

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING

Tuesday, July 13, 2004
11:30a.m. – 2:30 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;
- Robert P. Liscouski*, Assistant Secretary for Infrastructure Protection, Department of Homeland Security;
- Frances Fragos Townsend*, Assistant to the President and Homeland Security Advisor, Homeland Security Council;
- Erle A Nye*, Chairman of the Board TXU Corp; Chairman, NIAC; 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 for July 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> |
| V. FINAL REPORT AND DISCUSSION ON EVALUATION AND ENHANCEMENT OF INFORMATION SHARING AND ANALYSIS | <i>Thomas E. Noonan, Chairman, President, & CEO, Internet Security Systems, Inc
NIAC Member</i> |
| VI. ADOPTION OF NIAC RECOMMENDATIONS | <i>NIAC Members</i> |
| VII. NEW INITIATIVES | <i>Chairman Nye; NIAC Members</i> |
| VIII. NEW BUSINESS | <i>Chairman Nye; NIAC Members</i> |
| IX. ADJOURNMENT | |

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON

Chairman Nye; Mr. Berkeley; Mr. Conrades

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL

Vice Chairman Chambers; Mr. Carty; Mr. Davidson; Chief Gallegos; Ms. Grayson; Ms. Marsh; Mr. Martinez; Mr. McGuinn; Mr. Noonan; Dr. Rose; Ms. Ware

NIAC MEMBERS ABSENT:

Mr. Barrett; Mr. Dunham; Gen. Edmonds; Governor Ehrlich; Mr. Hernandez; Mr. Holliday; Ms. Katen; Commissioner Kelly; Mayor Santini-Padilla; Mr. Thompson and Mr. Webb

STAFF DESIGNEES PRESENT MONITORING PROCEEDINGS:

Mr. John Puckett (for Mr. Holliday); and Ms. Deb Miller (for Ms. Katen)

STAFF DESIGNEES MONITORING PROCEEDINGS VIA CONFERENCE CALL ON BEHALF OF

ABSENT NIAC MEMBERS:

David Rose (for Mr. Barrett); Richard Staff (for Mr. Hernandez); Howard Schmidt (for Mr. Webb); James F. Snyder (for Mr. Dunham); Jonathan White (for Ms. Katen); Gen. Robert Nabors (for Gen. Edmonds); Sgt. Paul Morrell (for Commissioner Kelly)

OTHER DIGNITARIES PRESENT:

U.S. Government: Ms. Frances Fragos Townsend, 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; The Honorable Robert P. Liscouski, Assistant Secretary for Infrastructure Protection; Mr. R. James Caverly, Director, Infrastructure Coordination Division (ICD) of the Department of Homeland Security; Ms. Cheryl D. Peace, Director of Cyber Space Security for the Homeland Security Council, 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 National Infrastructure Advisory Council (NIAC). Ms. Wong welcomed Ms. Frances Fragos Townsend, Assistant to the President and Homeland Security Advisor for the Homeland Security Council, Chairman Nye, Vice Chairman Chambers, Under Secretary Libutti, Assistant 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. Ms. Wong called to order the eighth meeting of the NIAC and the third meeting of 2004.

II. ROLL CALL

Ms. Nancy Wong called the roll.

Ms. Wong stated the Council approved the Final Report and Recommendations for Best Practices for Government Intervention to Enhance the Security of National Critical Infrastructures. She said this report and other reports previously transmitted to the President would be available on the NIAC website: www.dhs.gov/niac.

She said the NIAC has four more issues to report and the Final Report and Recommendations from the Evaluation and Enhancement of Information Sharing Working Group is ready for discussion. In addition, the Council will discuss and select new issues from a list of items it would like to take into consideration for work over the next twelve months.

Ms. Wong introduced Lt. Gen. Frank Libutti, Under Secretary for Information Analysis and Infrastructure Protection of the Department of Homeland Security. She noted the Under Secretary would make opening remarks on behalf of DHS and the directorate.

III. OPENING REMARKS

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

Robert P. Liscouski, Assistant Secretary for Infrastructure Protection, Department of Homeland Security;

Frances Townsend, Assistant to the President and Homeland Security Advisor, Homeland Security Council;

Erle A. Nye, Chairman of the Board TXU Corp; Chairman, NIAC; 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 address the NIAC once again. He welcomed all NIAC members, both members present and those on the telephone. On behalf of the President, he thanked the Council for taking the time to attend and apply their expertise and wisdom to develop valuable recommendations for the reports. He said he was

continually impressed with the level of thought and analysis—one of the hallmarks of this Council. He said he looked forward to seeing this continue as the Council addresses a new range of challenges within DHS and for the United States. Under Secretary Libutti stated two key issues addressed at the April meeting were 1.) developing the National Infrastructure Protection Plan (NIPP) in accordance with the Homeland Security Presidential Directive 7 (HSPD-7); and 2.) finalizing the National Response Plan (NRP). Versions of these two documents will be distributed to the Council. He said the Department anticipates the Council's insights and contributions and appreciates the engagement and commitment displayed to work on these issues in this critical time. Additionally, the Under Secretary appreciated the focus on public-private partnership—critical to protecting national infrastructure.

Under Secretary Libutti then said that it was his distinct pleasure to introduce a distinguished guest, Ms. Frances Fragos Townsend. She assumed the position of Assistant to the President and Homeland Security Advisor, Homeland Security Council at the end of May 2004 and is a respected and trusted advisor to the President. In addition to her duties of reporting to the President, she continues to serve on the National Security Council staff. Ms. Townsend has a distinguished public service career beginning with her service as Assistant District Attorney in Brooklyn, New York. She then went on to hold various high level positions over a thirteen year tenure at the Department of Justice. Her focus then was national security—intelligence, policy, and international law. Ms. Townsend was ultimately named Counsel to the Attorney General for Intelligence Policy. Prior to joining the White House, she served as the Assistant Commandant for Intelligence for the United States Coast Guard. Under Secretary Libutti said she is a dear friend and consummate professional and it was his privilege to ask her to speak before the Council.

Ms. Townsend thanked Under Secretary Libutti and all those in attendance, including members on the phone. She said she did not want to take too much of the Council's time, but did want the chance to introduce herself. Having only been in her position for slightly more than a month, she was still settling in, but is looking forward to working with the Council as well as Chief Information Officers at other federal agencies in regard to NIAC recommendations across the government. Gen. John A. Gordon, her predecessor, spoke highly of the NIAC, and she looks forward to working with the Council in the future. In advance of the July 15 meeting with the President, she wanted to inform the Council that the President understands the NIAC members operate the cyber systems that run the nation's networks. Along with Secretary Ridge, the President is counting on the NIAC for advice and recommendations to improve national cyber security.

Ms. Townsend stated she understood some of the members had received the *National Intelligence Estimate Briefing on Cyber Threats to the United States Information Infrastructure* and the NIAC is using this briefing as a baseline for the outline for the Council's upcoming year agenda. The White House is extremely concerned that the rapid convergence of telecommunication information systems has created a security gap. They are worried that technological developments have not sufficiently considered information and systems security—this will be a significant challenge because of the growing number of technology trends affecting both offensive capabilities and defensive efforts in the cyber domain. Infrastructure will

continually need better protection, response, and restoration as adversaries ranging from teen virus writers to fledgling cyber terrorists or dedicated nation-states continue attacking.

Ms. Townsend said she looks forward to the Report and Recommendations on the Evaluation and Enhancement of Information Sharing and Analysis that will come out of the meeting. The NIAC is one of the most effective advisory committees the President has; the Council's tenacity, commitment, and attention to detail yields powerful results. The individuals on the NIAC all play integral roles in contributing to the final product. In closing, Ms. Townsend reiterated the President's statement saying the "cornerstone of American cyber strategy is and will remain a public-private partnership." Everyone in business knows that partnerships are very difficult. The NIAC has a very important role to play in keeping the public-private partnership healthy, balanced, and productive. Ms. Townsend thanked Chairman Nye for the invitation to address the Council and she said she anticipated seeing everyone on Thursday, July 15 at their meeting with the President. With that, she returned the floor back to Under Secretary Libutti, who thanked Ms. Townsend and then introduced the Assistant Secretary for Infrastructure Protection Robert Liscouski.

Assistant Secretary Liscouski also thanked Ms. Townsend for her comments and said she really underscored the services the Council provides to both the President and to the Department of Homeland Security for information security guidance and implementing the Department's strategies. He said that he wanted to address some initiatives that were covered during the April meeting.

