

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING

Tuesday, January 13, 2004
4:00 p.m. – 6:00 p.m.

Washington Convention Center
801 Mount Vernon Place, NW
Washington, D.C.

AGENDA

- I. OPENING OF MEETING:** Nancy J. Wong, *U.S. Department of Homeland Security (DHS)/Designated Federal Official, NIAC*
- II. ROLL CALL:** Nancy J. Wong
- III. OPENING REMARKS:** *Lt. Gen. Frank Libutti (USMC, ret.), Under Secretary for Information Analysis and Infrastructure Protection, DHS;*
Richard K. Davidson, Chairman, President & CEO, Union Pacific Corporation; Chairman, NIAC; and
John T. Chambers, President & CEO, Cisco Systems, Inc.; Vice Chairman, NIAC
- IV. REVIEW OF THE ROLE OF SPECIAL GOVERNMENT EMPLOYEE** *Robert E. Coyle, Legal Advisor for Ethics, DHS/Office of General Counsel*
- V. STATUS REPORTS ON PENDING INITIATIVES:**
- A. Evaluation and Enhancement of Information Sharing and Analysis** *Thomas E. Noonan, Chairman, President & CEO, Internet Security Systems, Inc.; NIAC Member*
- B. Regulatory Guidance / Best Practices for Enhancing Security of Critical Infrastructure Industries** *Karen L. Katen, President, Pfizer Global Pharmaceuticals and Exec. V.P., Pfizer Inc.; NIAC Member*
- C. Hardening the Internet** *George H. Conrades, Chairman & CEO, Akamai Technologies; NIAC Member*

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

Meeting Minutes and Briefing Materials for January 13, 2004 Meeting

Page 2

- | | |
|---|--|
| D. Prioritization of Internet Vulnerabilities | <i>Martin G. McGuinn, Chairman & CEO, Mellon Financial Corporation; NIAC Member</i> |
| E. Vulnerability Scoring Research Task | <i>Vice Chairman Chambers; and John W. Thompson, Chairman & CEO, Symantec Corporation; NIAC Member</i> |
| VI. FINAL REPORT AND DISCUSSION OF THE SECTOR INTERDEPENDENCIES/RISK ASSESSMENT GUIDANCE WORKING GROUP | <i>Martin G. McGuinn, Chairman & CEO, Mellon Financial Corporation; NIAC Member</i> |
| VII. FINAL REPORT AND DISCUSSION OF THE WORKING GROUP ON VULNERABILITY DISCLOSURE | <i>Vice Chairman Chambers; and John W. Thompson, Chairman & CEO, Symantec Corporation; NIAC Member</i> |
| VIII. ADOPTION OF NIAC RECOMMENDATIONS | NIAC Members |
| IX. NEW BUSINESS | <i>Chairman Davidson; NIAC Members</i> |
| X. ADJOURNMENT | |

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON

Chairman Davidson; Mr. Berkeley; Ms. Katen; Mr. Thompson; and Ms. Ware

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL

Vice Chairman Chambers; Mr. Barrett; Mr. Carty; Mr. Conrades; Mr. Dunham; General Edmonds; Chief Gallegos; Ms. Grayson; Mr. Holliday; Ms. Marsh; Mr. Martinez; Mr. McGuinn; Mr. Noonan; Mr. Nye; Mr. Webb; and Mr. Kovacevich.

STAFF DESIGNEES MONITORING PROCEEDINGS ON BEHALF OF ABSENT NIAC MEMBERS:

Tom Lockwood (for Governor Ehrlich); Sgt. Paul Morrell (for Commissioner Kelly); and John Puckett (for Mr. Holliday);

MEMBERS ABSENT:

Mr. Hernandez; Mr. Kovacevich; Dr. Rose; Mayor Santini-Padilla; and Mr. Weidemeyer

OTHER DIGNITARIES PRESENT:

U.S. Government: Mr. Robert E. Coyle, Acting Legal Advisor For Ethics, the Department of Homeland Security; The Honorable Frank Libutti, Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection; 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 seventh meeting of the NIAC, including Chairman Davidson, Vice Chairman Chambers, 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.

III. OPENING REMARKS

The Honorable Frank Libutti, Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection, Department of Homeland Security (DHS)

Richard K. Davidson, Chairman, President & CEO, Union Pacific Corporation; Chairman, NIAC; and

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

Under Secretary Libutti opened his comments by welcoming the attendees to the meeting of the National Infrastructure Advisory Council, and said that he hoped everyone had an enjoyable holiday season. He thanked the attendees for their active participation in the meeting. Under Secretary Libutti asserted that the Department of Homeland Security values the partnership between the public and private sectors that NIAC brings to the issue of critical infrastructure protection.

Under Secretary Libutti reviewed the meeting's prepared materials and said that he was very impressed with the amount of work and thoughtfulness that have gone into the studies, the conclusions, and the proposed recommendations. He stated that everyone had accomplished a substantial amount of work to help DHS think through some difficult issues and he expressed his appreciation for the investment of time and energy for these efforts.

Over the two days [preceding the NIAC meeting], participants of DHS/IAIP's Private Sector Conference had wrestled with some tough issues. Under Secretary Libutti then stated that he would like to share some of the conference's key points, which were compiled from information gathered from breakout discussions involving members of the private sector. He showed slides to the members via the Internet slide show that had been set up for the Council's meeting.

The slideshow began on the following subject: responders to threat information require access to greater detail about the threat—there is a need for greater granularity of the information provided so they can take appropriate action. Associated with the control and security of such threat information are the issues of liability and privacy as well as the development of general communication mechanisms needed to transmit this information.

The second slide highlighted the fact that different sectors have different expertise. Standards and capabilities must be leveraged to create a holistic approach to homeland security. Metrics are critical—it is important to have measurements for reasonable expectations. It is important for the private and public sectors to work together to support common objectives. Referenced were operational, professional, academic, law enforcement, and the intelligence business. Also needed are the greater transparency, responsibility, and capability of the various public and

private control mechanisms. Strategies are supported by Standard Operating Procedures that create options for action. Also discussed was facilitation by third-party entities.

Ongoing, effective dialogue is another key component of DHS' strategy for engaging the private sector. DHS believes that it is currently involved and needs to remain involved. The concept of operation raised several months ago was engineered to reach out to the Department's customer base.

The discussions at the Washington Convention Center over the previous two days represented Phase II—the Private Sector. DHS needs to reach out with greater energy to other members of the private sector. Sector Coordinators and ISACs must be coordinated into DHS activities. The final phase involves sending teams of Homeland Security executives out to visit state and local officials, as well as private sector leadership within those regions of the country.

Information sharing is critical and important—information, particularly when oriented toward intelligence must be actionable to provide any value. There are issues affecting information sharing at the regional level. There needs to be some network connecting the regional piece with the smaller business community. Who should be the advocate for smaller business communities on a regional scale?

It is imperative for private sector organizations to develop business relationships with one another that include security considerations. It is also necessary to have business entities involved in the process of developing a national strategy with the federal government as opposed to having the federal government unilaterally impose some process on its own. Under Secretary Libutti said he hoped they were breaking in this new paradigm by engaging private sector partners to contribute to the development of actions. There should also be increased focus on the national alert level.

The NIAC'S work represents a continuing dialogue between the federal government and private industry; the ongoing work is also a source of potential improvements for carrying out the national program for critical infrastructure protection. The nation recently came down from code "orange" and, during the most recent period of alert, DHS applied many lessons learned from past alerts. Under Secretary Libutti asked for the council's help in identifying lessons learned from the most recent period of heightened (high) alert.

Under Secretary Libutti welcomed feedback from the members of this council on how effectively DHS performed and in identifying opportunities for improvement.

Chairman Davidson said that, from his point of view, it appeared as though the government acted with good information during the most recent period of high alert. Industry leaders appreciated the specificity of the information—this was really the first time the information had been provided in such a way. While the general alert level was raised everywhere, there were specific areas of concern, and alerting the council to these areas helped focus the group's activities. This alert exhibited a cycle of improvement.

Vice Chairman Chambers echoed Chairman Davidson's comments and said that the latest alert was handled well. These alerts are being handled more and more effectively with the industry partners. Each time these alerts are issued, it appears that they are dealt with more and more effectively. Vice Chairman Chambers said that he also realized that there is a balancing act between what can be shared and what cannot be shared—but this balancing seems to have improved. Vice Chairman Chambers gave the alert solid results.

Mr. Berkeley said that he was encouraged by a poll in the newspapers that citizens realized that there was a continued threat and expected this to go on for a while. It seems that educational efforts and the good common sense of the American public are coming together.

Chairman Davidson said that if there were no more comments, he would thank Under Secretary Libutti and move the meeting along.

Chairman Davidson welcomed the members of the NIAC Committee, members of the federal government, and the public. He said that while the public cannot speak during the meeting, it may contribute feedback through the NIAC website. He said that there was a big agenda with a lot of items to discuss. In a moment, the meeting will begin with an ethics presentation on the role of Special Government Employees.

There are several heroes serving on this committee—the group has taken on some huge assignments. People are working hard to do the right thing and come up with the right conclusions. He also thanked NSTAC members for their contribution to one of today's final recommendations—they have been working on CIP for a long time. Their input has helped us formulate our recommendations and letters that will be transmitted to the President.

