.

He said the NSTAC Outreach Task Force has been arranging meetings with key government shareholders as follow up on NSTAC products and recommendations. The NSTAC is working with officials from the Office of Science & Technology Policy, the Homeland Security Council, the National Security Council, the Office of Management and Budget, and the Department of Homeland Security in this endeavor. Dr. Coffman said the task force is also planning an industry executive sub-committee offsite meeting later this year. The purpose of the offsite is to enhance relationships between the Industry Executive Subcommittee (IES) members and the NSTAC's government stakeholders.

The Research and Development Task Force has produced follow-up materials from the March 2003 R&D exchange, including an NSEP definition white paper and a draft white paper on the possible development of a pilot test bed for the national security and emergency preparedness research and development purposes. The task force has scheduled the 2004 NSTAC R&D exchange to be held later this year on the west coast; Monterey, California will be the site.

He stated the Cyber Scoping task force was recently formed, at the request of NSTAC principals, to focus on and prioritize various issues related to cyber infrastructure interdependencies. The Cyber Scoping group is an addendum to the activities of the Financial Services Task Force, which addressed the physical aspects of the financial services sectors around resiliency and redundancy capabilities of the telecommunications infrastructure supporting those financial services.

Dr. Coffman acknowledged the NIAC's efforts in the areas of cyber security, specifically its work on Hardening the Internet, Prioritizing Cyber Vulnerabilities, and the final report and recommendations on Cross Sector Interdependencies Risk Assessment guidance. The NSTAC is also interested in providing support or inputs to those efforts.

He then invited Chairman Nye and Vice Chairman Chambers to NSTAC's next meeting and welcomed the opportunity for the NIAC and NSTAC to work together. He concluded his report and asked if there were any questions.

Chairman Nye thanked Dr. Coffman and asked if there were any questions.

Vice Chairman Chambers commented on how important it was for the NIAC and the NSTAC to work closely together, share information, and synchronize efforts.

Mr. Noonan said that part of the information his working group used to produce the report on information sharing and analysis originated from work done by the NSTAC over many years. He said the NSTAC are real pioneers and the Council could learn a lot from the challenges in public/private partnerships the NSTAC encountered.

Dr. Coffman said he appreciated the comments.

Chairman Nye thanked Dr. Coffman and extended best wishes to Mr. Ackerman, he then introduced Amit Yoran, Director of National Cyber Security Division at the Department of

Homeland Security to provide insight on how his division and the department are implementing the NIAC's recommendations.

B. NATIONAL CYBER SECURITY DIVISION *Amit Yoran, Director, National Cyber Security Division*

Mr. Yoran thanked Chairman Nye and the esteemed members of the NIAC for the opportunity to come and speak before them. He said he was asked to provide insight into how DHS and the National Cyber Security Division (NCSA) are implementing some of the many recommendations of the Council.

Mr. Yoran said DHS is already supporting the development of common vulnerability management architectures, with a sub-recommendation to establish federal stakeholder groups focused on vulnerability management and vulnerability management architectures. To that end, the department recently established the Chief Information Security Officer's Forum, comprised of over 120 Chief Information Security Officers, representing various departments and agencies of the federal government. DHS implemented a government forum of incident response and security teams that perform the 24/7 cyber incident response functions across departments and agencies of the federal government to collaborate and share information. DHS has also implemented a cyber interagency incident management group where the various departments and agencies with significant operating capabilities in the cyber realm are represented, which has operating authority in the cyber domain. The division had been asked to promote efforts such as the Common Vulnerabilities and Exposures (CVE) list. DHS is funding various CVE extension efforts such as Open Vulnerability Assessment Language (OVAL), which proves it can promote a thriving private sector security innovation to create greater efficiencies for the nation in the area of cyber security.

He said in order to support robust voluntary information sharing within the NCSA, DHS is having the Infrastructure Coordination Division (ICD), part of the Information Analysis and Infrastructure Protection directorate, actively engaged in working with the ISACs. The department is in the process of setting up a cyber partnership program to execute the private/public partnership, which will adopt NIAC information sharing and analysis work. The NIAC had made recommendations to promote advanced industry and university research in the area of cyber security.