HSPD-7 was briefed to the Council in April and an update touching on the NIPP would be presented at the July 15 meeting. Additionally, this addresses some issues emerging over the summer and next several months dealing with specific security initiatives. Assistant Secretary Liscouski also recognized the Council for the valuable input they have provided to DHS as Infrastructure Protection capabilities are being ramped up. In addition to the very well represented cyber components, highly relevant cross-sector implications and interdependencies have been identified.

Many of the ongoing study group efforts, especially the Internet Hardening Study Group and the Prioritization of Cyber Vulnerabilities are of great interest, and DHS is anxiously awaiting their culmination. Assistant Secretary Liscouski then thanked the Council for its efforts and Chairman Nye for his leadership.

Assistant Secretary Liscouski then turned the floor back to Under Secretary Libutti who introduced the Chairman of the NIAC, Mr. Erle A. Nye.

Chairman Nye thanked Under Secretary Libutti and welcomed everyone in attendance and thanked them for being present, including those on the phone. He thanked the Council for the dedication and commitment that they have shown. He said that from a personal standpoint, the NIAC continues to receive very positive comments and critiques of its work. As far as advisory councils go, the NIAC can take a great deal of pride in the fact that it drives toward positive results. The Chairman also expressed his appreciation for Under Secretary Libutti, Ms.

Townsend, and Assistant Secretary Liscouski for their presence and their interest in the Council's work.

As Ms. Wong mentioned earlier, the "Final Report and Recommendations for Best Practices for Government Intervention to Enhance the Security of National Critical Infrastructures" has recently been delivered to the White House, making it the third report to emerge from the NIAC. The Council has asked to receive feedback about the effectiveness and the usefulness of its work, and it was his understanding that the Council's secretariat would monitor the progress of the recommendations to provide feedback in future meetings. The Administration is working to provide additional representation in the sectors previously designated in the Final Report and Recommendation on Cross Sector Interdependencies Risk Assessment. He said representation of expertise will be pursued from the following sectors: 1) Food and Agriculture, 2) Postal and Shipping, and 3) Telecommunications. Chairman Nye said he was hopeful that there would be representation at the October meeting from these sectors.

A key agenda item for the NIAC is the selection of additional work topics for the next twelve months. Chairman Nye appreciated everyone's input into these items that will form the basis of the Council's discussion. This year, the Council has completed three reports with one more being discussed and deliberated on today. The NIAC is expected to complete the three currently open topics by the October meeting. Consequently, the energy level of the Council gives it the wherewithal to take on additional topics. Chairman Nye then asked Vice Chairman John Chambers if he had any further comments.

Vice Chairman Chambers thanked Chairman Nye and thanked the members and their staffs for all the hard work they have put in. This Council rapidly produces high-quality, very detailed reports. He said the key ingredient here is the very active involvement of Chief Executive Officers and their staffs—one without the other does not result in the same high level of effectiveness. Vice Chairman Chambers said that the upcoming proposed work items are difficult to prioritize and, as Ms. Townsend said earlier, these kinds of partnerships are challenging and time-consuming for both the public and private participants. He emphasized the importance of the government being direct with the Council around areas that can really be valuable to build recommendations. He echoed the Chairman's earlier statement that it is imperative the NIAC be sure to add value to these topics. The President will likely help prioritize and select new topics at the July 15 meeting, and he asked the group to be flexible. Vice Chairman Chambers then opened the floor back to Chairman Nye who thanked him and asked former Chairman Richard K. Davidson if he had any comments.

Mr. Davidson said he was thankful that there are two leaders like Chairman Nye and Vice Chairman Chambers who are willing to take on the leadership role of the NIAC.

Chairman Nye thanked Mr. Davidson and said it was important to receive status reports on all the open items. Chairman Nye turned the floor over to Mr. George Conrades to discuss the effort of his study group's report on Hardening of the Internet.

IV. STATUS REPORTS ON PENDING INITIATIVES:

A. HARDENING THE INTERNET

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

Hardening the Internet

Mr. Conrades thanked Chairman Nye and said he was delighted to present this brief status report on the Internet Hardening Working Group. Mr. Conrades said the study group was aiming to propose recommendations at the October NIAC meeting. He was pleased to report that the study group has featured expert and active representatives from the Internet and related security communities. Mr. Conrades then turned the floor over to Mr. Andy Ellis, the Director of Information Security at Akamai Technologies, to discuss the study group's recent activities and upcoming goals.

Mr. Ellis thanked Mr. Conrades and said he intended to review the study group's history, the challenges lying before it, and to provide an overview of proposed recommendations. This study group was chartered last July after President Bush asked the NIAC to identify the best practices for hardening the Internet based on findings from earlier study groups. The study group began by evaluating the work of many other organizations including the National Security Telecommunications Advisory Committee (NSTAC), the National Cyber Security Partnership (NCSP), the Computer Emergency Response Team (CERT), as well as many other organizations.

The challenge of defending the Internet lies in two areas: 1) core infrastructure and 2) the customer environment. Core infrastructures are routers and name servers which are the Internet's backbone and true heart. The customer environment is comprised of personal computers, enterprise networks, and e-business servers that connect to the network and support the nation's businesses and economy. The study group discovered a wealth of pre-existing best practice guidelines that, if implemented, could significantly strengthen the Internet. Recommendations will focus on implementing accepted best practices and developing new technology recommendations to improve the underlying environment. The study group recognizes that the private sector controls much of the infrastructure and environment; policy recommendations will reflect what the government does well to encourage good behavior in the private sector. This includes convening groups of experts such as the NIAC, using the bully pulpit to educate and motivate citizens in the private sector, sponsoring research, and catalyzing private development of best practices and standards. The methodology began by creating two study groups to look at each of these target areas and share information through weekly teleconferences to assess the state of best practices and begin putting together potential recommendations. As Mr. Conrades mentioned, there has been a wealth of study group participation from both private sector as well as public bodies.

The study sees the challenges as two-fold. The first challenge is the ease of distributed denial of service attacks (DDoS). DDoS attacks leverage idle resources on equally compromised machines to flood critical systems with seemingly valid traffic. The challenge in dealing with these attacks lies not only in technologies and practices to better protect these critical systems, but also with removing attackers' capability to use false or drone networks—machines that should not have been under control in the first place. The second challenge stems from security

protocols the core infrastructure uses to communicate with itself and to create a shared platform. These protocols were not designed to ensure that only legitimate infrastructure could send controlled messages nor does it limit what an existing piece of infrastructure can send. There are mitigating best practices that can aid in reducing risk in this area, but it is clear that there is a need to explore more secure protocol and understand the upgrade path to infrastructures themselves.

Tasked to address these two challenges, the study group has explored different means the government might consider to improve the existing situation. Education and awareness centers around looking at ways machines on the Internet are currently protected. This is especially useful where there are known methods and practices that, if applied regularly, would significantly improve the Internet's security posture. This is done by reducing the number of systems that can be added to the networks and by protecting pieces of the core infrastructure. The second method, research stimulation, not only involves investing new technologies in the security and management space, but also examining the cost of migrating existing infrastructure to newer protocols in a more cost-effective manner. The last recommendation, empowerment, will identify more effective ways to deal with these cyber threats and ensure that the risks to them outweigh the benefits of these types of behaviors.

Within education, the study group has identified several key areas to target for potential recommendations. Educating software developers while still in academic programs on secure system design will have a long-term payoff in generating more secure systems for infrastructure in the future. Educating end-users in much the same way people are taught the perils of nicotine, alcohol, and drugs will pay off in reducing the number of infectable end systems. Many ethics organizations have created awareness education programs to date. However, outreach to end-users on the Internet has much room for improvement. Reaching out to corporations will be equally important in order to enhance awareness of securing all of their systems, not just their financially critical ones. Corporations already have vehicles in place that can be leveraged for this communication including Control Objectives for Information and related Technology (COBIT) and Sarbanes-Oxley.

When looking at areas of research funding and prioritization, it is clear that understanding how to implement good security systems is as important as - if not more important - than developing secure systems. To that end, potential recommendations will include proposals to further direct research in these areas. How to cost-effectively implement more secure protocols including operationally implementing and maintaining routing registries and easily managing route and package filtering at the edge of the internet. Continuing to advance the study group's real time analysis of the network threats in consumable fashion—providing actionable information on threats to the Internet.

Finally, there is a need for models to support business case analyses within the private sector to assist in good decision-making. This would ensure the proper funding of the necessary security activities corporations must take to secure the Internet.

One of the recurring themes from the Internet Security Provider (ISP) community is the desire to help protect the network by providing some control over traffic. There is a great deal of concern

from the ISP community about being liable for those inadvertently impacted as well as from failing to provide even greater control. Network providers seek both a safe harbor and a Good Samaritan protection to feel empowered to act in many of these cases. Additionally, there are many barriers restricting the abilities of law enforcement professionals to apprehend and prosecute cyber criminals and receive assistance from the private sector in doing so. Whether or not there is the ability to receive intelligence proactively, there are jurisdictional and statutory barriers in some areas.