Chairman Davidson said that as he looked at Homeland Security Presidential Directive 7 (HSPD 7) and Homeland Security Presidential Directive 8 (HSPD 8), comments from this group have had an impact. A number of the thoughts coming from the NIAC are reflected in those two documents. He also said he was pleased to hear the Under Secretary's thoughts on DHS working more closely with the Private Sector—there is no question that cooperation is needed for a successful effort.

Vice Chairman Chambers thanked the Chairman and began by echoing the Chairman's statements. He thanked the Interdependency Risk Assessment and Vulnerability Disclosure Working Groups for concluding their work. It is important to take on new projects, but it is also important to complete them in a timely fashion and get conclusions. He hoped the Council would appreciate the professional deliverables that were going to be presented. He thanked other groups, the NSTAC in particular, for their help in the review, and for their comments on the Interdependency Risk Assessment Working Group Report.

Vice Chairman Chambers said the Working Groups are making great progress, the NIAC is seeing to it that topics chosen are both meaty and important, and that the interdependencies between them becomes immediately clear when one thinks about the Vulnerability Disclosures, Information Sharing, the Role of Regulation, Internet Vulnerabilities, and Internet Hardening.

The NIAC can begin to see these reports are not just separate independent reports, but can begin to tie them together constructively.

The Vice Chairman also noted the intensity in which the Working Groups were operating at. He thanked the staffs for their hard work. He lauded the groups for keeping focused while trying to turn around substantial topics in a relatively strict and short time period.

Vice Chairman Chambers also asked the members of the NIAC if they agreed the quarterly meeting schedule was working well, and the teleconferencing and web technology is enabling the Council to be extremely productive and efficient.

The NIAC responded affirmatively to the Vice Chairman's question. Mr. Edmonds said he thought the meetings were being coordinated with a perfect combination of in-person meetings and teleconferencing.

Vice Chairman Chambers concluded his opening remarks and turned the floor back to Chairman Davidson.

Chairman Davidson thanked Vice Chairman Chambers and introduced Mr. Robert E. Coyle, Legal Advisor for Ethics in the Department of Homeland Security.

IV. REVIEW OF THE ROLE OF SPECIAL GOVERNMENT EMPLOYEE

Robert E. Coyle, Legal Advisor For Ethics, DHS/Office Of The General Counsel

Mr. Coyle briefed the council on the legal compliance issues inherent with serving as a Special Government Employee. Chairman Davidson thanked Mr. Coyle for his thoroughness and for his offer to follow up with members on any questions they might have. He said that if there were no further questions, the meeting would move on.

Chairman Davidson said that one of the things that needed to be done was for the council to approve the minutes of the October 14th meeting. There have been a few minor changes such as getting names clarified and reporting on who was on which working group. Chairman Davidson asked for a motion to approve the minutes of the last meeting, Ms. Ware seconded the motion and the minutes were unanimously approved.

V. STATUS REPORTS ON PENDING INITIATIVES

A. Evaluation and Enhancement Of Information Sharing and Analysis

Thomas E. Noonan, Chairman, President & CEO, Internet Security Systems, Inc.; NIAC Member

B. Regulatory Guidance / Best Practices For Enhancing Security

Karen L. Katen, President, Pfizer Global Pharmaceuticals and Exec. V.P.,

Of Critical Infrastructure Industries	Pfizer Inc.; NIAC Member
C. Hardening the Internet	<i>George H. Conrades</i> , Chairman & CEO, Akamai Technologies; NIAC Member
D. Prioritization of Internet Vulnerabilities	<i>Martin G. McGuinn</i> , Chairman & CEO, Mellon Financial Corporation; NIAC Member
E. Vulnerability Scoring Research Task	<i>Vice Chairman Chambers; and John W. Thompson</i> , Chairman & CEO, Symantec Corporation; NIAC Member

Evaluation And Enhancement Of Information Sharing And Analysis

Chairman Davidson turned the meeting over to Mr. Tom Noonan for his working group on the role of the ISACs. Mr. Noonan began by saying that the Evaluation and Enhancement of Information Sharing and Analysis Working Group was established during the April 22, 2003 meeting of the NIAC, during which there had been a recommendation that a working group focus upon this item for further study. Accordingly, Mr. Noonan agreed to chair the working group. He said that sharing information within sectors, across sectors, and between the private sector and government is critical to understanding and responding to threats and to remediating vulnerabilities and hardening the infrastructure. With the speed and scale of cyber attacks, the only way to develop defensive action is by correlating events across companies and governments; industry ISACs were created with that in mind. Many ISACs have seen mixed results and mixed charters or varied levels of participation. The goal of this project was fairly simple and direct—to analyze the state of information sharing and analysis and identify current best practices while simultaneously developing guidelines and recommendations for enhancing the information sharing and analysis capabilities within both the public and private sectors. This has proven to be a formidable project with all of the change underway.

This project is focused on four key points of information sharing and analysis:

- ❑ Current business models for sharing and analyzing information, which have been established among many different industry sectors but not necessarily with a common charter, and financial models for supporting information processes and dissemination.
- ❑ The level of information analysis in aggregation.
- ❑ How that level of information is disseminated from a breadth and coverage perspective.
- ❑ Ultimately, the identification and documentation of best practices to ultimately recommend guidelines for information sharing and analysis.

The approach taken by this working group is leveraging existing ISAC analysis and findings. The working group had worked with DHS and interacted with the eleven main ISACs, reviewed the existing ISAC organizations, funding models, memberships, and challenges. The working group made specific progress in these areas. The group is in the process of reviewing government reports to remain up to date on all changes. Specific research goals have been defined to identify funding options and incentives geared to gain ISAC participation of all owners and operators in each sector.

Mr. Noonan turned the presentation over to Peter Allor, the leader of the group supporting Mr. Noonan's NIAC working group. Mr. Allor said that the group intends to have the recommendations together in time for the next NIAC meeting. The reason for the change is:

- ❑ HSPDs 7 and 8 were released.
- ❑ Significant changes have taken place within DHS.
- ❑ The ISAC Council made significant inroads in terms of what needs to be shared.

The study group has developed a great deal of information—some of it overlapping with information already uncovered. This exercise provided new data sources and a new focus for a lot of the group's activities and the group is trying to take this information and crosswalk it with DHS, the ISAC Council, and Sector Coordinators. These same groups are working matrices and discovering gaps previously identified as work tasks.

Mr. Noonan said that the group is anticipating making a final presentation at the April 13th meeting. Mr. Noonan thanked all the members of the working group and IAIP for actively participating in this. The group is awaiting additional feedback and input from the ISAC Council. Despite receiving some information on a financial sector review, the group is waiting for additional information. The group made a specific request to the Designated Federal Officer at DHS for information on how the federal government was presently funding ISACs.

Ms. Wong said that in terms of funding information, the working group is free to make a request of those private entities with ISACs. Whether they can provide that information to the working group is up to each of the ISACs. The private entities do not necessarily provide the federal government with information on their total funding. However, she stated that she had worked out a process with DHS's Office of General Council to make requests to the appropriate Federal agencies to release government-owned information to the working group.

Mr. Noonan thanked Ms. Wong for the clarification.

Chairman Davidson thanked Mr. Noonan for the presentation and said that the importance of the work being done is evident by the fact that other groups have picked up parts of this work as components of their own studies. Chairman Davidson moved the meeting on to Karen Katen's presentation on the role of regulation.

Regulatory Guidance/Best Practices for Enhancing Security of Critical Infrastructure Industries

Ms. Katen said that the review of the progress of the NIAC sub-team on "Regulatory Guidance Best Practices for Enhancing Security of Critical Infrastructure Industries" would consist of a brief progress report and a proposed timeline for the final delivery of the report to NIAC. At this point, Ms. Katen asked Jonathan White to report on the progress of the study being done.

Mr. White began by saying that at the last NIAC meeting, this working group reported on the results of an extensive data gathering exercise conducted with NIAC members and other sector

industry bodies. The group reviewed the requirements for regulation to enhance critical infrastructure security and identified some best practices for the introduction of new regulations. At that time a white paper on these issues was drafted.

NIAC members agreed that the working group should more thoroughly test these findings in four sectors—Chemicals, Finance, IT, and Water—before final submission. The volunteering NIAC members each proposed a lead for their sectors to help conduct this work. Ms. Katen thanked them for their work. Their contributions are helping to ensure a robust set of final recommendations. Ms. Katen also thanked Ms. Wong for her continued high standards of professional guidance on this project.

The initial discussions of the team have not generated any fundamental disagreements on the initial premise of the working document. Participants have been comfortable using the document to gain further input from critical stakeholders and to refine the recommendations.

However, while the need for speed and action on this work is evident, there was unanimous agreement that a slightly extended period of review and discussion would ensure a broader and more accurate representation of the sectors discussed in the final document. Discussions with DHS reinforced the view that wider review and endorsement was the preferred approach.

The working group proposed the following timeline for completion:

1. Additional sub-team activity through January and early February to complete the discussions with industry stakeholders;
2. Final composition of the document and review by lead NIAC members through late February; and
3. Distribution of the document to sector reviewers (in late February) and NIAC members (in March)—well in advance of the next meeting to allow time for each member to review and assess the implications.

Ms. Katen then asked for NIAC's approval to direct the team to deliver the final document according to these proposed dates.

Chairman Davidson next directed the meeting towards the Hardening the Internet Working Group, chaired by Mr. George Conrades. Mr. Paul Nicholas from The White House was also present to help define the scope.