Mr. Yoran stated DHS is engaged with the National Security Agency on the Centers for Academic Excellence program and the National Science Foundation on its Scholarship for Service Program (CyberCorp) in the areas of information assurance. DHS is funding research-facilitating initiatives such as the development of large data sets available to private sector cyber security researchers. The department is also funding and making available a distributed, large-scale virtual machine system and network architecture for researchers to better test and evaluate the effects of their cyber security solutions in a realistic environment. Again, the goal of the Department of Homeland Security, in many of our cyber security initiatives, is to encourage private sector progress in the area of cyber security. Mr. Yoran thanked the Council for the opportunity to address them.

Chairman Nye thanked Mr. Yoran and said the Council was privileged to have a briefing by Mr. Stroech, Chief of Staff for Infrastructure Protection in DHS. He asked Mr. Stroech to make some comments on the critical infrastructure protection plan called for in that Homeland Security Presidential Directive.

C. HSPD 7 BRIEFING

Ken Stroech, Chief of Staff for
Infrastructure Protection

Mr. Stroech thanked Chairmen Nye and the Council for the opportunity to brief the NIAC. He said Robert Liscouski, Assistant Secretary for Infrastructure Protection, regrets he was unable to attend in person.

Mr. Stroech said the key policy drivers his office is using to develop the National Infrastructure Protection Plan (NIPP) come out of two key documents.

First, the Homeland Security Act calls for developing and implementing protective measures, administering warning capability, coordinating with industry, federal partners and state and local government, and assisting in incident response. The other, HSPD-7, defines how the federal government can accomplish critical infrastructure protection activities set forth in the Act. The framework identified in HSPD-7 divided responsibilities amongst various department agencies but give DHS overall leadership. He said it identified DHS as responsible for coordinating the national effort for protecting and enhancing critical infrastructure and key resources. It also identified sector-specific agencies having roles amongst the six or seven identified sectors and also laid out additional sector-specific responsibilities for DHS. HSPD-7 also addressed the roles and responsibilities and special functions other department agencies have as well.

Mr. Stroech said the critical infrastructure protection program is risk-based, and DHS must normalize, analyze, and prioritize those infrastructures and their vulnerabilities before implementing protective programs. DHS is doing this across all sectors and will incorporate that into a national plan.

He said each sector plan would include effectiveness measures, protection measures, vulnerabilities, priorities, and asset identifications as a first step. The department has the responsibility to connect the interdependencies across all sectors, rolling them into the overall national plan. The national plan will have common methodologies and metrics.

The HSPD requires that the NIPP be issued in December, but DHS is working to produce a draft plan by June and a final version by October, because of current threat situations and business urgency.

Mr. Stroech stated the way ahead is to continue engaging with sector-specific agencies, other department agencies, Congress, state and local governments, and the private sector through phase one. DHS agencies are now working on their sector-specific plans. In the May/June timeframe, the plan's first draft cut will be developed and incorporated into an integrated plan. In the end, for each of the sector-specific plans, DHS would like a scorecard and measurement on its progress and potential next steps.

Chairman Nye thanked Mr. Stroeck for his remarks asked if there were any questions. He said each Council member may have a fair amount of interest in what Mr. Stroeck is working on and asked to be kept up to date as much as possible.

Mr. Stroeck said he looked forward to that opportunity.

Vice Chairman Chambers said he would like to compliment the speakers because it helps the NIAC know where the results or output are being used effectively, particularly after hearing the last two speakers. He said the Council has a unique opportunity to build a base for critical infrastructure protection for decades to come. He thanked the Council and participants for their commitment and for coming to the meeting.

VIII. NEW BUSINESS

Chairman Nye; NIAC Members

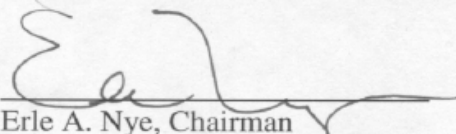
Chairman Nye asked whether there were any other items or issues the Council wished to discuss.

While no one had pressing issues to raise, Chairman Nye encouraged the Council to think about the subjects the Council has addressed, what other subjects need to be addressed, and to let Ms. Wong know between now and the July 13, 2004 meeting. The meeting is scheduled to be teleconference, but Chairman Nye said it might be more appropriate for the Council to meet in Washington and asked for everyone's flexibility. He said that information would be forthcoming.