The group expects to have its draft report completed within the next month and distributed for review so the draft is ready for deliberation and vote at the next NIAC Meeting.

Chairman Nye thanked Mr. Conrades and Mr. Ellis and asked if there were any questions.

Vice Chairman Chambers said he thought Mr. Conrades and the entire working group and study group are developing a very thorough answer to the President's question. He stated it is easy to underestimate the complexity of this task and wanted to encourage the study group to continue to closely examine both technical and non-technical items relating to this subject matter. Education on good security management policy is a very key point. It is usually not the technology causing the problems; it is people not adhering to the recommended policy associated with the technologies. Vice Chairman Chambers said the status report was quite thorough.

Chairman Nye thanked Vice Chairman Chambers and asked if there were any further comments or questions. There were none, and Chairman Nye introduced Mr. Martin McGuinn to brief the Council on the work of the Prioritization of Cyber Vulnerabilities study group.

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

**B. PRIORITIZATION OF CYBER
VULNERABILITIES**

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

Prioritization of Cyber Vulnerabilities

Mr. McGuinn said since the NIAC last met in April, there has been a steady stream of cyber vulnerabilities that have continued to plague networks. For example, the US-CERT provides a current activity calendar, which has reports of new server compromises, worms, and other vulnerabilities. Within his company, Mellon Financial Corporation, the security group is tracking 127 new vulnerability alerts that have been issued since April. In addition to traditional cyber attacks, new methods are also emerging. One vulnerability especially concerning the sector is the growing "phishing" trend. Phishing is an attack that tricks users into entering personal data information into a fraudulent website. The frequency of these attacks has grown from approximately 80 attacks per week in March, to 300 per week in May. Another rising trend is the use of bots for automated cyber attacks. Bot networks aggregate compromised computers, allowing them to be remotely controlled by hackers. The ability to harness this computing power and generate bot attacks greatly enhances cyber attack sophistication and threshold of damage.

As cyber vulnerabilities research continues to advance, a positive theme has emerged from the survey distributed by the Prioritization of Cyber Vulnerabilities Working Group. Some responders referred to their ability to recover using existing disaster recovery plans regardless of the outage's cause. Whether it is a cyber attack, physical issue, or user error the result can be the same—no system available. Each business needs to have a plan flexible enough to adapt and address the situation.

The status report will provide an update on what has been accomplished since the April meeting. Mr. McGuinn extended his thanks to the members of the study group and the Council for supporting these efforts.

The study group is attempting to rank the impact of potential cyber attacks on various sectors. Each task is a direct response to a question posed by President Bush at the July 2003 meeting. Mr. McGuinn then introduced Ms. Susan Vismor, Senior Vice President at Mellon Bank, to provide extended dialogue on the research.

Ms. Vismor thanked Mr. McGuinn and began by asserting the first key question on the survey. What are the top three uses of information systems and what revenue or efficiencies does the system support? The study group also incorporated questions about national security, emergency preparedness, and interdependencies with other critical infrastructures into the survey. The survey examined the implications that sector-specific vulnerabilities associated with various types of cyber attacks. For example, participants were asked about the impact on their firms if information systems had false information deliberately inserted into them. By compiling responses and translating percentages, the study group is able to look across sectors to determine which sector would potentially be most impacted by specific kinds of attacks. To extend this example, a subsequent question asks how long it would take for their companies to protect their systems if this information services critical systems. If a sector cannot detect the attack that impacts it most, the problem is exacerbated.

Ms. Vismor continued by summarizing the study group's actions to date. In April, the survey was finalized and distributed to a sample group representing each critical infrastructure sector. These surveys were returned to the study group by the end of May and follow-up correspondence was provided to encourage responses. The study group is currently analyzing the collected data. Due to participants' concerns about data confidentiality, the study group requested that DHS host a closed meeting to discuss the survey's results. This meeting will be held in October. Ms. Vismor thanked DHS for accommodating this request.

Ms. Vismor provided an update on the survey of responses that were received from the various sectors. As of the meeting, the study group had received responses from the following sectors:

- Telecommunications
- Transportation
- Postal and Parcel Shipping
- Banking and Finance
- Public Health and Health Care
- Water and
- Energy.

Sectors not responding include:

- ❑ Information Technology
- ❑ Agriculture and Food
- ❑ Defense Industrial Base
- ❑ Chemical and
- ❑ Government Emergency Services

Ms. Vismor stated that two additional sectors have indicated that they will respond within a few weeks. Prior to the final presentation of survey results in October, the study group will continue to collect any additional data, especially from currently unresponsive sectors. The Council's support in pushing for survey responses would be much appreciated. Thus far, banking and finance, energy, and public health and health care sectors are the most willing to participate in the survey. These sectors recognize the value in confronting the survey's thought provoking issues and questions. Responding sectors gauge this effort as an opportunity to advance their respective disaster recovery planning plans.

One of the survey's fundamental questions called for respondents to indicate which sector they most depended on. Ms. Vismor listed the current rankings and said they will be updated to include any late survey responses. Ranked from one to eleven, they are as follows:

1. Telecommunications
2. Energy
3. Banking
4. Postal and Parcel Shipping
5. Transportation
6. Water
7. Agriculture and Food
8. Emergency Medical Services
9. Chemical
10. Public Health and Healthcare
11. Information Technology

These results are very similar to the findings of the Cross-Sector Interdependency Study Group. In both cases, Telecommunications was undisputedly ranked as most important with Energy ranked second.

Ms. Vismor said that based on agreements to respect respondents' confidentiality, the study group came to the following non-sensitive, preliminary observations

1. Privacy was the top concern for many participants
2. Typical disaster planning respondents felt that answers to questions would vary greatly depending on the nature of the disaster
3. As Mr. McGuinn noted, a number of respondents refer to their current capabilities for disaster recovery. A transition to an auxiliary system is generally not as efficient as the primary system. It does, however, provide protection against a total outage. In some cases, this redundancy's cost did not represent an additional cost; business recovery burdens are mitigated through a company's existing disaster recovery program

4. One of the survey's questions asked about the cost to restore or replace systems rendered useless by a cyber attack-- respondents seemed more willing to reconstruct a system than to replace it
5. Systems at the heart of some of the sectors may be proprietary or from third-party vendors. This makes an attack more complicated than an attack against common desktop products

Ms. Vismor's said the study group's next step is to incorporate any additional late surveys to the analysis. The study group will accept late responses and will finalize the analysis for presentation at the October meeting. Ms. Vismor thanked the Council and concluded the status report.

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

Vice Chairman Chambers said he viewed these as excellent starts and he emphasized that the types and complexities of attacks are ongoing concerns. In addition to phishing or bots, the Trojan horse is a major approach to data distribution, substitution, destruction, and denial-of-service attacks. These attacks will continue to become more complex. The way this issue is being handled makes more sense than some of the earlier theoretical approaches. Vice Chairman Chambers congratulated the group on their progress thus far, but stressed this topic's difficulties.

Chairman Nye concurred and asked Vice Chairman Chambers to proceed with the status report on the Common Vulnerability Scoring System.

**C. COMMON VULNERABILITY SCORING
SYSTEM**

Vice Chairman Chambers; and John W. Thompson, Chairman & CEO, Symantec Corporation; NIAC Member

Common Vulnerability Scoring System

Vice Chairman Chambers thanked Chairman Nye and stated the Vulnerability Disclosure Study Group's work was published six months ago but the lone remaining task was to set up a common vulnerability scoring system dependent upon a number of variables. There was a status update in April and the final presentation should be ready by the October meeting. Vice Chairman Chambers asked Ken Watson to present for himself and Mr. Thompson.

Mr. Watson thanked Vice Chairman Chambers and said the study group has made steady progress this past quarter and is ready for NIAC members and other to assist in the final testing validation and approval scoring system. He said he would provide the Council with a brief status update and then demonstrate a visual representation of how the system could be used to score three different vulnerabilities.

He stated the system was complete with only final validation testing and approval remaining. The study group is currently engaged in extensive in-house testing. Mr. Watson extended his appreciation for extra effort by Symantec, eBay, Qualys, Cisco, and DHS. He added that if

anyone would like to participate in the next phase, the study group will be asking for technical points of contact in NIAC members' companies and organizations at the end of this presentation to be part of the study group. Both Qualys and Symantec have committed to using the final system developed by the study group. This is the first step to making a common scoring system.