Hardening The Internet

Mr. Conrades thanked Chairman Davidson and said that the working group was tasked on October 14th and it has just begun its real work. Four members of the NIAC have expressed interest in participating on the committee—himself, Mr. Alfred Berkeley, Ms. Peg Grayson, and Mr. Tom Noonan. Mr. Howard Schmidt of Ebay and Mr. Ken Watson of Cisco Systems have volunteered to be members of the study group.

The scope of the working group comprises determining methods to protect the Internet and mitigate its vulnerabilities. The impact of vulnerabilities on other critical infrastructures has been deemed out of scope. Some material on the subject has been distributed:

- Testimony before Congress;
- Internet Vulnerabilities;
- National Criminal Intelligence Sharing Plan;
- Output from the NIAC Interdependencies Working Group; and
- Cyber Vulnerabilities Guidelines.

As for next steps, the group is working to hold its first meeting within the next week. Mr. Conrades asked if there was a desired or expected date for the output of this working group—otherwise the group will set one itself and move forward as expeditiously as possible.

Chairman Davidson said that he did not think a date had been set, but everyone has forged ahead with due deliberation and speed. He said that there is no timeline, but that he was sure the study would be handled with the appropriate speed.

Mr. Conrades thanked the Chairman and concluded his report.

Mr. Nicholas from the Homeland Security Council spoke, saying that it may be appropriate to have the group develop a scope upon its first meeting. At that point, the group can come up with a timeline for deliverables. This is a complex task, and as the group begins to unfold what needs to be examined, it may be appropriate to have a prolonged dialogue about scope. Providing some kind of a report in the late summer or early fall may give insight into the draft recommendations of the group by that point.

Mr. Conrades thanked Mr. Nicholas and said that he would be sure to follow up. Vice Chairman Chambers said that it would be a mistake to develop a timeline before a scope is established.

Mr. Nicholas said that the Homeland Security Council is more than happy to discuss the scope of the work with the working group.

Mr. Chambers recommended that this working group include representatives from the NSTAC.

Mr. Davidson concurred and requested that Mr. Nicholas coordinate with the NSTAC to ensure that their input is included in this project.

Chairman Davidson thanked Mr. Conrades and turned the meeting toward Mr. McGuinn and his working group.

Prioritization of Internet Vulnerabilities

Mr. McGuinn began by saying that at the October meeting, the working group agreed to take on the task of looking at the impact of cyber vulnerabilities to our critical infrastructures. The core

working group that explored cross-sector interdependencies had begun this effort, and Mr. McGuinn turned the meeting over to Susan Vismor to provide a status update.

Ms. Vismor thanked Mr. McGuinn and said that at the October meeting, the group agreed to take on the task of answering the question: “Is the working group ranking critical infrastructures relative to their vulnerability to cyber attacks?” From the perspective to the NIAC working group, the answer to that question was, “no”. However, it was unclear whether there were any other efforts underway that might provide the answer.

The working group asked that DHS representatives provide their interpretation of the project scope and for information they might have on similar efforts, as well as guidance on how to deal with any issues related to confidential information.

Through various contacts, the study group had a number of briefings from individuals who had done some work in this area. Each of the briefings provided a very different way to look at the problem; none of them were “ranking” the critical infrastructures relative to their vulnerability to cyber attacks. Bell Labs recommended that the group contact National Labs about its capabilities to work through these types of issues.

Gartner, in conjunction with the U.S. Naval College, held a war game entitled “Digital Pearl Harbor” to determine the feasibility of cyber attacks crippling the U.S. economic and national infrastructure. Four sectors participated – telecommunications, the Internet, electrical power, and financial services. They did not build a model to rank the infrastructures.

CERT CC made the group aware of efforts that had been completed by several working groups under the direction of Mr. Richard Clarke as part of the NSTAC process. These efforts looked at the various vulnerabilities from the perspective of an Internet Service Provider. This information will be valuable to the working group looking at what can be done to “harden” the Internet. CERT CC also said that it was working through the issues per sector, and that our working group might be able to provide the touch points to the sector.

The working group received clarification back from DHS and the White House on the working group’s scope, to include:

- Does the group understand our major vulnerabilities and what are we doing about them?
- What are the most major problems with the security and reliability of the Internet?
- Does the working group understand the problems and has it prioritized them?

Ms. Vismor said that the working group needed to translate potential vulnerabilities into meaningful issues and analyze impacts on business operations based on NIAC members’ experience and knowledge. Priorities should be presented from an Internet user’s perspective. Systemic problems and design issues with the way the Internet operates are important to the President.

CERT CC will provide the working group with a matrix of current initiatives that are either underway or complete; the matrix is expected by February. The objective of this effort is to

understand where gaps exist. Any confidential information gathered can be protected under the Critical Infrastructure Information Protection Act.

Ms. Vismor said that the group is open to more direction and clarification from the NIAC on the purpose of the working group. Despite the information received thus far, this remains a complex issue, and the working group would like reassurance that it is on track.

The working group's charter is to:

- Identify the impact of a cyber attacks against critical infrastructures;
- Rank critical infrastructure by their vulnerability to cyber attacks; and
- Identify any potential mitigants.

This has been addressed as a point of clarification between this working group, and the working group is looking at ways to “harden the Internet.” This working group will be looking at the consequences of a threat (the threat being a cyber attack). The Hardening the Internet Working Group will look at the vulnerabilities of the Internet and potential ways to address some of the vulnerabilities.

Referenced, was a study published in 2001 that looked at the various types of cyber attacks. The report highlights the issue of interdependency among the critical infrastructures and that they are all dependent on information systems—the extent to which is not well understood. This report framed the issue or problem that the current working group is trying to solve. Drilling down further, it provided one example of one critical infrastructure, and the report summarized its vulnerability to a cyber attack. However, this report is dated and written only at a very high level.

The group proposed the following information-gathering method. Given the broad industry base within the NIAC, it may be more successful than a university setting for obtaining accurate and relevant information.

The working group will create a survey to be taken by the members of the NIAC and the participating sector groups that will:

- Identify the uses of the Internet by the “Major Players” in that sector.
- Analyze the impact to either National Security/Emergency Preparedness.
- Identify broad economic or business impacts.
- Identify any other significant impacts.

1. Using the information culled from the survey, it is important that the working group assign a metric.
2. Determine whether there is a substitute to fill the void.
3. Rank the substitutes.

Mr. Nicholas said that he thought the scope of what has been outlined is very good. One of the reasons behind constituting the NIAC was that when there is a cyber-disruption, the Federal Government does not really understand the implications for each industry. The government does

know that it is problematic but the outline highlighting what the vulnerabilities and their impacts are, will really help broaden national planning efforts and what needs to happen on the federal side.

Chairman Davidson said that Mr. Nicholas' words were good supporting comments because the NIAC does think it is working on very important issues and the enthusiasm brought to the table is remarkable.

At this point, Ms. Vismor thanked all of the NIAC Members for lending their valuable resources to this project.

Chairman Davidson then introduced Vice Chairman Chambers and Mr. John Thompson for their presentation on Vulnerability Scoring Research.

Vulnerability Scoring Research Task

Vice Chairman Chambers spoke and asked the NIAC whether he and Mr. Thompson could deliver this update as a component of their Final Report and Discussion of the Vulnerability Disclosure Working Group.

Chairman Davidson asked the Council for agreement; the Council agreed by voice and Chairman Davidson moved the meeting along to Mr. McGuinn's Final Report and Discussion on Sector Interdependencies and Risk Assessment Guidance Working Group.

VI. FINAL REPORT AND DISCUSSION OF THE SECTOR INTERDEPENDENCIES/RISK ASSESSMENT GUIDANCE WORKING GROUP *Martin G. McGuinn, Chairman & CEO, Mellon Financial Corporation; NIAC Member*

Mr. McGuinn extended his thanks to the various members of the working group, both from the NIAC companies and the Sector Coordinators that participated in this project. A special thanks goes to Chris Terzich, Wells Fargo, and Teresa Lindsey, BITS, who were both heavily involved and provided a great deal of support to Susan Vismor, chair of the study group on Cross Sector Interdependencies and Risk Assessment Guidance.

Mr. McGuinn thanked Mr. Duane Ackerman on behalf of the NSTAC, for its review and insightful feedback on the report—he believed that the NSTAC's comments were in agreement with the issues that were identified and that the NSTAC is supportive of our recommendations.

Mr. McGuinn continued his comments by saying that at the April meeting a working group was established to study cross-sector interdependencies and to provide risk assessment guidance. As reported at the October meeting, the chief benefit stemmed from the critical infrastructure sectors' ability to prepare for and manage an event.

As the group studied interdependencies, it concluded that cross-sector crisis management coordination was fundamental to the rapid restoration of critical infrastructure. The working

group identified nine issues and supporting recommendations that, if addressed, could improve restoration efforts.

At the October 14th NIAC meeting, the group reviewed its findings and recommendations on Cross Sector Interdependencies and Risk Assessment Guidance. Since that time, the NIAC has had a chance to review and express its opinions on the document. There was an overwhelming acceptance of the document by all of the NIAC members, with two suggested modifications. These changes have been incorporated and include:

- Removal of the recommendation that sector coordinators be consistently funded; and
- A modification to reflect the concept of a “sector coordinating mechanism”, as opposed to a specific sector coordinator.

The group agreed with these modifications and believed they accommodate changes that have occurred with the issuance of HSPD 7 in mid-December. This new directive provides greater flexibility for each sector to develop the most appropriate coordination mechanism. This is also in line with the NSTAC review, which noted the varying levels of development of each sector and recommended that each sector be examined within its own unique circumstances.