IX. ADJOURNMENT

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: 
Erle A. Nye, Chairman

Dated: 7/15/04

ATTACHMENT A
(Status Report on Hardening The Internet)

NIAC Working Group on Internet Hardening

Interim Progress Report

George Conrades, Chairman and CEO - Akamai Technologies

Presented by

Andy Ellis, Director of Information Security - Akamai Technologies

13 April 2004

1

Agenda

- Background
- Methodology
- Key Issues and Preliminary Considerations
- Next Steps

2

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 incentivize 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

Study Group Participants

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

Overall Findings

- Best Practices
 - Best Practice recommendation are usually aimed at the small and medium size players
 - We need to understand *why* people don't implement best practice recommendations to change their behavior
 - Because best practices take a long time to be adopted, improving the existing "best" practice is a good place to impact the large players
- New Technologies
 - New technologies can present opportunities to improve existing methods of engaging in business
 - Investment in new systems is often a barrier to adoption.

7

Key Issues & Findings

- Infrastructure
 - Two types of attacks that present risk
 - Attacks against pieces of the infrastructure
 - Attacks using the infrastructure
 - Areas of investigation
 - BGP - the routing fabric of the Internet
 - DNS - The name server that supports human-readable names
 - DDoS - Distributed attacks using or directed at the infrastructure

8

Key Issues & Findings

- Three possible ways to secure the infrastructure:
 1. Secure individual network elements
 - Educate users: harden passwords, etc.
 - Implement processes to ensure secure initial/default installations
 - Run systems against security checkers
 - More secure “control planes”

Key Issues & Findings

2. Prefix Filtering
 - Explore development of a routing registry to store “allowed routes”
 - Potentially use soBGP or sBGP as an alternative
 - Many operational and management issues need to be addressed prior to global implementation
3. Packet Filtering
 - BCP38 in non-multi-homed environments
 - When filtering on source addresses, filter on allowed prefixes vs. announced prefixes

Key Issues & Findings

□ Customer Environment

- Non-enterprise end users
 - Represent a target-rich environment for attackers to collect assets to use in DDoS attacks
 - Best practices are oriented around individual participation and education.
- Incentives: public education and awareness, financial incentives to encourage the acquisition of security tools

11

Key Issues & Findings

□ Customer Environment

- Enterprise users
 - Protection steps need to be taken by corporate and public entities, not individuals
 - Incentives
 - Negative: regulation of private sector companies
 - Neutral: Government buying requirements
 - Positive: Provide education to company boards and audit committees to better enable broad corporate oversight

12

Next Steps

- Develop guidance based on current recommendations and existing best practices

- Draft and review report for the NIAC

ATTACHMENT B
(Status Report on Prioritization of Cyber Vulnerabilities)

NIAC Working Group on Prioritization of Cyber Vulnerabilities

Working Group Update

Martin G. McGuinn, Chairman & CEO
Mellon Financial Corporation

Tuesday – April 13, 2004

1

Presentation Outline

- Background
- Report on Actions to Date
- Survey Content
- Proposed Mission
- Proposed Framework
- Appendix

2

Background

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

Deliverables

- Summary of the types of Cyber Attacks
- Analysis of which Critical Infrastructures are vulnerable to those attacks – and rank if appropriate
- Summary of mitigants/protective measures
- Summary of implications/ramifications associated with successful attacks (based on results of a “Vulnerability Assessment Survey” customized for each critical infrastructure)

Report on Actions Taken to Date

- BGP Security Research Summary Jan. 28
 - Cisco Systems
- Draft survey developed and vetted Feb. 2
- Cyber Attack Economics Report Feb. 25
 - Scott Borg, Senior Research Fellow *
- Health Care sector sample Mar. 9
- Survey revised to reflect Borg model Mar. 15

* Institute for Security Technology Studies, Dartmouth College

5

Cyber-Attack Models

Types of Cyber Incidents (CERT)

- Probe
- Scan
- Account Compromise
- Root Compromise
- Packet Sniffer
- Denial of Service
- Exploitation of Code
- Internet Infrastructure Attacks