The technical component of the study group's work continues to improve the system—the steps are simpler than they were at the April meeting, but they still follow the same principle:

- The system starts with a base score for vulnerability that does not change over time or as a result of being in a different environment. The base score can stand alone as a measure of vulnerability's relative significance
- Time-sensitive modifiers—the existence of an exploit or a patch, are added
- Individual organizations apply metrics to the score in their specific environment to arrive at a final score. The final score is only valid for a point in time and a specific environment. However, it should be very useful to executives and operators who are prioritizing actions to resolve vulnerabilities

The study group has structured formulas to give the base score the greatest weight of all three. Within the base score, the vulnerability's potential impact is also weighted more than other factors. Within the base score, impact to confidentiality, integrity, and availability carry the greatest weight.

- Confidentiality refers to limiting access only to authorized users. An impact on confidentiality would be a vulnerability that allowed access to sensitive critical infrastructure information;
- Integrity is the guaranteed access to trustworthy data. A vulnerability that impacted integrity would allow systems to change information;
- Availability means that the information needed is accessible by information resources. If it prevented the flow of traffic, it would impact availability.

As the study group has previously mentioned, the temporal score can be affected by factors such as whether actual antidote code exists or whether there is a vendor patch or other workarounds.

Environmental factors affect the potential for collateral damage including financial, physical, or human casualties. The environmental calculus measures the scope of infected systems-- how widespread the use of affected systems is or how rich the provider environment is.

The study group is currently conducting stress testing and is ready for wider industry and government participation. This next round of testing will further simplify realizing the goal of a common vulnerability scoring system. Currently, the study group is putting the module in Microsoft Excel spreadsheet format. Mr. Watson said this format can be converted to any recommended form. The revised timeline includes time for NIAC members and others to test and validate the system. It also provides time to provide the final report to the NIAC to review it for the October meeting.

Mr. Watson walked the Council through three examples of the Common Vulnerability Scoring System and highlighted some of the ways formulas raise or lower the score. The Common Vulnerability Scoring System is designed to produce a score between zero and ten, with ten

signifying the most significant or impactful vulnerability. He reminded the NIAC the system rates vulnerabilities, not threats. Typical threats that exploit the vulnerabilities were shown in the second row of the module. Using three vulnerabilities as examples, Mr. Watson showed the Council how the base and current temporal scores are derived and demonstrated how differences in specific environments can affect the final score.

The first example is a Microsoft Outlook vulnerability exploited by the Netsky B virus. Even though the vulnerability can allow complete compromise of confidentiality, integrity and availability, access complexity is rated high, as the user has to enable it by downloading and opening a tainted email. High access complexity lowers the score.

The temporal score was based on the fact that functional exploit code is available on the Internet, keeping the score high. However, there is a complete solution—a patch provided by Microsoft—which lowers the score.

The environmental score is dependent on specific local factors. Collateral damage would include potential for significant financial losses, potential physical damage or human casualties. Target distribution reflects how highly populated an affected system is used in a specific environment. If there is no target distribution, the final score is zero. No environmental modifiers had been provided for the demonstration because the study group did not select a hypothetical environment.

The second vulnerability was exploited by the Sasser Worm, which completely compromised confidentiality, integrity and availability. The key difference between the Sasser Worm and the Netsky B virus is low access complexity. If a system has this bug, it is always exploitable and requires no user interaction.

Temporal score highly rates exploitability--there is not only an exploit code for every situation, but the exploit is actively delivered via mobile autonomous agent, in this case the Sasser Worm.

The recently announced Border Gateway Protocol (BGP) vulnerability highly rates access complexity as an attacker needs specialized access to BGP machines running that is part of a group of BGP systems. This increases access complexity and lowers the score. The vulnerability cannot cause a compromise of confidentiality or integrity, as the worse case scenario is a denial of service attack. Temporal scores reflect the fact that there is enough information about a vulnerability for a hacker to build proof of content exploits, but there is no publicly available exploit code available, thus lowering the score. Several vendors have released patches, but because this affects multiple vendors, the moderate score does not reflect a complete solution—that will only apply when all affected vendors release patches.

Mr. Watson concluded by inviting NIAC members and their companies or other organizations to help the study group simplify, validate, and ensure the system is useful not only for coordinators or vendors working with vulnerabilities, but also to end users. Mr. Watson concluded his remarks and thanked the Council.

Chairman Nye thanked Vice Chairman Chambers and Mr. Watson and asked if there were any questions or comments. He was curious if there was a code for the use of this technique. He also asked if there was a set of instructions or term definitions.

Mr. Watson indicated that there is an instruction manual. The system itself is on Microsoft Excel but can be changed to whatever is needed. This will be provided to anyone volunteering to help further test the system.

Vice Chairman Chambers said direct email to Mr. Watson would be appropriate. The study group can handle all 25 NIAC members, two of who have already helped, and would take a subset of the total group for any volunteers.

Chairman Nye said everyone should provide someone to work on this and encouraged the NIAC to do so. He said the status report represented good work and he again thanked Vice Chairman Chambers and Mr. Watson for their presentation. He asked if there were any other questions or comments.

No comments were offered and Chairman Nye said he appreciated these status reports. He asserted the working groups are making excellent progress on important, high quality work.

The Chairman introduced Mr. Tom Noonan for the final discussion on the Evaluation and Enhancement of Information Sharing and Analysis.

V.	FINAL REPORT AND DISCUSSION ON EVALUATION AND ENHANCEMENT OF INFORMATION SHARING AND ANALYSIS	<i>Thomas E. Noonan, Chairman, President, & CEO, Internet Security Systems, Inc NIAC Member</i>
-----------	--	---

Mr. Noonan thanked Chairman Nye and said he would be providing his report by telephone with Mr. Peter Allor from Internet Security Systems present in Washington assisting with the discussion and presentation. Mr. Noonan again thanked Chairman Nye and Vice Chairman Chambers and said he was honored to be presenting to the NIAC. He said he was happy to provide the Council with this final report and discussion on the complex but strategically important issue of information sharing and analysis within critical infrastructure. Mr. Noonan thanked the members of both the study group saying they were a dedicated group who had driven towards clear, actionable conclusions and recommendations.

He stated he had provided a detailed review of the working group's interim report on the Evaluation and Enhancement of Information Sharing and Analysis at the April NIAC meeting. He specifically focused on findings in the areas of:

- ❑ Business models for sharing and analyzing industry-wide information; and
- ❑ Financial models supporting the information sharing process, the level of information analysis and aggregation within industry, and the dissemination, breadth, coverage, and ultimately, the actionability of the distributed information.

The group has reviewed many Information Sharing and Analysis models and analyzed an extensive amount of reports published by the individual Information Sharing and Analysis

Centers (ISACs), as well as work that other groups have undertaken, including DHS, CERT, and others.

Out of necessity, the study group has curtailed the review of materials to complete the report. The first component curtailed was the evaluation of federal funding of private sector ISACs. Additionally, work related to the degree of federal aid to establish supporting infrastructure that provides secure private sector to private sector exchanges remains under discussion and evaluation with DHS.

Mr. Noonan said the agenda would begin with a status report to include changes made since the April meeting, including edits from the study group, minor report format changes, and DHS edits. He said he would like to advance recommendations for next steps including a review and edits by working group members. As of the July meeting, the NIAC Secretariat at DHS has completed and reviewed edits. The report was delivered June 30 to the NIAC and should soon be available to the members. He said he and the working group looked forward to discussions around the final report.

In terms of next steps, the working group wished to incorporate all input from a full NIAC review and prepare and submit a NIAC-approved letter for the President. The study group is in the final stages of drafting the letter for the Chairman and Vice Chairman of the NIAC to submit to the President, contingent upon the Council's approval. The final draft letter will be prepared by July 20, 2004. The study group is asking for discussion or any additional inputs to be provided no later than July 30, with the expectation that a final report has been completed by August 1 with an expectation of delivery on August 10.

Mr. Noonan said the working group seeks discussion around this report from the NIAC and a recommendation that the report and its recommendations for the Evaluation and Enhancement of Information Sharing and Analysis be approved for submission to the President. Mr. Noonan said he sincerely appreciated all the support provided on many occasions both within this group and within industry working groups. The nature of the threats the United States faces today is becoming increasingly complex and important. The ability to effectively preempt these threats is largely dependent upon being able to effectively and efficiently detect, analyze, and communicate the presence of these threats so they can be appropriately addressed. Information sharing lies at the center of this effort. He asked that the NIAC members please make final comments today or no later than July 30 so that the final report can be delivered on August 10. He then asked Mr. Peter Allor to open up discussion to address any questions or discussion. Mr. Noonan thanked the NIAC and turned the floor over to Mr. Allor.