Mr. McGuinn stated that significant effort has been directed toward addressing concerns expressed in the report. This progress is due to many factors, including effective staffing and organization of the Department of Homeland Security. Many of the issues raised in the preliminary report have been acknowledged in recent Presidential Directives. The interaction between DHS and the NIAC provided an effective forum for private industry to be heard on these issues, and the Council thanks the DHS staff supporting the NIAC for helping to make this happen.

With that, Mr. McGuinn turned the platform over to Susan Vismor to walk through the presentation in detail.

Ms. Vismor thanked Mr. McGuinn and said that since the group presented its final report on October 14, DHS provided a briefing concerning its internal efforts and a briefing on HSPD 7. DHS also provided information from the Critical Infrastructure Protection Retreat, which included the Sector Coordinators and Information Sharing and Analysis Council.

With these briefings and comments from the NSTAC, the working group drafted a transmittal memorandum to be sent to the President with its final recommendations. This document was sent to the Council in advance of this meeting.

Ms. Vismor stated that the working group was encouraged that many of the issues that were raised at the October meeting were acknowledged in some manner, by DHS and the Administration. She believed that the NIAC process provided an effective forum to enable the private sector to voice its views with DHS, in a timely manner as policies were being formulated.

With that said, Ms. Vismor stated that the working group believes that at a summary level, two recommendations remain as top priorities. These include:

- The need to formalize the public/private partnership; and
- The need to prioritize the most important critical mitigation activities.

The private sector—as owners of 85 percent of the nation’s critical infrastructure—embraces its responsibility to ensure the protection of the country’s key assets. In order to do so effectively, the private sector must be regarded as an equal partner and included in all phases of developing, implementing, and sustaining processes designed to protect our homeland. These sentiments are echoed in the newly released report from The Gilmore Commission.

Ms. Vismor further described that a recent example of the private sector being excluded from processes is reflected in the publicly available draft version of The National Incident Management System (NIMS). NIMS mentions the importance of the private sector to this overall system, however, there is no formal process to include the private sector, particularly the critical infrastructure sectors, in incident response. It is imperative that NIMS provide the formal framework for public and private critical infrastructure incident management and emergency prevention, preparedness, response, recovery, and mitigation activities.

The President directed DHS to develop and administer a National Incident Management System, or NIMS. NIMS provides a consistent approach to incident management and emergency response for all levels of government.

The NIAC was provided a week to review the NIMS draft in December, and Ms. Vismor stated that the Council was grateful for the opportunity.

The private sector needs to be an integral part of the framework that is described in NIMS. In the document's current state, this inclusion appears to be missing. The public-private partnership should have private sector representation included throughout the process of development. It is unclear how "prioritization" of recovery efforts could take place without this inclusion.

In addition to these recommendations, it should be noted that the NSTAC had additional comments relative to NIMS that we encourage DHS to consider.

The Council’s second recommendation is to concentrate federal efforts on those critical infrastructures on which there is a higher degree of interdependency. The working group agrees that there is a universal dependence on the telecommunications infrastructure, with no real ability to self-mitigate the risk of this infrastructure.

The council credits Steve Malphrous and Angela Diamond from the Federal Reserve with this depiction of where Telecommunications fits in relationship to the other critical infrastructures. Colleagues in the study group from the electric sector have a slightly different interpretation, visualizing a coffee table with Telecommunications in the center, and electricity as the pedestal base.

Since 9/11, and more recently, with the recent Blackout of 2003, the country is more aware of its dependency on other critical infrastructures, most notably, power, transportation, and telecommunications. The council recognized a need to understand the recoverability of the critical infrastructures upon which the nation depends, and for infrastructure providers to understand the most critical requirements. Telecommunications represents a base infrastructure on which society depends and over which other infrastructures have little control, especially regarding the mitigation of the risks associated with its potential unavailability. If electricity goes out, generators can provide an alternate source of power. Telecommunications does not have that luxury. Therefore, sound business recovery practices require an awareness of the nation's dependencies on telecommunications, and an understanding of any single points of failure within that infrastructure. The NIAC is supportive of federal efforts to help address these risks. As the working group moves into cyber vulnerability analysis, the NSTAC reinforces the idea that in the telecommunications/IT area, the telecommunications infrastructure really provides the underlying core network for all cyber activities.

Ms. Vismor turned the briefing over to Mr. McGuinn for concluding remarks.

In closing, the Council still believes that the following fundamental principles hold true, and encourages DHS to embrace them.

- Provide short-term deliverables until longer-term visions can be executed.
- Measure progress.
- Realize that the partnership between the public and private sectors is a two-way street; with the timely and substantive exchange of information the partnership will grow to be the trusted partnership that is needed to insure our nation's security.

VII. ADOPTION OF NIAC RECOMMENDATIONS NIAC Members

Chairman Davidson said that he hoped everyone on the call has had the opportunity to take a look at the draft document and that NSTAC has been kind enough to provide the council with its comments as well. He asked if any other member of the committee had anything further to add and he asked whether everyone was in agreement with the way the recommendations were going. Mr. Erle Nye said that he had been impressed with the thoroughness and suggested that the NIAC proceed. Mr. Don Carty echoed Mr. Nye's sentiments and said that this was a job extremely well done.

Chairman Davidson thanked them for their comments. He asked Mr. McGuinn whether he wanted to talk about the proposal going to the President. Mr. McGuinn said that he believed a copy of the letter was distributed to everyone in advance. Chairman Davidson confirmed this and said that everyone should have received a copy and had a chance to review the document. Mr. McGuinn suggested that the NIAC go ahead with the letter unless there were any further comments. Vice Chairman Chambers said that he thought the letter was well written and that Mr. McGuinn summarized it well.

Chairman Davidson said that if the group heard no comments to the contrary, he suggested that the group approve the letter and move forward. The NIAC motioned for the approval of the

resolution; it was seconded and unanimously approved. Chairman Davidson thanked the council.

**VIII. FINAL REPORT AND DISCUSSION OF THE
WORKING GROUP ON VULNERABILITY
DISCLOSURE**

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

Vice Chairman Chambers opened by saying that both he and John Thompson were going to present a summary of the final report of the Vulnerability Disclosure Working Group. He trusted that everyone had time to review the written report and said that they would be asking for the NIAC's approval at the conclusion of this presentation.

Vice Chairman Chambers reiterated a point he made during the October meeting—that there had been an extraordinary level of participation by reviewers with extensive experience on all sides of this issue. Contributing to this report were: noted researchers; various industry user groups, including ISACs; service providers; government; vendors; U.S. and international coordinators; and members of the FIRST community. He believed the richness of the members' perspectives significantly enhanced the usefulness of the guidelines. These multiple perspectives also served as a sanity check; the report was neither a vendor report nor one slanted toward its discoverers. Neither was it U.S.-centric.

The working group's primary aim was simplifying the vulnerability management process through use of common communications mechanisms and processes. The group welcomed comments, and Vice Chairman Chambers said that it would work to find an appropriate vehicle for maintaining and updating this framework.

At this point, Vice Chairman Chambers turned the floor over to Mr. Thompson who would go through the charter, methodology, findings, key guidelines, and conclusions in the report. Vice Chairman Chambers intended to follow him with the proposed recommendations, next steps, and a couple of requests for this council.

Mr. Thompson thanked Vice Chairman Chambers and said that he was going to walk the meeting through the main points covered in the report. He asked that council interrupt him at any time with any questions. Also present were Mr. Rob Clyde, Chief Technology Officer for Symantec, and Ken Watson who led the study group's day-to-day activities associated with these efforts.

Mr. Thompson said that the initial charge of the group was the development of a "National Responsible Disclosure Policy." The working group quickly discovered that to be effective, this effort would have to be global, not national. Also, the word "responsible" applied equally to multiple perspectives; it was therefore dropped. Finally, U.S. policy applies to the federal government, but not to a set of global guidelines. Therefore, the group established two goals: first, the development of a framework for global vulnerability disclosure guidelines; and, second, derivation of specific policy recommendations for the President from those guidelines.

The scope of this framework covered notification, investigation, disclosure, and resolution of discovered and reported network security vulnerabilities. The report centered on communications among key stakeholders and common procedures to be used by all.

Mr. Thompson said that in the report, there is a list of all working and study group members, references, and reviewers in Appendix A (pages 37-45). These include NIAC member Tom Noonan and his team at ISS, the CERT CC with special attention to Sean Herndon, Richard Pethia, and Jeff Richter, who had done a terrific job in helping structure the report. Also included were MITRE, the Telecom ISAC, and the IT-ISAC.

Mr. Thompson echoed what John Chambers said in his opening remarks about the quality of input from external reviewers. He reaffirmed that without their extensive involvement—and it was substantial—the working group could not have completed this work in the allotted timeframe.

With the goal of common understanding in mind, the working group developed definitions for vulnerability, the vulnerability lifecycle, and stakeholders, and identified the need for a common scoring process. The NIAC also commissioned a research project last October to develop a common scoring methodology.

The key to effective communication is obviously common understanding and that goes beyond definitions. The working group found that stakeholders use very different methods of reporting and communicating about vulnerabilities, and that there is no consistency in the use of encryption for transmitting information about these vulnerabilities. In the vulnerability discovery community, PGP is most common, but various government agencies and some vendors use other forms of encryption, or none at all.