Information Security Model

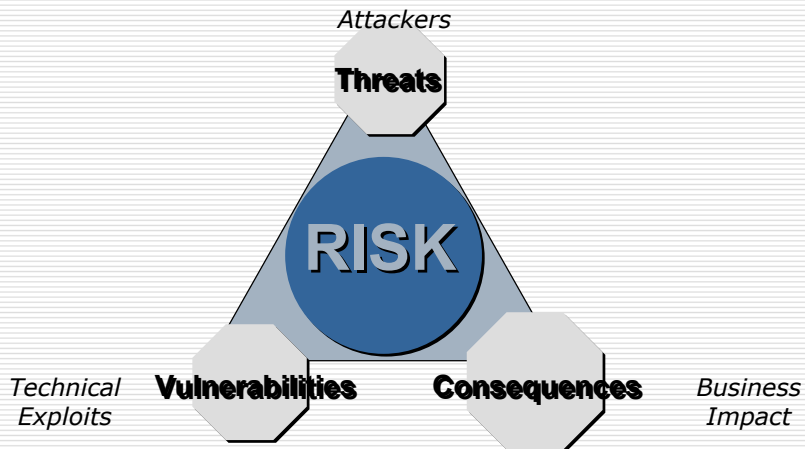
- Confidentiality
- Availability
- Integrity
- Authentication
- Non-repudiation

Business Categories (Borg Model)

- Interruption of data in order to interrupt business operations
- Corruption of data in order to cause it to operate defectively
- Obfuscation of data, causing people to be in the wrong business
- Publication of confidential data, undermining the ability to engage in any business

Technical Exploit → Compromises Security → Business Impact ⁶

Risk = Threats x Vulnerabilities x Consequences



7

Survey Content

- Identification of key information systems and what they accomplish
- Economic metrics of these systems
- Implications to National Security/Emergency Preparedness
- Dependency on any other network based critical infrastructure
- Dependency of a critical infrastructure on this service

8

Survey Content

- Evaluate the possible consequences of “types” of cyber attacks on each of the identified key systems:
 - Interruption of business operations
 - Business operates in a defective way
 - Distrust of the system
 - Undermine the ability to engage in that business

Survey Content

- Identifying what alternatives might be utilized in the event of a sustained attack on each of these systems

Next Steps

- Finalize survey April 14
- Survey distribution April 21
- Survey returned May 26
- Compilation and analysis June 30
- Deliverable July 13

Appendix

- Working Group Participants

Study Group Participants

- Susan Vismor, Mellon Financial Corp., Study Group Chair
- Teresa C. Lindsey, BITS
- Peter Allor – Internet Security Systems
- Bruce Larsen – American Water
- Chris Terzich - Wells Fargo & Company
- Ken Watson - Cisco Systems, Inc.
- 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
- David Sanders, DHS, National Cyber Security Division

ATTACHMENT C
(Status Report on Common Vulnerability Scoring System)

CVSS

The Common Vulnerability Scoring System

April 13, 2004
NIAC Vulnerability Disclosure Working Group
Scoring Subgroup

John Chambers
President & CEO
Cisco Systems, Inc.

John Thompson
Chairman & CEO
Symantec Corp.

Agenda

- Background
- Scope
- Status
- CVSS Framework
- Next Steps
- Timeline

Background

- ❑ Vulnerability Disclosure WG determined need for common scoring methodology in Jul 2003
- ❑ NIAC tasked Scoring Subgroup Oct 2003
- ❑ Purpose: Develop common vulnerability scoring methodology to promote understanding of severity, risk, and potential impact to aid in prioritizing response actions

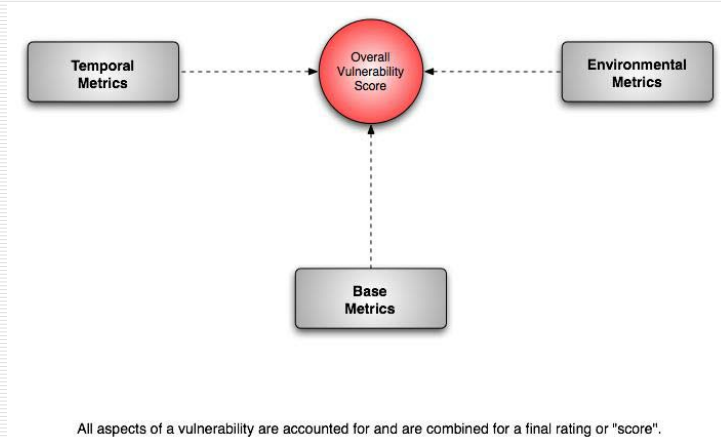
3

Scope

- ❑ "Common Vulnerability Scoring System (CVSS)"
 - Provides a way to evaluate vulnerabilities with a composite score representing overall severity and risk presented by a vulnerability
- ❑ Modular Approach
 - Promotes consistency; easy to use
 - Accounts for time-dependent properties
 - Adaptable for different environments
- ❑ Does not address disclosure issues
 - Refer to NIAC disclosure guidelines