Mr. Allor said he would answer the questions of the NIAC and asked if the Council had a chance to read the report.

Mr. Alfred Berkeley, III asked if the working group was comfortable with the feeling that any shared information is shared at the appropriate confidentiality levels.

Mr. Noonan said there is little consistency in this area from industry to industry. There is, however, a convergence of practices. A capabilities maturity model--one of the outputs and

recommendations of the Evaluation and Enhancement of Information Sharing and Analysis Report also catalyzes these practices. From a security perspective, this area--information between private sector organizations--for which operational infrastructure does not really exist.

Mr. Allor added that maturity points vary by sector. The operations discussions between the ISACs, DHS, and sector coordinators have enabled the ISACs to now have daily communication and information sharing. This interaction is not at the fullest maturity level, but the degree of change has accelerated substantially in the last six months, especially in comparison with its level two years ago.

**VI. ADOPTION OF NIAC
RECOMMENDATIONS**

NIAC Members

Chairman Nye thanked Mr. Noonan and Mr. Allor and asked if there were any more comments or questions. He said he intended to bring this to a formal decision and seek the approval of the Council subject to any comments over the next thirty days--the standard protocol. He said he would entertain a motion to approve this report as it has been presented subject to any changes made as a result of comments received within the next thirty days.

Mr. Berkeley moved for an approval and it was seconded.

Chairman Nye thanked Mr. Berkeley and asked if there was any further discussion.

Ms. Marilyn Ware thanked the study group for its very important, well-constructed work. This is a difficult effort considering the changing landscapes that Mr. Noonan and Mr. Allor alluded to.

Chairman Nye thanked Ms. Ware and asked if there were any further questions or comments. There were none and the Chairman called for a voice vote. Hearing no opposition, Chairman Nye said the report was approved unanimously subject to comments that may be received within the next thirty days. He again thanked Mr. Noonan, Mr. Allor, and all those contributing to the working and study groups. He said he thought the report would be very well received.

VII. NEW INITIATIVES

Chairman Nye; NIAC Members

Chairman Nye wanted to discuss some other items for informational and explanatory purposes. The National Response Plan (NRP) was provided to Council members earlier this year for review for comments back to DHS. The NIAC had a relatively brief window to turn the document around for comments. Some members expressed the desire to form a special working group addressing a coordinated response on behalf of the Council. Chairman Nye said it was impossible to organize this in time to report back to DHS. He knows that everyone understands the critical importance some of these matters hold and it is imperative that the Council moves forward as quickly as possible. The Chairman stated he appreciated each individual's diligence in reviewing and providing feedback on the NRP. It does raise the issue of how the NIAC responds to some of these rapid turnaround matters. There is another similar situation arising with respect to the National Infrastructure Protection Plan (NIPP). The NIPP will be released in

draft form to the members of the Council later this month for comments. The projected turnaround will be ten days to two weeks. He said that this will be a somewhat difficult undertaking considering the summer vacation season, but he still wanted members to make every effort to comment.

Vice Chairman Chambers said the short window for turnaround might not be conducive to quickly producing NIPP comments from a NIAC working group. He recommended individual response to a central point within DHS.

Chairman Nye concurred and thanked Vice Chairman Chambers. He encouraged members to take this matter seriously using all knowledge and information available to them. He asked if Under Secretary Libutti or Assistant Secretary Liscouski had any comments.

The Under Secretary said ideally, if there were sufficient time to review documents, he would prefer it go to the Council for review. However, under the circumstances, the best approach probably follows guidance from Chairman Nye, supported by Assistant Secretary Liscouski and himself. He said the door to the NIAC leadership should not be closed but the bottom line is to return the comments to the Information Analysis/Infrastructure Protection Directorate (IAIP) with the Assistant Secretary for Infrastructure Protection as the lead. Under Secretary Libutti emphasized collegiality—he said he was always open to suggestions from the NIAC leadership.

Chairman Nye thanked the Under Secretary and said he thought his point was well made. He said the Council does want to share comments within the NIAC to stimulate any crosscutting issues that may need to be addressed at a later date. He trusted these were not the last drafts of the NRP and NIPP and indicated they will be improved as time goes on.

Chairman Nye said the Council is making progress on its initial work and is able to consider additional work areas; many of the members have provided comments and suggestions. The NIAC has also received White House input and would likely receive additional comments from the President at the July 15 meeting.

Chairman Nye said that he and Vice Chairman Chambers reviewed these suggestions and tried to formulate six potential topics for the Council's consideration. These are not the only matters the NIAC might undertake, but these are the distilled priorities from those suggested topics. Additional suggestions are archived in a working list and may be brought forward in the future. It may be preferable to narrow these suggestions to perhaps only three or four. The council should be flexible enough to allow for additional topics the President may bring forward. Clearly, the NIAC would prioritize around his additional topics. Furthermore, the Council will likely have additional members by the October meeting and it may need to address issues these new members raise. Vice Chairman Chambers agreed to lead a discussion on these initiatives. The NIAC will need to prioritize two or three undertakings and gather suggestions as to the leadership that might handle these items. Chairman Nye said if there were no questions, he would turn the program to Vice Chairman Chambers.

Vice Chairman Chambers thanked Chairman Nye and echoed his words, saying they examined multiple inputs from all the working groups with special emphasis obviously placed on White

House areas of interest. These items were reviewed with an eye toward potential policy recommendations. Another issue the Council seeks to avoid is duplication of effort—the NIAC should not expend resources to research items already being addressed by other organizations. Vice Chairman Chambers said he would outline each topic and create an environment for discussion, and then refer back to the Chairman to lead prioritization of tasks by vote.

1. The first item, originally proposed by the White House and NIAC members, is whether or not the way critical infrastructures interact with the intelligence community can be improved. The intelligence community selectively works with critical infrastructures and agencies on specific issues. These processes are primarily based on past experiences and existing relationships such as: the manner in which the Council has dealt with challenges in the past; how challenges are currently approached; or will be addressed in the future. Without better coordination and rapid evolution there could be some rough challenges ahead. With the creation of DHS and growing network interdependencies, questions about critical infrastructures in both the physical and cyber spaces will drive the thought process around these six questions:
 - ❑ What kind of intelligence is meaningful to critical infrastructure owners and operators?
 - ❑ What is the appropriate role of critical infrastructure representatives in the intelligence cycle?
 - ❑ What are the key intelligence processes and terminologies? Critical infrastructure owners and operators must understand these to clearly exchange information during challenging times and to cohesively build a response together.
 - ❑ What constitutes a threat and how is it communicated to the critical infrastructure environment?
 - ❑ Does it make sense to place industry representatives at intelligence agencies or DHS?
 - ❑ Are new processes and professional disciplines needed within the critical infrastructure sectors to interact with the intelligence communities?

Vice Chairman Chambers said it might also be wise to anticipate questions generated by these items if they end up being selected. A potential starting point, for example, could be an intelligence community briefing for the NIAC.

Vice Chairman Chambers asked if there were any questions or comments.

Chairman Nye said he thought this was an excellent proposal.

Vice Chairman Chambers asked Mr. Conrades what his thoughts and comments on the issues were.

Mr. Conrades responded, that one of the challenges he faces is his lack of understanding of the intelligence community and processes. He said this lack of understanding makes it difficult to estimate the scope and depth of what the NIAC would be doing if it undertakes the initiative.

Under Secretary Libutti said that by working through Assistant Secretary Liscouski, an intelligence briefing could be arranged. Maj. Gen. Patrick M. Hughes, Assistant Secretary for Information Analysis, may be available to educate, instruct, and provide comments that are germane to the subject. Under Secretary Libutti thought the outline is superb and as a response to Mr. Conrades' point, everyone would benefit from listening to Gen. Hughes. He asked the

Meeting Minutes for July 13, 2004 Meeting

Page 21

NIAC to work this through Assistant Secretary Liscouski. He asked the Assistant Secretary if this was acceptable.

The Assistant Secretary said it was.

Under Secretary Libutti said any resource he has would be made available to the NIAC at any time.

Mr. Conrades said that all members have their areas of interest and domain expertise but was unsure of his participation given that he did not have a strong understanding how the intelligence community actually operates relative to the various sectors.

Under Secretary Libutti said it was a great question and that DHS faces many challenges as the newest members of the National Intelligence Community in its effort to be fully mature and aggressive.

Chairman Nye asked if there were any other comments by the members. He said that he thought Mr. Conrades made the point that there may be trouble obtaining leadership if there is not a strong knowledge base on the NIAC. He asked Vice Chairman Chambers his thoughts.