There is also little consistency regarding procedures to protect sensitive vulnerability information. Vulnerability information must be protected from leaks until users can protect themselves from exploitation. Some stakeholders have no process for protecting against these leaks.

Additionally, consumers and the press often rely on inaccurate vulnerability reports based on anonymous, unauthorized, or bootleg copies of software. Robust information sharing of authorized vendor advisories, through ISACs and other recognized vehicles, must be encouraged.

Finally, the complex legal landscape inhibits communications among stakeholders. Some provisions of privacy protection laws could criminalize legitimate security testing, which is how many vulnerabilities are discovered. Conflicting U.S., state, and foreign laws can cause stakeholders to pause before taking prompt action to manage vulnerabilities.

Mr. Thompson wanted to set these findings in the right context. Again, for common understanding, the working group developed the following definition of a vulnerability: vulnerabilities can be caused by software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or

improvements to current practices. Regardless of cause, the exploitation of such vulnerabilities may result in real threats to mission-critical information systems. The working group recommended universal use of common naming conventions, such as MITRE's Common Vulnerabilities and Exposures (CVE) project.

Mr. Thompson noted that there are a few lifecycle models in use. The working group simplified this into nine primary steps: research; verification; reporting; evaluation; acknowledgement; repair; advisory and patch evaluation; patch release; and feedback and case closure. Each vulnerability is unique, so there will always be variations and overlap between steps. This model provided a solid starting point for dealing with that potential confusion.

Mr. Thompson further noted that there are also many different groupings of stakeholders vitally important to the process. The working group developed four major groups into which others fit: discoverers; vendors; users; and coordinators. As with the lifecycle steps, there is overlap among stakeholder groups—for example, vendors often conduct research, performing the function of “discoverer.”

Among the most important suggestions for all stakeholders are the guidelines for communicating vulnerabilities. Vendor websites should clearly explain how and to whom to report vulnerability, including the use of standardized e-mail addresses and web domains. Consistent communications mechanisms and solid contracts and secure controls apply to all stakeholders.

The remaining guidelines were written specifically to each major stakeholder role.

The working group drew six conclusions.

1. Most discoverers and vendors have the same goal, but approach the problem differently. Some of this disagreement has been based on an environment of distrust—hopefully, the Council's report will help in breaking through this environment and promoting greater trust and cooperation.
2. Mr. Thompson mentioned the need for common terms and procedures. He noted that it should be obvious that this is fundamental to common understanding and a more consistent working environment.
3. No one should be transmitting unresolved vulnerability information in the clear. Wherever possible, such communication among stakeholders should be encrypted and digitally signed. Of course, there will always be “anonymous” discoverers that contact vendors with helpful information—even this should be encrypted. The problem is that the encryption schemes in use (PGP, S/MIME, OpenPGP, and a host of others) are not compatible or universally used. That means only a few of the stakeholders can participate in the process, or that some must transmit vulnerability information in the clear, making it accessible to those who would use it for ill effect.
4. The study group tested several threat scoring methods. While these methods worked for the organizations that developed them and their constituencies, they produced very different results for test vulnerabilities used in comparison. A common scoring mechanism (NOT a common score) could provide the foundation for common understanding of severity, helping all stakeholders to prioritize their actions.

5. Rapid, targeted information sharing is a key to winning the vulnerability “arms race.” This requires robust protection of the information, knowledge of to whom to report and how to prioritize it, compatible encryption schemes, and common awareness of recognized authorities regarding threats and vulnerabilities.
6. Any laws or regulations affecting how stakeholders manage or communicate about vulnerabilities should be reviewed to be sure they enable effective resolution without fear of incurring financial or other liabilities.

At this point Mr. Thompson turned the presentation back to Vice Chairman Chambers, who outlined the working group’s recommendations.

Vice Chairman Chambers thanked Mr. Thompson. He noted that the guidelines apply to all stakeholders worldwide. These seven recommendations are suggested for the President to direct appropriate departments and agencies.

1. It is important to establish a common architecture for handling vulnerabilities. This architecture should be mandated for the federal government and voluntary for all other stakeholders. Federal departments and agencies should adopt common terms and procedures for managing vulnerabilities. They should also use standardized e-mail addresses like “security@agency.gov” and web sites like “www.agency.gov/security” for reporting and communicating about vulnerabilities. They should also include information on how to report, whom to contact, and procedures to follow. In addition, each federal department and agency should:
 - Establish appropriate stakeholder groups in alignment with this report’s guidelines and assist the States to do the same;
 - Promote the use of universal naming conventions such as MITRE’s Common Vulnerability and Exposures (CVE) project; and
 - Support development and use of a universally compatible scoring methodology.
2. The federal government should provide policy and funding to ensure that trusted environments exist to:
 - Ensure the continuous security and integrity of vulnerability investigations in process and manage the disclosure of related information through secured, trusted mechanisms;
 - Protect the confidentiality of vulnerabilities for which no known exploitations have been reported while affected vendors are working toward a solution; and
 - Coordinate the voluntary disclosure of information regarding exploited vulnerabilities to take into account:
 - The risks of damage to the nation's critical information infrastructure;
 - The need for completion of ongoing investigations, and
 - The coordinated release of suitable solutions or remedies for the vulnerability.
3. The federal government can participate in the global vulnerability management process. It should designate a specific office within each participating agency to:

- Review appropriate Federal regulations;
- Define guidelines;
- Act as a clearinghouse to distribute open-source message format standards (such as OpenPGP or S/MIME) that are compatible with current vulnerability management community practices;
- Choose a key validation and distribution system; and
- Provide a profile of which encryption and signature algorithms all federal vulnerability management stakeholders should use.

Widespread use of compatible encryption would have benefits far beyond vulnerability management. All types of incident information being exchanged within and among ISACs, victims of computer crimes, domestic and international law enforcement, and incident response teams would benefit. This kind of standardized infrastructure is key to improving communications that deal with attacks on critical infrastructures, as well as lesser incidents.

4. The federal government should review existing federal regulations and practices in order to identify barriers to resolving software vulnerabilities. Barriers to vulnerability resolution include:
 - Possible penalties for conducting security research and transmitting results to stakeholders;
 - Mandatory informing of individuals regarding inadvertent disclosure of their private information; and
 - Restriction on the use of encrypted e-mail for government agencies.

This review should also include a survey of related international and state laws. Where applicable, the federal government should assist the states by identifying barriers to effective vulnerability management in state statutes, and work with other national governments to ensure harmony of international law with the same goals.

5. The federal government should set up or support a neutral clearinghouse for vulnerability management that is accessible to researchers, the private sector, and federal agencies. Reporting vulnerabilities to the clearinghouse must be voluntary for any non-government entity. This clearinghouse must be able to:
 - Conduct secure and trusted research;
 - Analysis;
 - Remediation support;
 - Disclosure activities; and
 - Work in close cooperation with the private sector entities, including:
 - Information Sharing and Analysis Centers (ISACs);
 - Research companies;
 - Security vendors; and
 - Universities.

The clearinghouse should not supplant direct communication between a discoverer and a vendor. The working group recommends such a clearinghouse as a key node supporting information exchange among industry ISACs and between ISACs and the federal government.

The clearinghouse should maintain a database with references to vendor-supported vulnerability databases, along with recommendations for protection of the databases themselves and for their format and content.

6. Ensure a single point of reference exists for private-sector entities and governments to share information, coordinate efforts, and resolve security vulnerabilities. This should include: establishing a consistent, secure communications means; working with foreign governments and non-government organizations to spread knowledge of common procedures; collaborating in ongoing investigations; and conducting joint research to improve global vulnerability management.
7. The federal government should expand current research funding programs to encourage advanced university and industry research and education into the nature and causes of vulnerabilities, vulnerability management, secure software development, and the coordination and validation of public keys to support an infrastructure for secure electronic mail for all vulnerability management stakeholders.

Vice Chairman Chambers stated that the next step is for the NIAC to approve or modify the report and its recommendations.

He moved on to the topic referred to earlier in the meeting. He reminded the Council that at the meeting in October, the NIAC launched a research group on vulnerability threat scoring. The threat scoring research task is already ongoing. So far, the group has decided on a two-tiered methodology.

- The first tier represents a stand-alone score, which will articulate environmentally independent, immutable qualities, not specific to any site or infrastructure operation.
- The second tier will be a local modification of the standard score, to allow for site or operationally specific circumstances. This score will include provisions and weights for potential loss of life, great economic harm, and other effects not universal across network or computer vulnerabilities.

The group is still working on weights and formulas. It will report its progress at the April NIAC meeting.

Mr. Thompson further stated that the working group believed the guidelines in this report were immediately applicable to several NIAC working group efforts, including:

- Enhancement of Information Sharing;
- Internet Vulnerability Prioritization; and
- Hardening the Internet.

The group also recognized that guidelines like these are not static, so the Council needs to find a home for future updates. Mr. Thompson and Vice Chairman Chambers volunteered to chair a short follow-up task to develop a recommendation for maintaining and updating this framework.

Chairman Davidson said that the two of them had made a tremendous working team and that this was great work.

Finally, Mr. Chambers stated that the working group had two requests. First, approve the working group report and the draft letter of submittal. Mr. Chambers asked the Chairman to open the floor for discussion.

XI. ADOPTION OF NIAC RECOMMENDATIONS NIAC Members

Chairman Davidson thanked Vice Chairman Chambers and asked the Council whether there were any questions or concerns after reviewing the draft recommendations and the letter, other than what had been raised during the presentation.