4

Proposed Common Vulnerability Scoring System



April 2004 Status

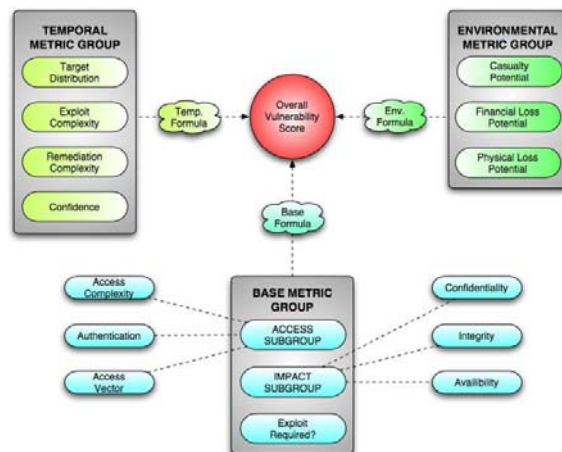
- 75% complete
 - Components, formulas drafted
 - Standard process developed
- Planning real-world testing
 - Dry runs using selected vulnerabilities
 - Adding additional industry participation in study groups for validation

Metrics

- ❑ A constituent component or characteristic of a vulnerability that can be quantitatively or qualitatively measured
- ❑ Three classes:
 - Base Metrics
 - Temporal Metrics
 - Environmental Metrics
- ❑ CVSS uses a total of 14 different metrics

7

CVSS with Metrics



Base Metrics

- ❑ Intrinsic and fundamental qualities of a vulnerability
- ❑ Do not change over time
- ❑ Do not change in different environments

Temporal Metrics

- ❑ Time-dependent characteristics
- ❑ Allow for change as the vulnerability ages

Environmental Metrics

- ❑ Characteristics that are tied to implementation and environment
- ❑ Can be different for different stakeholders

Scoring and Formulas

- ❑ Each metric is weighted and combined according to specific formulas
- ❑ One formula for each group
 - Base formula
 - Temporal formula
 - Environmental formula
- ❑ End result is a single score

Next Steps

- Testing:
 - Test with selected vulnerabilities
 - Validate with industry study groups
- Take feedback from testing and improve system
- Complete report to NIAC
- Propose draft standard
- Pending NIAC approval and industry acceptance, submit IETF draft

Timeline

- June 1, 2004: Complete real-world testing
- June 15, 2004: Complete validation
- June 30, 2004: Complete feedback and finalize CVSS
- June 30, 2004: Complete report for NIAC
- July 30, 2004: Draft proposed standard

Discussion

Questions?

ATTACHMENT D
*(Status Report on Evaluation and Enhancement of
Information Sharing and Analysis)*

NIAC Evaluation and Enhancement of Information Sharing and Analysis (EEIS)

Final Report and Proposed Recommendations

April 13, 2004

Tom Noonan
President, Chairman and CEO
Internet Security Systems, Inc.
tnoonan@iss.net

Presentation Outline

- Charter
- Methodology
- Areas for Review
- Findings – Facts
- Findings – Issues
- Proposed Recommendations
- Participants
- Requests of the NIAC

Charter

- ❑ NIAC established the Evaluation and Enhancement of Information Sharing and Analysis in April 2003
- ❑ Tasks: to analyze the current environment for information sharing and analysis across the critical industry sectors and make recommendations to the government regarding enhancements, increased effectiveness and broader influence across industry sectors

Methodology

- ❑ Leverage existing ISAC analysis/findings
- ❑ Review existing ISAC organization, funding models, membership, and challenges
- ❑ Review government information sharing organizations
- ❑ Review GAO and other reports on critical infrastructure information sharing
- ❑ Identify funding options and incentives to gain ISAC participation of all owners/operators in each sector