Vice Chairman Chambers felt the NIAC should consider this topic. This really depends upon DHS and other key government organizations deciding whether or not briefing the Council would add value here. If so, a classified briefing is necessary. Additionally, the Council members need to have the proper clearance. If somebody does not take this responsibility or if there are architectural barriers to the problem, there could be negative consequences. The NIAC's government partners are best prepared to determine the optimal way to handle this.

Assistant Secretary Liscouski underscored Vice Chairman Chambers' comments, saying this is supported from a government perspective. Ensuring the right partnerships with the private sector is crucial and the Assistant Secretary would provide support to the Council to help them grasp what intelligence communities can do for them.

Chairman Nye mentioned security clearances and said he would like members of the Council to seek clearances, hopefully prior to the October meeting. He said he knew these take time, but felt that the Council needs to have some clearance to work in classified areas.

Assistant Secretary Liscouski said he could provide the support to ensure the clearance process is initiated and is rapidly accelerated.

Vice Chairman Chambers thanked Assistant Secretary Liscouski and asked Chairman Nye if he could proceed to the second topic.

Chairman Nye said yes.

2. Vice Chairman Chambers said the second topic also came from the White House and from the suggestion of NIAC members. The NIAC report on Cross-Sector Interdependencies was a good start on how risk can be reduced through:
 - ❑ Additional analysis
 - ❑ Considerations of the supply and value chain
 - ❑ Participation in local, state, regional, and federal planning
 - ❑ Table-top exercises

Vice Chairman Chambers said the question surrounding interdependency-based risk could be requantified but may have an overly complex scope. The government has largely led local, state and regional exercises, which have been very constructive. One approach is to examine how the private sector can better participate in the design and execution of these exercises. Advice the Council provides after modeling should be more than nominal comments—if critical infrastructures can provide meaningful value they should be involved earlier in the cycle. For example, if they are only brought in after computer modeling studies, how can the private sector ensure that modeling premises are realistic, useful, and accurate? Actions can be prioritized if risk can be quantified.

Chairman Nye said this is a subject that could take time and the NIAC needs manageable tasks to ensure it does not take on something too vast in scope.

Vice Chairman Chambers said it could indeed take much work without producing the desired results.

Chairman Nye solicited comments.

Under Secretary Libutti supported the study proposal and left it up to NIAC leadership to determine the course of action. He reiterated that he and Assistant Secretary Liscouski would be advocates for the NIAC as long as the Council's message was clear.

Vice Chairman Chambers said that this issue might be best addressed by the NIAC by breaking the issue into exercises or computer models and following up with other activities to make the scope more manageable.

Mr. Donald Carty agreed that this was a large topic and the Council needs more focus as to what its output would be.

Assistant Secretary Liscouski said the government is currently involved in a great deal of interdependency analysis that can potentially be leveraged for the Council to determine how to better refine this initiative. This may be an area where current work can be enhanced with the Council's input to determine if ongoing efforts need adjustments.

Chairman Nye suggested that the Council could simply respond and cooperate with those efforts as they go forward.

Assistant Secretary Liscouski said the government might be able to offer the sponsorship of tabletop exercises to demonstrate modeling for the Council.

Chairman Nye said this would be more effective if the NIAC had security clearances. He asked Vice Chairman Chambers to move on to the next item.

3. Vice Chairman Chambers stated the third topic has to do with Risk Management approaches. Private sector manages risk on multiple levels. Risk Management is something that they have either grown up with or become accustomed to. The NIAC might want to consider looking at methods to develop meaningful guidance for the President's National Critical Infrastructure Planning. There could be meaningful items overlooked if the nation becomes primarily focused on worst-case events to establish priorities. Perhaps a better focus might explore these variables:
 - ❑ The likelihood of occurrence
 - ❑ The impact of occurrence
 - ❑ Threat capabilities

It is impossible to protect against every likelihood and the government must avoid spreading itself too thin in an attempt to guard against everything. Prioritization becomes key and the challenge is to use risk management techniques to prioritize:

- ❑ High impact, low probability events
- ❑ Magnitude and duration of the consequences
- ❑ Costs versus benefits of a defense
- ❑ Chief positive business cases security
- ❑ Customer and public impact of those threats
- ❑ Defensive measures

Vice Chairman Chambers said he thinks the NIAC understands defensive actions might be more costly and also create more problems than the original problem placed before it. Given all of the above, how does the Council begin to prioritize needed actions?

Chairman Nye said this topic had some appeal but he was unsure of how practical it was. Advice is only helpful if it is constructive and well-received.

Under Secretary Libutti stated there is an ongoing process within DHS and other agencies that takes a fairly solid, professional approach at doing what has been outlined regarding different scenarios, whether they are worst case or best case. There is a classified daily briefing that might have some value as a sidebar effort. This briefing uses indirect private sector inputs. This may be helpful to look at, with the right clearances of course, to potentially apply to the NIAC's focus areas instead of starting from nothing.

Chairman Nye said they might need to reformulate this proposal.

Chairman Nye noted that Mr. R. James Caverly is present representing the agency as well and the NIAC invited his comments as it moves forward. He asked Vice Chairman Chambers for his thoughts on reformulating the topic.

Vice Chairman Chambers said he would be comfortable with eliminating excess topics to prioritize the Council's interests. Whether it's a reformulation of this one as one of the top three priorities or one of the other issues.

Chairman Nye asked the Vice Chairman to move on to the next topic.

4. Vice Chairman Chambers presented the fourth issue, one of long-term critical infrastructure erosion. The NIAC has considered the catastrophic events of 9/11 but not the persistent, long-term erosion of infrastructure. The essential question is whether or not the aging infrastructure system contributes to the risk of large-scale infrastructure failure. Could the impact to the economy, both at the national level or state level, be much more than anticipated and are new policies or procedures needed? He asked Ms. Marilyn Ware and Mr. Martin McGuinn for their thoughts.

Ms. Ware said this certainly has appeal at three time horizons—immediate, middle, and long-term. This item revolves around a constant maintenance process.

According to Mr. McGuinn, in the financial sector the infrastructure is more a private obligation because of how it is controlled but there might be specific suggestions for new or revised policies.

Mr. Conrades said there might be a possible linkage of the last few topics. Finding new ways to assess risk for these critical infrastructures may tie into the long-term erosion issue. If critical infrastructure protection would include the erosion concept, it could link to what DHS is already working on to help prioritize how to look at the various infrastructures. There is a thought that if the Council learned more about what DHS is thinking it might be able to help evaluate the possible effects of erosion on various infrastructures.

Chairman Nye thought this topic to be longer term and perhaps as something the Council could take up at a later date.

Vice Chairman Chambers agreed and asked if Mr. Carty had any thoughts on this overall topic.

Mr. Carty echoed Vice Chairman Chambers' comments and said it is largely a private-sector issue--in aviation, these infrastructures are really government infrastructures. This is a longer-term issue than some of the time-sensitive, critical topics the Council has been discussing.

Ms. Ware stated the Risk Management approach and the erosion question could be looked at in conjunction with critical infrastructure maintenance. Combining risk assessment with critical infrastructure erosion is a good idea if the Council can find a way to simplify the topics.

Mr. Berkeley stated some of the efforts in DHS are developing prioritization and risk assessment schemes; these would be useful to avoid effort duplication, have commonality, and established standards.

Assistant Secretary Liscouski said the government has a variety of efforts underway that look at prioritization based on consequential loss as well as the importance of infrastructure to the various components served. He said the government would share this. Seeking input from the Council, Assistant Secretary Liscouski would like to consider the terms of measuring from a quantitative as well as qualitative perspective in order to assess whether the efforts currently underway are actually having a material difference in protection. So much of what is being done is from a risk management standpoint and is focused on output where the threat is mapped as it relates to the vulnerability itself. Metrics are the single largest gap that both sectors, public and private, face. It is important to have a business case to ensure a return on investment and, even more importantly, a security profile increase. This is a very rich area and should be further developed over time.

5. Vice Chairman Chambers began the discussion of the fifth issue, Crisis Management for National Network Infrastructure System Events. The key question is: What are the strategies and processes that help manage recovery and reconstitution? It is important to have a better understanding about what the private sector's approaches are, how they work, and especially how government stakeholders are involved. What government resources might be needed for this? What are the proper roles for DHS and sector specific agencies?

Chairman Nye asked if there were any comments or questions. There were none. He advised Vice Chairman Chambers to move into the sixth and final topic.