Mr. Noonan said that he thought Vice Chairman Chambers and his team had done an excellent job—there were plenty of opportunities to provide input and make constructive comments, many of which appear in the final report. He thought they had done a good job in reaching out to a broad, diverse group, including suppliers and vendors, in establishing the framework to effectively share vulnerability disclosure information in an efficient, timely way. He thanked them for their great leadership.

Chairman Davidson said that he would never forget how this group began. There was quite a divergence of opinion. Vice Chairman Chambers said that it was amazing what listening to a number of different resources can do in terms of generating a common goal.

Chairman Davidson said that the presentation was good evidence of a team-oriented effort. Ms. Katen agreed and applauded the effort as impressive—not only is the information sound but also it is also very practical, good advice. Reflecting the global nature of these issues is important. Recognizing the essential interdependence between the private sector and the government in preventing problems and aligning to work together, it reflects well upon the NIAC as a whole.

Chairman Davidson asked if there were any further comments. He then motioned to approve the letter to the President—the motion passed unanimously. Chairman Davidson congratulated the working group. Vice Chairman Chambers said that once again he would like to thank all the members of the working and study groups, as well as all the reviewers that made the work possible. Vice Chairman Chambers asked Mr. Thompson whether he had any further comments. Mr. Thompson said he thought the Vice Chairman had covered everything—he noted it had been a pleasure doing this and it will be even more interesting to see the follow-through as these are implemented.

IX. NEW BUSINESS

Chairman Davidson asked whether there were any other items or issues that came under the heading of New Business that the council wished to discuss.

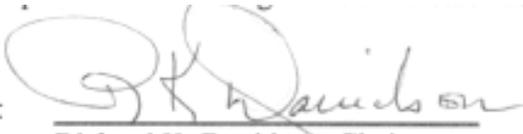
Mr. Dunham asked if the April 13th date for the next meeting of the NIAC was still valid. Chairman Davidson responded that he thought that the date was firm and that the dates set up for the remainder of the year should also be solid. There were no other questions.

Before the meeting adjourned, Paul Nicholas from The White House asked whether he could make one final comment. He noted that there are a lot of federal advisory committees in Washington, but the NIAC is the rare exception where this type of work gets done in the time and the substance intended. He further said that watching the council's deliberations today and seeing the reports that are being forwarded to the President, the council really will make a difference. He expressed the White House's appreciation for the tremendous contributions that everyone involved in the working groups and the principals have made. This is certainly a big step forward. Mr. Nicholas thanked the committee again.

XII. ADJOURNMENT

Chairman Davidson said that it is important that the minutes reflect Mr. Nicholas' comments, especially for those who stepped off of the call because of the Chairman's rush to conclude on time, so that everyone will be advised of them. He stated that the NIAC really does appreciate his comments. Chairman Davidson thanked the attendees once more and adjourned the meeting.

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

By: 
Richard K. Davidson, Chairman

Dated: April 14, 2004

ATTACHMENT A
(Review Of The Role Of The Special Government Employee)



Welcome!

Ethics for the Special Government
Employee

Bottom Line:
Public Service is a Public Trust



Questions You Should Be Able to Answer

- Where do the standards come from?
- How are the standards implemented?
- Where may I find the standards?
- What are the standards?
- Where should I direct my questions?
- Summary



Where do the Standards of Conduct come from?

- Title 18, United States Code, Chapter 11, Bribery, Graft, & Conflicts of Interest
- Executive Order 12,731
- 5 C.F.R. Part 2634 (Financial Disclosure)
- 5 C.F.R. Part 2635 (Standards of Conduct)
- 5 C.F.R. Part 2637 (Post-Government Service Employment)(Revised Part 2641 is forthcoming--68 FR 7,843(amendment at 68 FR 15,383))
- 5 C.F.R. Part 2640 (Interpretation of 18 USC 208)



How are the Standards implemented in DHS

- Secretary appoints head of ethics program, the Designated Agency Ethics Official (DAEO) and an alternate.
Robert E. Coyle, (202) 692-4248
- Many deputy ethics officials
- First-line supervisor of employee whose interests are at issue has been designated the "agency designee" as that term is used in the Standards of Conduct
Melissa Allen



Where Do You Find the Standards

- U.S. Office of Government Ethics–
www.usoge.gov
- Office of Special Counsel –
www.osc.gov/hatchact.htm -
Hatch Act/political activities
www.osc.gov/wbdisc.htm -
Whistleblower



The Essence of the Ethics Program

- The 14 Bedrock Principles – p. 5 of the handout titled, “A Brief Wrap on Ethics.” Three of particular note:
- Public service is public trust
- May not allow improper use of Government information for private gain
- Shall not use public office for private gain



Criminal Prohibitions – during your service

- 203/205 – Representing others to the Government
- 208 – Conflicting interests & affiliations
- 219 – Agent of a foreign principal



18 U.S.C. §§ 203/205

- Prohibits communicating on behalf of another to the Government with intent to influence
- Only in connection with “particular matters involving specific parties”
- Only as to matters you actually participated in for the Government
- Remember § 2635.702--appearances



18 U.S.C. § 208

- Prohibits acting as Government official in matters that will have an economic impact on the official's financial interests or affiliations
- General waiver re your employer



18 U.S.C. § 219

- Prohibits service as a representative of a foreign principal that requires registration under either the Foreign Agents Act or the Lobbying Disclosure Act



43 U.S.C. § 423

- Prohibits disclosing and obtaining certain information regarding procurements
- Requires reporting of employment contacts by an offeror
- It is anticipated that your duties will not involve you in matters covered by this statute



Criminal Prohibitions -- after you leave the Government

- 18 U.S.C § 207 – Restrictions on Communicating



18 U.S.C. § 207(a)(1)

- Prohibits communicating to the Government regarding any “particular matter” involving specific parties that you worked on personally and substantially
- Prohibition last for life of “particular matter.”



18 U.S.C. § 207(a)(2)

- Prohibits communicating to the Government regarding any “particular matter” involving specific parties that was actually pending under your supervision during your last one year of Government service
- Prohibition lasts for first two years after leaving Government
- Should not apply as a matter of fact to your service



Regulatory Standards

- All of the regulatory standards, 5 C.F.R. Part 2635, apply to Special Government Employees, except § 804, outside earned income
- Rules regarding serving as an expert witness (805) and compensated outside speaking, writing, & teaching (807) are substantially narrowed--
those to which actual assigned and personally involved



Regulatory Standards – Gifts from outside sources

- The prohibition on receiving gifts applies fully to SGEs
- The exception that is tailored to SGEs is that permitting accepting gifts based on outside business or employment relationships--
§2635.204(e)



Regulatory Standards—Misuse of position or inside information

- Prohibited from using either for the gain of a private interest—your own or anyone else’s
- You must know whether you are acting as HSAC member or as a private person
- Those you deal with must know the capacity in which you are acting



Fundraising – for nonprofits

- Fundraising means solicitation of cash for nonprofit organizations
- Barred from personally soliciting from those whose interests may be affected substantially by the performance or nonperformance of your duties



Fundraising – for political causes

- You are barred from soliciting contributions--as well as other acts serving political purposes, while you are on Government duty or on Government property



Financial Disclosure

- Questions?



Summary

- Public service is a public trust
- Know in what capacity you are acting/appearing and ensure those seeing/hearing/dealing with you know the capacity in which you are appearing
- Use your official position and official information for authorized official purposes

ATTACHMENT B

*(Status Report on Regulatory Guidance/Best Practice for
Enhancing Security of Critical Infrastructure Industries)*

Regulatory Guidance Best Practices for Enhancing Security of Critical Infrastructure Industries

NIAC Working Group
Progress Report

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

January 13th, 2004
Washington D.C.

1

Presentation Outline

- Review of expected deliverables
- Final Timeline

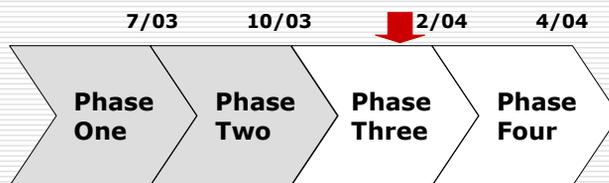
2

Working members

- NIAC Member / Lead Sector Institutions
 - Chemicals: Dupont
 - Finance: Stirling Bank / NASDAQ
 - I.T.: Cisco
 - Water: American Water

- DHS Support
 - Nancy Wong, DHS

Where we are ...



- Define goals
- Survey NIAC opinion
- Gain broad input from 72 institutions
- Draft initial white paper
- Refine white paper with broad sector-led input
- Complete and deliver final white paper for NIAC review

Final Delivery Timeline

- 27th Jan '04
 - Complete broad industry discussions of document
 - Finalize and validate regulatory framework

 - 10th February '04
 - Final input from team members on local sector issues

 - 24th February '04
 - Final edit of consolidated document by team
 - Distribution to key sponsors for review

 - 17th March '04
 - Delivery to DHS for NIAC distribution.
-

ATTACHMENT C
(Prioritization of Internet Vulnerabilities)

NIAC Working Group on Prioritization of Cyber Vulnerabilities

Working Group Update

Martin G. McGuinn, Chairman & CEO
Mellon Financial Corporation

Tuesday - January 13, 2004

1

Presentation Outline

- Background
 - Report on Actions to Date
 - DHS Response
 - What We Need
 - Working Group Purpose
 - Proposed Deliverables
 - Existing Study
 - Vulnerability Assessment Survey
 - Discussion
 - Appendix
-

2

Background

- October 14 – NIAC Members recommend establishment of working group to answer the question – “Are we ranking our critical infrastructures relative to their vulnerability to cyber attacks?”