Areas for review

- Establish objective-focused groups:
 - Business models for sharing and analyzing information
 - Financial models for supporting information processes
 - Level of information analysis and aggregation
 - Dissemination breadth and coverage
-

5

Findings - Facts

- Significant Changes in the landscape
 - Release of HSPD 7 and 8
 - DHS has significant staffing and procedural development
 - Major ISACs have formed the ISAC Council with eight White Papers written
 - ISAC Restructurings
 - Sector Coordinators now have more formal working relationship
 - Coordination between DHS, ISAC Council and Sector Coordinators is quickening
-

6

Findings – Facts (2)

- Information Sharing has many levels
 - Strategic
 - Operational
 - Tactical
- Information Sharing has many elements:
 - Vulnerability Information
 - Exploits
 - Threats
 - Incidents
 - Best Practices
 - Early Warning System

7

Findings – Facts (3)

- Two levels of Private Sector delivery:
 - Critical Infrastructures
 - Non-Aligned Businesses
- Cross-Sector Operations between ISACs have begun on their own initiative
- ISAC Operations are communicating with DHS and their lead Agencies
- ISACs are at differing levels of maturity

8

Findings – Issues

- Information Sharing is clearly needed and Must be More Effective
 - Definitions are necessary
 - i.e. ISAC; Critical Infrastructure
 - Roles need to be more clearly defined (i.e. Sector Coordinators to ISACs and to Government)
- Various Business Model Frameworks
 - Associations
 - Government-centered
 - Market-driven

9

Findings – Issues (2)

- ISACs can provide unique sector analysis and research
 - Private Sector Owner/operators understand their unique operational problems
 - Private Sector analysis grows with trust and communication – focused primarily on Sector vulnerabilities (operational)
 - Able to provide more than just raw data – finished products – must understand Government requirements for analytical products

10

Suggested ISAC Maturity Model

Maturity >> Dimension	Level 1 Framework and Policies Established	Level 2 Procedures Developed	Level 3 Procedures for Communications and Responses Implemented	Level 4 Procedures and Responses Tested	Level 5 Procedures, Communications and Responses are Integrated Cross-Sector
Vulnerability Analysis	Identified	Defined	Distributed – Primarily Alerting	Impact Advice and Mitigations Available	Trend Analysis and Cross-Sector Integration
Threat Analysis	Identified	Defined	Distributed – Primarily Alerting	Impact Advice and Mitigations Available	Trend Analysis and Cross-Sector Integration
Cross-Sector Coordination	None	Some	Moderate – 30% to 50% of Sector Participation	Majority of Sector Participates	Cross-Sector Integration
Data Availability – real time flow	Little Except Vendor-Specific	Some	Can Be Collected From Sector and Vendors	Readily Available	Standard Repository and Analysis Available
Response Time	Uncertain	Key Enterprises Can Prevent or Diminish Impacts	Most Sectors can Diminish Impacts Quickly	Most Threats Have Little or Localized Impact	Anticipates Emerging Threats

11

Proposed Recommendations

1. Adopt the following roles for ISACs and Sector Coordinators
 - The Information Sharing and Analysis Centers (ISAC) should be the central source in each sector for dissemination, sharing and communications of information on cyber, physical, and all threats, vulnerabilities and incidents in order to defend the critical infrastructure.
 - Sector Coordinators should work Policy development and sector wide vulnerability analyses for risk mitigation

12

Proposed Recommendations (1 cont)

- Joint work with the Private Sector to:
 - Further refine the Role and responsibilities of the Sector Coordinator
 - Further refine the Relationship of the Sector Coordinator to the ISAC
 - Establish criteria to determine if Critical Infrastructure (sector) or Key Asset meets the definition in the PATRIOT Act

Proposed Recommendations (cont.)

2. Enhance Private Sector ISAC Reach
 - Assist ISACs in delivering basic Alerts and Advisories to their sectors
 - Sponsor ISAC Operations and Leadership Security Clearances
 - Provide Sector Specific and Broad Based Strategic Information thus increasing ISAC value and government communication

Proposed Recommendations (cont.)

3. Incorporate the strengths of the Private Sector Analysis and Focus with the Reach and Communication for Alerting from Government in a two tier information node
 - General Alerts and information (Reach)
 - Good across all sectors
 - Provides warning and notices to Private Sector
 - Sector Specific Alerts and Analysis (Analytical)
 - Detailed information from the Government
 - ISAC Analysis Derived Specific info to the Sector, or across Sector and/or to the Government

15

Proposed Recommendations (cont.)