6. Vice Chairman Chambers presented the sixth topic that deals with human resources. This concept is something everyone intellectually grasps, but he was unsure as to whether everyone understood the long-term implications. How do we ensure adequate development of intellectual capital to protect American critical information infrastructure and infrastructure concepts? Many global peers emphasize engineering and security education. Data from a recent Wall Street Journal article indicates that China and India graduate up to five times more engineers than U.S. colleges do. At the end of the decade, that number is very likely to be in excess of ten times more. The U.S. was ranked nineteenth in the most recent ranking of math skills for eighth-graders. Some NIAC members have asked if this is adequate as it relates to education and security infrastructure policy issues.

Vice Chairman Chambers continued, asking if the U.S. needs an educational policy change as it relates to critical infrastructure. Can academic programs attract adequate numbers of students and provide adequate quality of education? Specifically, does computer security curriculum include topics relative to critical infrastructure? There must be a way to plan five and ten years out to attract America's best and brightest to these fields and also vary some of the current studies on academia to be expanded in this area. American education is falling behind when it comes to networking security knowledge; while there are good programs like the Federal Cyber Corps, a scholarship program, are these really meeting their goals? Looking at this issue from a

human resources perspective, attracting talent, and encouraging the proper curriculum might create the desired environment for a Cyber Corps type of activity.

Mr. Conrades thought this was a need as well. As he stated in the Hardening the Internet report, the effect of security on information systems and the Internet will be addressed as the need for better courses and better training at the collegiate level

Mr. Berkeley stated he thought the issue was important.

Dr. Linwood Rose thanked Vice Chairman Chambers for his excellent summary of this item. As a university president, he said his concern is that schools are not producing engineering and computer science graduates in the numbers that are desperately needed to serve the needs of business and industry and also the professorial needs for American institutions to conduct research. He said he hoped this was an item to which the Council the NIAC could devote attention.

Mr. McGuinn said the NIAC is addressing many urgent issues as quickly as possible, but there are long term issues, such as the need for bolstered education, that the Council should begin to take certain actions now.

Mr. Carty said the NIAC should ask itself if it is going to add significant voice and light to an issue because he thought the government was already addressing it. Is it more appropriate for the NIAC to focus on things more directly impacting national security?

Chairman Nye said Mr. Carty's point was valid. He asked if this extended to the peripheral issue of student visas.

Vice Chairman Chambers stated he thought the key issue, referred to by Dr. Rose, was to focus on curricula to generate relevant skill sets and to attract the best and brightest talent within the country. If there's an additional issue on visas he said he thought it might be manageable. A large part of the sub-issues, such as software quality, security issues, architectural security issues, or security processes and procedures might be worth making a subset. Subsets might narrow the overall scope of this issue.

Mr. Conrades said creating subsets puts the issue on target for the scope of the NIAC. He supported breaking the task down to narrow the scope.

Vice Chairman Chambers asked the Chairman to propose a voting process. He said it might be best to go through each of the items and have members pick their top two. He re-emphasized that no one is necessarily looking for work, so as a group the NIAC should be sure that the government thinks the issues will be worthwhile.

Chairman Nye asked Assistant Secretary Liscouski for any preference on these issues.

Assistant Secretary Liscouski said the first item, intelligence, was a critical one. In fairness to the Council, there are some efforts in which the government is engaged which the NIAC could

put off; for instance, there is a need for a stronger engagement with the Council and private sector in tabletop exercises. Also, there are impediments like security clearances. Nonetheless, trying to work in ways to integrate modeling and tabletop exercises and focus on bringing the private sector further into this process is important.

Mr. Caverly said he doubted government has a clear picture of exactly what the infrastructures' replacement capabilities are. Critical infrastructure's response to serious damage hinges on the private sector's ability to convey the realities of restoring a large electrical system or a large water system to the government. These types of recovery activities are not well comprehended and would be valuable to the government.

Chairman Nye said he would go through the roll and ask each Council member for comments, listing the number of their preferred topic.

1. Intelligence Process & Work Products Regarding Critical Infrastructures
2. Interdependencies: Analysis, Planning, Exercises & Practice
3. Risk Management Approaches to Protection
4. Long-Term Erosion of Critical Infrastructure
5. Crisis Management for a National Networked-Information-Systems Event
6. Human Resources

Member	Topic Preference
Nye	
Chambers	
Berkeley	1,3,6
Carty	1,3,6
Conrades	1,3,6
Davidson	1,5,6
Gallegos	1,3,5
Grayson	1,3,6
Marsh	1,3,5
Martinez	1,3,5
McGuinn	1,5,6
Noonan	1,3,5,6
Rose	1,5,6
Ware	1,3,5

Regarding Mr. Davidson's vote, Mr. Noonan asserted that the fifth issue, Crisis Management for a National Networked-Information-Systems Event, was tied to the role of ISACs and their enhancement. Ultimately, he said, ISACs will need to manage crises as well as the ability to disseminate information effectively and coordinate with first responders.

Meeting Minutes for July 13, 2004 Meeting

Page 28

Chief Gallegos said the fifth issue, Crisis Management for a National Networked-Information-Systems Event, is critical in handling other issues, especially the Intelligence Process and Work Products Regarding Critical Infrastructures.

Ms. Marsh voiced her concern of whether these issues are in-scope, since they are so broad reaching.

Vice Chairman Chambers said he was trying to strike a balance between what the NIAC could do to really make a difference and recommended the first and sixth issues. The first issue would be best served by looking at a subset.

Chairman Nye asked Ms. Cheryl Peace, a representative from the White House, if she had any comments.

Ms. Peace said she wanted the NIAC to take on the first issue. She said one of the concerns she has about number six is there are existing programs already in place looking at human resources.

Chief Gallegos asked if a motion to vote would be in order, and if so, he motioned for a vote on these issues.

Mr. Conrades seconded the motion and supporting a vote on the first issue, intelligence, and the third issue, risk.

Chairman Nye asked for volunteers to lead the study on these issues.

Vice Chairman Chambers volunteered for the first item, intelligence, and said he would be honored to have somebody serve with him as co-chair.

Chief Gallegos volunteered.

Mr. Noonan offered his leadership or co-leadership for the third issue, risk management.

Ms. Marsh volunteered to co-chair with him on initiative three.

Vice Chairman Chambers asked Chairman Nye determine if there was a majority on the sixth item, education. He said it would not be difficult if done right. This might be an item that the NIAC can make a recommendation on and see tangible results in twelve months.

Chairman Nye asked the Vice Chairman to make a motion. He did so and the motion was seconded.

Chairman Nye asked the NIAC if it was in favor of addressing the Human Resources issue as well as issues one and three.

This was voted on and agreed upon by the Council.

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

Meeting Minutes for July 13, 2004 Meeting

Page 29

Chairman Nye asked if Dr. Rose would lead this initiative.

Dr. Rose agreed and asked if he could be provided with a business co-chair.

Chairman Nye asked Mr. Berkeley if he would be willing to co-chair with Dr. Rose.

Mr. Berkeley agreed.

Chairman Nye said he thought the Council made real progress and those three items will be well received. Chairman Nye said the NIAC would presumably get more information from the President on July 15.

VIII. NEW BUSINESS

Chairman Nye then requested approval for the minutes of the April 13 meeting.

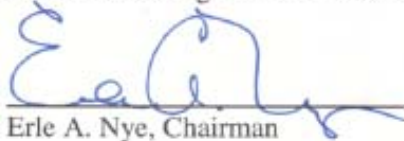
A motion was made and seconded and the minutes were approved.

Chairman Nye said he appreciated the patience of all those attending, whether in person or by telephone. He said the Council made a lot of progress and he thanked the members for all the contributions they have made. The NIAC is making a good contribution and he trusted that everyone is receiving some personal satisfaction from that.

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: 10-12-04

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 July 2004

1

Agenda

- Background
- Methodology
- Challenges
- Recommendation Areas
- 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 encourage private sector security improvements

Methodology

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

5

Study Group Participants

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

6

Challenges

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

7

Recommendation Areas

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

8

Education and awareness

- ❑ Develop academic curricula targeted at security needs.
- ❑ Target, via mass media, end-users on Internet security requirements.
- ❑ Corporate information security—board level issue.

Research and Development

- ❑ Investigation of secure protocol versions
 - Exploration of costs and benefits; implementation schemes; new, more secure core technologies
- ❑ Advanced security management technologies, including:
 - Scalable tools for network analysis
- ❑ Security governance issues
 - Understanding factors relating to adoption of best practices
 - Security ROI business case studies

Empowerment

- Investigate methods for ISPs to provide security controls.
- Investigate barriers to law enforcement prosecution of cyber crimes.