3

Report on Actions Taken to Date

- Memo to DHS November 12
- Lucent Bell Labs Briefing November 12
 - Dave Picklesimer
- Gartner Briefing December 3
 - Digital Pearl Harbor
- CERT CC Briefing December 12
 - Per request of Amit Yoran
- DHS Response December 18

4

DHS Response

- Clarification of Working Group Purpose
- Identification of similar efforts
 - National Cyber Security Division is producing a matrix of current programs and initiatives underway or completed. This should be available by February 2004
- Guidance on Information Protection
 - Covered under Critical Infrastructure Information (CII)

5

What We Need

- More direction and clarification from the NIAC as to the purpose of this Working Group

6

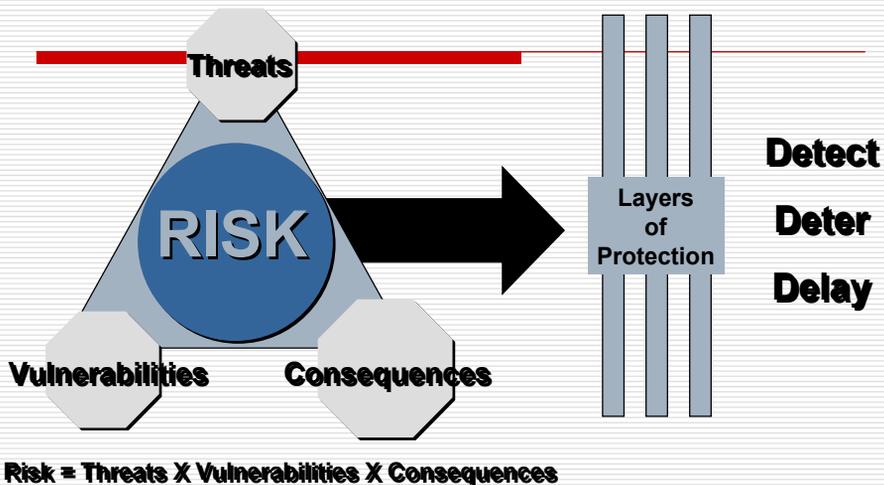
Working Group Purpose

- ❑ Identify the implications/ramifications associated with successful cyber attacks against our critical infrastructures – from both a national security/emergency preparedness perspective as well as the business impact.
- ❑ Rank our critical infrastructures by their vulnerability to cyber attacks.
- ❑ Identify mitigants/protective measures to lessen vulnerabilities.

Proposed Deliverables

- ❑ Summary of the types of Cyber Attacks
- ❑ Summary of implications/ramifications associated with successful attacks based on results of a “Vulnerability Assessment Survey” customized for each critical infrastructure
- ❑ Summary of mitigants/protective measures

Risk Components



9

Existing Study

- Dartmouth College Institute for Security Technology Studies – A National Center for Cybersecurity and Counterterrorism Research, Development & Analysis
 - Cyber Attacks During the War on Terrorism: A Predictive Analysis, September 22, 2001

10

Excerpt from Report¹

- “The specter of an unanticipated and massive attack on critical infrastructures that disables core functions such as telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government systems, and emergency services, has been raised in a number of reports on national security. The degrees to which these infrastructures are dependent on information systems, and interrelated to one another, are still not well understood. Neither is the extent to which these information systems are exposed to outside entry from the Internet.”

¹“Cyber Attacks During the War on Terrorism: A Predictive Analysis”; Institute for Security Technology Studies at Dartmouth College; September 22, 2001.

Excerpt from Report¹, continued

- Banking and financial institutions....
 - ...utilize infrastructures that are vulnerable to cyber attack due to their dependence on networks. However, this sector still operates largely private networks and intranets with very limited external access, thus affording it some protections from external cyber attack.

¹“Cyber Attacks During the War on Terrorism: A Predictive Analysis”; Institute for Security Technology Studies at Dartmouth College; September 22, 2001.

Vulnerability Assessment Survey

- The Working Group may build a Vulnerability Assessment Survey. This risk assessment tool will be validated by member companies of the NIAC as well as working group participants.
- The survey will involve the identification of “Major Players” in each sector (e.g., the top five market leaders in a given sector). Consideration will be given to looking at the top five “known” uses of cyber space for each of these “Major Players”. It will consider the impact on:
 - National Security and Emergency Preparedness,
 - Broad economic or business impacts, and
 - Other significant impacts identified during the analysis.

Discussion

Appendix

□ Working Group Participants

Working Group Participants

□ NIAC Member Institutions and DHS Support

- Susan Vismor, SVP, Mellon Financial Corp., Working Group Chair
- Teresa C. Lindsey, Chief of Staff, BITS
- Peter Allor - ISS
- Bob Bergman, UPS
- Andy Ellis - Akamai
- Bobby Gilham - Conoco Phillips (Also listed as sector coordinator)
- Rick Holmes - Union Pacific Corp.
- Douglas Hurt - V-One
- Bruce Larsen - American Water
- Aaron Meckler - Wells Fargo & Company
- Chris Terzich - Wells Fargo & Company
- Ken Watson - Cisco Systems, Inc.
- Nancy Wong, DHS

Working Group Participants

□ Sector Coordinators

- Kathryn Condello, CTIA, Telecommunications *
- Matthew Flanigan, TIA, Telecommunications*
 - Dan Bart, TIA
 - David Thompson, TIA
- Michehl Gent, North American Electric Reliability Council, Electric Power *
 - Lou Leffler, NERC
 - Dave Nevius, NERC
- Bobby Gillham, ConocoPhillips, Inc., Oil and Gas *
- Ed Hamberger, Association of American Railroads, Surface Transportation*
 - Nancy Wilson, Association of American Railroads
- Rhonda MacLean, Bank of America, Financial Services *
 - Peggy Lipps, Bank of America
- Harris Miller, ITAA, Information*
 - Greg Garcia, ITAA
- Daniel Phythyon, USTA, Telecommunications*
 - David Kanupke, USTA
- Diane Van DeHei, Association of Metropolitan Water Agencies, Water *
- Tim Zoph, Northwestern Memorial Hospital, Healthcare *

* *Accepted to participate to date (or send substitute).*

ATTACHMENT D

*(Final Report and Discussion of the Sector
Interdependencies/Internet Risk Assessment Guidance
Working Group)*

NIAC Working Group on Cross Sector Interdependencies & Risk Assessment Guidance

Proposed Transmittal Letter

Martin G. McGuinn, Chairman & CEO
Mellon Financial Corporation

Tuesday - January 13, 2004

1

Presentation Outline

- Background
 - Report on Actions to Date
 - DHS Briefings
 - Key Issues and Proposed Recommendations
 - Fundamental Principles
 - Appendices
-

2

Background

- April 22 – NIAC Members recommend establishment of working group to:
 - Provide risk assessment guidance based on cross-sector interdependencies and gaps identified in the process.
 - Provide advice and guidance to the President on what needs to be addressed.

Report on Actions Taken to Date

- | | |
|-----------------------------|---------------|
| □ Project Initiation | May 8, 2003 |
| □ Kick-off Meeting | May 14, 2003 |
| □ Progress Report | July 22, 2003 |
| □ Recommendations Presented | Oct. 14, 2003 |
| □ NIAC members review | |
| □ DHS updates provided | Dec. 1, 2003 |
| □ HSPD 7 & 8 issued | Dec. 18, 2003 |
| □ DHS reviews HSPD 7 | Dec. 19, 2003 |
| □ Draft Transmittal Letter | Dec. 24, 2003 |

DHS Briefings

- Briefing on role of Infrastructure Coordination Division – December 1
 - Coordinates with and across sectors
- Briefing on new Homeland Security Presidential Directive 7
 - HSPD 7 - Critical infrastructure identification, Prioritization and Protection
 - HSPD 8 – National Preparedness

5

Key Policy Recommendations:

- Formalize the Public/Private Partnership
- Prioritize Federal Critical Mitigation Activities

6

Formalize the Public/Private Partnership

- Formalize a framework for including private sector in all phases of developing, implementing, and sustaining processes designed to protect
 - Private sector wants to insure the security and resiliency of its strategic assets
 - Private sector needs to be an integral part of the planning process
 - Federal government needs to provide the structure by which private sector can interact – before, during and after an emergency
-

7

The National Incident Management System (NIMS) can provide a framework for public-private critical infrastructure incident management and emergency response.