4. Provide for timely flow of unique Private Sector information to Government
 - Sector-specific analysis of unique data can become actionable intelligence
 - Sectors often house the only means to take action during incidents
 - Concept of Government as “supported organization”

16

Participants

- Working Group Chair:
 - Tom Noonan, Internet Security Systems, Inc
- Study Group members: ISS, Wells Fargo, EDS, Union Pacific, Inter-Con Security Systems, V-ONE, NERC, SIAC, ConocoPhillips, Cisco, Symantec, DuPont, US CoC, and IAIP

Requests of the NIAC

- Approve EEIS report
 - Discuss any changes and agree
 - Working group will make modifications as required
- Approve letter submitting report to President

ATTACHMENT E
*(Final Report and Discussion on Government
Intervention/Best Practices for Enhancing Security of
Critical Infrastructure Industries)*

Best Practices for Government Intervention to Enhance Security of National Critical Infrastructures

NIAC Working Group Final Report

Ms. Karen Katen,
Executive Vice-President,
Pfizer Inc.

April 13th, 2004

1

Presentation Outline

- Charter
- Methodology
- Proposed Recommendations
- Requests of the NIAC

2

Charter

- Conduct a study to assess the impact of focused regulation on the security posture of each critical infrastructure sector
- Raise awareness of the scope of regulation and other tools to improve security and mitigate risks and vulnerabilities in each critical infrastructure sector
- Identify the most effective drivers of security improvement in each sector

Recommendations address:

- Understanding how sectors are operating
- How to interact with industry
- Defining the scope of discussions with sectors
- Adopting best practices in market intervention

Methodology

- ❑ Surveyed NIAC members for views on benefits of regulation and government intervention
- ❑ Conducted extensive interviews across multiples industries to shape framework
- ❑ Worked with NIAC teams to test and validate findings in four designated sectors: chemicals, financial services, information technology, and water
- ❑ Shared and discussed broadly with multiple industry stakeholders
- ❑ Submitted final report to NIAC Members

5

Proposed recommendation: Industry dynamics

- ❑ Harness market forces
- ❑ Interact with industry sectors at the appropriate level
- ❑ Assess existing sector and organization responses

6

Proposed recommendation: Need for intervention

- Consider both the strength of market response and the impact of failure
- Three guiding questions
 - Will market forces work over time?
 - Can sector provide its own solution?
 - Can regulation be applied successfully

7

Proposed recommendation: Scope of discussions

- Eight “filters” for assessing response
 - Are there network interdependencies?
 - Does security drive customer switching?
 - Is voluntary sector activity occurring?
 - Can the sector exert peer pressure?
 - Do attacks occur frequently?
 - Could attacks cause catastrophic injury or major economic damage?
 - Is industry profitable enough to invest?
 - Is there sufficient expertise to execute a plan?

8

Proposed recommendation: Intervention best practices

- Develop plans in concert with industry
- Mandate outcomes rather than specific actions
- Ensure alignment between Federal, State, and Local regulations
- Evaluate all new and existing rules through a “security filter”
- Incorporate flexibility or sunset provisions
- Recognize that funding may be necessary to fulfill government mandates


9

Requests of the NIAC

- Approve “Best Practices” report
 - Discuss any changes and agree
 - Working group will make modifications as required
- Approve letter submitting report to President

10

ATTACHMENT F
(NSTAC Briefing Materials)




NSTAC Subordinate Groups

For the NSTAC Cycle XXVII (May 1, 2003 – May 19, 2004), the NSTAC has eight task forces and working groups

- 1 Financial Services Task Force (FSTF)
- 2 Satellite Task Force (STF)
- 3 Operations, Administration, Maintenance, and Provisioning (OAM&P) Working Group
- 4 Trusted Access Task Force (TATF)
- 5 Legislative and Regulatory Task Force (LRTF)
- 6 NSTAC Outreach Task Force (NOTF)
- 7 Research and Development Task Force (RDTF)
- 8 Cyber Scoping Group (CSG)


As of April 13, 2004

2

 **NSTAC Task Forces**

The FSTF was tasked to:

- Examine vulnerabilities related to infrastructure interdependencies between the telecommunications and financial services industries
- Analyze issues regarding network resiliency that could impact the financial services sector and, consequently the U.S. economy and the welfare of the Nation, from an NS/EP perspective



The FSTF is producing a report that:

- Advises the President on methods to ensure resilient services
- Focuses on the physical aspects of resiliency

3

 **NSTAC Task Forces**

The STF was tasked to:

- Examine the usage of commercial satellites in national security and emergency preparedness (NS/EP) missions, vulnerabilities, and mitigation techniques

The STF has:

- Coordinated with representatives from many non-NSTAC companies and Government agencies
- Completed a report that advises the President on enhancing the security of the commercial satellite infrastructure and increasing the robustness of NS/EP communications



4



NSTAC Working Groups

The OAM&P Working Group has:

- Examined the Standard on Operations, Administration, Maintenance, and Provisioning (OAM&P) Baseline Security Requirements for the Management Plane
- Sent recommendations to the President on the adoption and use of the OAM&P Telecommunications Standard by the Federal Government, adaptation of the standard by other critical infrastructures, and coordination of the standard with other standards and further development of the standard



5



NSTAC Task Forces

The TATF is tasked to:

- Examine how industry and the Government can work together to address concerns associated with implementing a national security background check program for access to key facilities

The TATF is currently:

- Examining existing background check processes in both the public and private sectors to better identify shortcomings in the current systems
- Developing criteria and guidelines for national background check processes



6

The LRTF is tasked to:

- Explore the policy landscape to identify barriers to information sharing of critical infrastructure data
- Monitor and analyze legislative and regulatory activities affecting the NS/EP community

The LRTF has recently:

- Developed recommendations to the President on barriers of information sharing under the *Critical Infrastructure Information Act of 2002*
- Completed a letter to the President on policy conflicts between agencies and sectors and inter-jurisdictional NS/EP matters



The LRTF is currently:

- Examining the issue of open-source infrastructure information

The NOTF is tasked to:

- Raise the awareness of the NSTAC across the Federal Government, Industry, and academic and research communities
- Solicit feedback and input on NSTAC products and outreach initiatives
- Promote the adoption of NSTAC recommendations

The NOTF has:

- Developed NSTAC outreach materials
- Arranged meetings with key government stakeholders as follow-up to NSTAC products and recommendations
- Scheduled the IES offsite meeting to be held September 15-17, 2004, at Kingsmill Resort in Williamsburg, VA



The RDTF is tasked to:

- Continue to engage those involved and/or interested in NSTAC R&D Exchanges
- Explore potential future R&D Exchange topics
- Facilitate annual R&D Exchange

The RDTF has produced:

- A proceedings document on the 2003 NSTAC R&D Exchange, and formed actionable plans to address the findings
- An NS/EP definition white paper



The RDTF is currently:

- Examining the development of a pilot testbed for NS/EP research and development purposes
- Planning the 2004 R&D Exchange for October 28-29, 2004, at the Naval Postgraduate School in Monterey, California

The Cyber Scoping Group is tasked to:

- Focus and prioritize the issues associated with cyber-related infrastructure interdependencies

The Scoping Group may examine:

- Voice over Internet Protocol (VoIP) and network convergence issues
- Software quality
- Cyber attack vulnerabilities
- Cyber issues associated with infrastructure interdependencies





Wednesday, May 19, 2004

U.S Chamber of Commerce

- 8:00 a.m.-8:45 a.m. Executive Breakfast – Herman Lay Room**
Speaker – Governor James S. Gilmore III (confirmed)
- 9:00 a.m.-11:45 a.m. Business Session – Hall of Flags**
Targeted Speakers Include – Mr. Robert Liscouski,
Representative Christopher Cox (R-CA), Representative
Joe Barton (R-TX), Mr. John Gordon, Mr. Joseph J. Grano,
Gen. Patrick Hughes, and Secretary Colin Powell
- 12:00 p.m.-12:45 p.m. Executive Lunch – Herman Lay Room**
Speaker – Chairman Michael Powell, FCC (confirmed)
- 1:00 p.m.-3:30 p.m. Executive Session – Hall of Flags**
Includes Remarks By NSTAC Principals and Government
VIPs, Discussion of Issues for NSTAC Consideration for
the Next Cycle, and Gavel Exchange by Senior Government
Representative