Next Steps

- Finalize draft report for the NIAC
- Submit report to NIAC for review

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 – July 13, 2004

1

Presentation Outline

- Background
 - Deliverables
 - Survey Content
 - Report on Actions to Date
 - Critical Infrastructures Surveyed
 - Preliminary Observations
 - Next Steps
 - 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”)

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
- Implications of various types of cyber attacks on these key systems

Report on Actions Taken to Date

- | | |
|---|----------|
| <input type="checkbox"/> Survey Finalized | April 28 |
| <input type="checkbox"/> Survey Distribution | April 30 |
| <input type="checkbox"/> Return Date for Surveys | May 26 |
| <input type="checkbox"/> Follow Up | June |
| <input type="checkbox"/> Compilation and analysis | July 10 |

Critical Infrastructures Surveyed and

✓ *Responses Received to date*

- Telecommunications
 - Information Technology
 - Transportation
 - Postal and Parcel Shipping
 - Banking and Finance
 - Public Health and Health Care
 - Agriculture and Food
 - Water
 - Energy
 - Defense Industry Base
 - Chemical
 - Government Emergency Services
-

7

Preliminary Observations

Weighted Rankings of Dependencies

1. Telecom
 2. Energy
 3. Banking
 4. Postal
 5. Transportation
 6. Water
 7. Food
 8. EMS
 9. Chemical
 10. Public Health
 11. IT
-

8

Other Preliminary Observations

- ❑ Respondents very concerned about confidentiality of data.
- ❑ Answers are dependent upon the nature and duration of disaster.
- ❑ Sound business continuity practices provide some protection:
 - Ability to revert to back up systems, and further ability to revert to manual systems, though less efficient, can minimize impact in some sectors.
 - Inefficiency of manual procedures would result in increased costs or lost revenue for some sectors.
 - Redundancy expense is often already realized as part of existing business continuity programs.
 - System restoration would happen more often than system replacement.
 - Costs to reconstruct data, or to run in a manual mode, would be great.
 - Diversity of vendors within core systems provides some additional protection.

Next Steps

- ❑ Addition of any late surveys
- ❑ Finalize analysis
- ❑ Submit report to NIAC for review

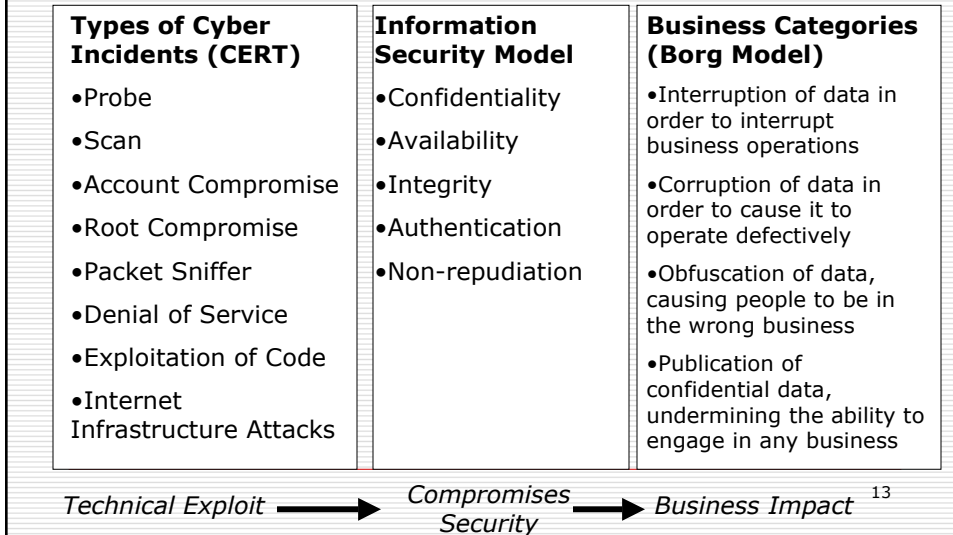
Appendix

□ 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
- Gail Kaufman, DHS
- David Sanders, DHS, National Cyber Security Division
- Tran Trang, NCSD

Cyber-Attack Models



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

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

ATTACHMENT C
(Status Report on Common Vulnerability Scoring System)

CVSS

The Common Vulnerability Scoring System

June 2004
NIAC Vulnerability Disclosure Working Group
Scoring Subgroup

John Chambers
President & CEO
Cisco Systems, Inc.

John Thompson
Chairman & CEO
Symantec Corp.

1

Agenda

- Status
- CVSS update
 - Changes to the model
 - Scoring process
 - Formulae
- Next steps
- Timeline

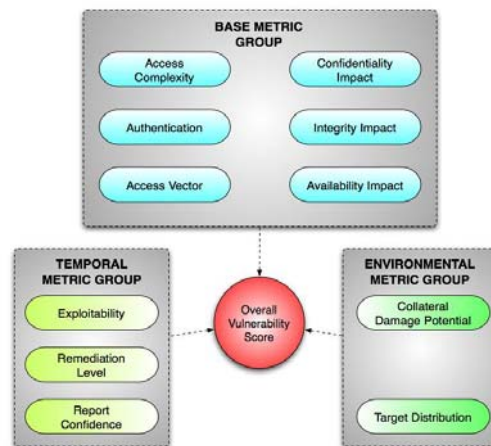
2

June 2004 Status

- ❑ 90% complete
 - System designed, metrics, formulae, scoring methodology completed
 - Completed formulas and scoring
 - ❑ Engaging industry for testing
 - Phase one
 - ❑ In-house testing by designers
 - Phase two
 - ❑ Tapping other industry for participation
 - ❑ Commitment from Qualys and Symantec to implement the final version of CVSS
-

3

The CVSS



4

Base Metric Group Scoring

- Has the largest bearing on the final score
 - Provides the foundation for the final score
- The impact metrics have the strongest weight on the base score
 - Confidentiality
 - Integrity
 - Availability

Temporal Metric Group Scoring

- Can modify the base score by 0 to 25% downwards from the initial value
- Allows for the introduction of mitigating factors to reduce the threat score of a vulnerability
- Designed to be re-evaluated at specific intervals as a vulnerability ages

Environmental Metric Group Scoring

- Potentially decreases or increases the final score
- Environmental metric group allows for organizations to adjust the severity of a vulnerability within on the context of their own environment

Next Steps

- Testing:
 - Stress tests: dry run system through several selected vulnerabilities
 - Validate with industry study groups
- Take feedback from testing and improve system
- Complete report to NIAC
- Pending NIAC review, implement CVSS (TBD: html/asp/xml/Excel)
- Pending NIAC approval and industry acceptance, submit IETF draft

Timeline

- ❑ August 01, 2004: complete real world testing
- ❑ August 30, 2004: complete feedback and finalize CVSS
- ❑ September 15, 2004: complete report for NIAC

Three Examples

Vulnerability	Microsoft Outlook Express scripting vulnerability	Microsoft LSASS vulnerability	BGP route flapping denial of service vulnerability
Typical Exploit	W32/Netsky.B virus	Sasser worm	None known

Access Vector	REMOTE	REMOTE	REMOTE
Access Complexity	HIGH	LOW	HIGH
Authentication	NOT-REQUIRED	NOT-REQUIRED	NOT-REQUIRED
Confidentiality Impact	COMPLETE	COMPLETE	NONE
Integrity Impact	COMPLETE	COMPLETE	NONE
Availability Impact	COMPLETE	COMPLETE	COMPLETE
BASE SCORE	8.3	10.0	2.8

Exploitability	FUNCTIONAL	HIGH	PROOF-OF-CONCEPT
Remediation Level	OFFICIAL-FIX	OFFICIAL-FIX	TEMPORARY-FIX
Report Confidence	CONFIRMED	CONFIRMED	CONFIRMED
TEMPORAL SCORE	7.2	9.1	2.3

Collateral Damage Potential	NONE	NONE	NONE
Target Distribution	HIGH	HIGH	HIGH
ENVIRONMENTAL SCORE	7.2	9.1	2.3

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

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

Final Report and Proposed Recommendations

July 13, 2004

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

Agenda

- Status
- EEIS Update
 - Changes to the report
 - Edits from Working Group
 - Report format updated
 - Edits from DHS
- Next Steps
 - Review by NIAC and final edits
 - Deliver report
- Timeline

July 2004 Status

- Edits completed
 - Reviewed and edited by the NIAC Secretariat at DHS
- Report forwarded to NIAC for comment
 - Initial Input – during / prior to meeting
 - Final Input – within 30 days

3

Next Steps

- Incorporate input from full NIAC review
- Prepare Letter for the President
- NIAC final approval
- Submit Letter to the President

4

Timeline

- Letter Final Draft: July 20, 2004

- Final Report: August 01, 2004

- Deliver Report: August 10, 2004

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