- HSPD – 5 directed DHS to develop and administer NIMS. NIMS provides a consistent approach for all levels of governments to prepare for, respond to, and recover from domestic incidents.
 - The directive also required development of a National Response Plan. This plan, using NIMS, provides the mechanism for national-level policy and operational direction for Federal support to State, tribal, and local incident managers and for exercising direct Federal authorities and responsibilities.
 - All Federal departments and agencies are required to adopt NIMS. Adoption by State and local organizations is a requirement for Federal preparedness assistance.
 - The current NIMS draft should be revised to include a critical infrastructure role for the private sector to ensure a coordinated and effective approach to emergency planning and crisis response at all levels.
-

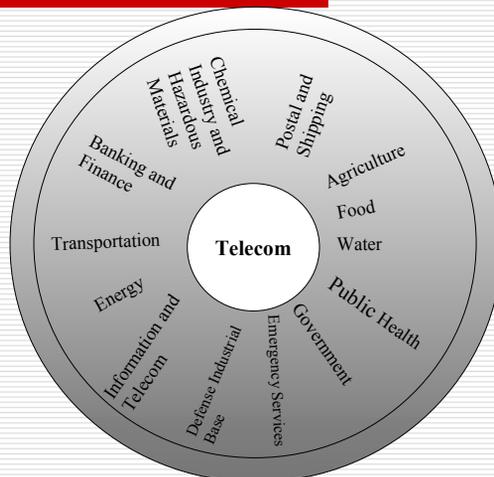
8

Prioritize Federal Critical Mitigation Activities

- Concentrate Federal efforts on those industries on which we are most reliant:
 - Nearly universal dependence on telecommunications to operate other infrastructure components.
 - Energy is necessary for facilities and equipment used in telecommunications to operate.
-

9

Telecommunications represents a “base” infrastructure on which all other sectors depend.



Source: Based on concept designed by Steve Malphrus and Angela Desmond, Federal Reserve Board

10

Fundamental Principles

- ❑ Projects must be structured to provide short-term deliverables to address the most pressing issues in a useful, if non-optimal, fashion.
- ❑ Progress must be monitored to ensure adequate progress is made toward implementing approved recommendations.
- ❑ Partnership between the public and private sectors must be a two-way street in order to evolve to a “trusted” partnership.

Appendices

- ❑ Cross Sector Interdependencies and Risk Assessment Guidance
 - October 14 Proposed Recommendations
 - Relevant portions of Homeland Security Presidential Directives 7 and 8
- ❑ Working Group Participants
- ❑ Deliverables Contained in Report of Proposed Recommendations

1. Inconsistencies exist in the definition of the critical infrastructures.

- Promote organizational consistency using the definitions for Critical Infrastructures contained in the National Strategy for Homeland Security.

 - HSPD 7 - Section 6a
 - The term critical infrastructure has the meaning given to that term in the USA Patriot Act , and referenced in the National Strategy for Homeland Security.
-

13

2. The sector coordinator role is not broadly understood by private industry.

- We support the concept of sector coordination – participating in, coordinating, and supporting private/public and cross sector collaborative efforts.
 - Coordinator role should be defined and publicized to the CEOs, CIOs, and crisis managers of their sectors.
 - HSPD 7 – Section 14
 - Establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors, along with metrics and criteria for related programs and activities.
-

14

3. Crisis Management plans do not exist for each sector and are not tested end-to-end, across the sectors.

- Crisis Management Plans should exist for each sector and be tested.
 - Testing should include cross-sector coordination.
 - Testing and exercising sector crisis management plans should be under the purview of the sector coordinator.
 - HSPD 7 – Section 19
 - Sector-Specific agencies shall conduct vulnerability assessments of the sector, and encourage risk management strategies to mitigate the effects of attacks against critical infrastructure and key resources.
-

15

4. A National Command Center does not exist as a confluence point for the private sectors during times of crisis.

- DHS should establish a virtual command center that provides a call tree, alerting mechanism, and communication point for use by critical sectors during an emergency situation.
 - Each sector should have a seat at the Homeland Security Operations Center.
 - Homeland Security Act of 2000
 - Homeland Security Operations Center (for DHS) and the National Incident Command Center (for IAIP) will provide.
-

16

5. Government sponsored exercises (e.g., TOPOFF2) do not actively solicit private industry representation.

- DHS should sponsor crisis management exercises that include the participation of the critical infrastructures as soon as possible, and annually thereafter.
 - Lessons learned from such exercises should be made available as appropriate and provided to the private sector.
 - HSPD 8 – Section 18
 - Establish a national program to conduct homeland security related preparedness exercises.
 - Develop a system to maintain and disseminate lessons learned, best practices and information from exercises, training events, research and other sources.
-

17

6. There is an underestimation of the dependency of the Nation's critical infrastructures on the Internet.

- Support initiatives to enhance awareness of Internet dependencies, by encouraging the:
 - Private industry to:
 - Adopt security practices
 - Encourage users to keep skills and knowledge current
 - Help educate users
 - Technology Vendors to:
 - Design virus resistant-virus proof software
 - Reduce implementation errors
 - Ship products with high-security default configurations
 - Government to:
 - Provide incentives for higher quality software
 - Support a research agenda that seeks new approaches to software security
 - Encourage more technical specialists
 - Provide more awareness and training for internet users
 - HSPD 7 – Section 22c
-

18

7. Coordination in planning and response between public emergency management and private critical infrastructure is inadequate and/or inconsistent.
-

- Provide a framework for public and private emergency management interaction at the national, sector, state, and regional levels. The framework should integrate with public and private information sharing models and account for Information Sharing and Analysis Centers and InfraGard.
 - HSPD 7 – Section 27
 - Produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources, including a strategy to identify, prioritize and coordinate the protection of critical infrastructure and key resources, including how the government intends to work with Federal departments and agencies, state and local governments, the private sector, and foreign countries and international organizations.
-

19

8. There is a lack of incentives that would help defray the expense burden resulting from strengthening the resiliency of the critical infrastructures.
-

- Consider forming a working group to explore the potential for creating tax incentives or other instruments to incent the private sector to enhance the resiliency of the critical infrastructures.
 - HSPD 8 – Section 8 – 13
 - The primary mechanism for delivery of Federal preparedness assistance will be awards to the states.
 - There may be activity going on in DHS; should be synchronized with any other efforts underway.
-

20

9. Sophisticated modeling capabilities exist at the national laboratories and multiple research and development studies on cross-sector interdependencies have been completed.

- The national labs should focus their interdependency modeling and research on the regions and sectors whose failure would have the greatest impact on the economy and national security.
- The working group suggests modeling the telecommunications and energy sectors, and the interdependencies among them and the other critical infrastructures.
- Existing research and development studies should be indexed and cross-referenced in such a way to make these materials accessible to appropriate parties.
- HSPD 7 – Section 32
 - Use existing and develop new capabilities as needed to model comprehensively the potential implications of terrorists exploitation of vulnerabilities in critical infrastructure and key resources, placing specific focus on densely populated areas. Agencies with relevant modeling capabilities shall cooperate to develop appropriate mechanisms.

Appendices

- Working Group Participants
- Deliverables Contained in Report of Proposed Recommendations

Working Group Participants

□ NIAC Member Institutions and DHS Support

- Susan Vismor, SVP, Mellon Financial Corp., Working Group Chair
- Teresa C. Lindsey, Chief of Staff, BITS
- Peter Allor - ISS
- Bob Bergman, UPS
- Andy Ellis - Akamai
- Bobby Gilham - Conoco Phillips (Also listed as sector coordinator)
- Rick Holmes - Union Pacific Corp.
- Douglas Hurt - V-One
- Aaron Meckler - Wells Fargo & Company
- Chris Terzich - Wells Fargo & Company
- Ken Watson - Cisco Systems, Inc.
- Nancy Wong, DHS
- Eric Werner, DHS
- Clay Woody, DHS

23

Working Group Participants

□ Sector Coordinators

- Kathryn Condello, CTIA, Telecommunications *
- Matthew Flanigan, TIA, Telecommunications*
 - Dan Bart, TIA
 - David Thompson, TIA
- Michehl Gent, North American Electric Reliability Council, Electric Power *
 - Lou Leffler, NERC
 - Dave Nevius, NERC
- Bobby Gillham, ConocoPhillips, Inc., Oil and Gas *
- Ed Hamberger, Association of American Railroads, Surface Transportation*
 - Nancy Wilson, Association of American Railroads
- Rhonda MacLean, Bank of America, Financial Services *
 - Peggy Lipps, Bank of America
- Harris Miller, ITAA, Information*
 - Greg Garcia, ITAA
- Daniel Phythyon, USTA, Telecommunications*
 - David Kanupke, USTA
- Diane Van DeHei, Association of Metropolitan Water Agencies, Water *
- Tim Zoph, Northwestern Memorial Hospital, Healthcare

* Accepted to participate to date (or send substitute).

24

Deliverables

- Critical Infrastructures
 - Critical Infrastructures and Federal Liaison Organizations
 - Matrix of Roles Related to Critical Infrastructure Protection
 - Status of Current Information Sharing and Analysis Centers
- Sector Coordinators
 - Roles and Responsibilities Definition
- Crisis Management Coordination
 - Sector Call Trees
 - Sector Approaches to Security/Crisis Management
 - Railroad, Electricity, and Financial Services Sectors
- National Command Center Presentation Overview
- Government Sponsored Exercises
 - Blue Cascades' Key Findings

25

Deliverables (*continued*)

- Dependency on the Internet
 - Business Impact Survey Questions
 - Excerpts from Testimony of Richard D. Pethia, CERT
- Coordination in Planning
 - Business Incident Coordination System (Example)
 - National Crisis Management Partnership (Example)
- Lack of Incentives
 - Recommendation for a Future Working Group Study
- Research and Development and Modeling Capabilities
 - Matrix and abstracts of Reports on Critical Infrastructure Interdependencies
 - Ranking of Interdependencies by Critical Infrastructure Sector Representatives

26

ATTACHMENT E
*(Final Report and Discussion of the Working Group on
Vulnerability Disclosure)*

NIAC Vulnerability Disclosure Working Group (VDWG)

Final Report and Proposed Recommendations

John T. Chambers
President and CEO
Cisco Systems, Inc.

John W. Thompson
Chairman and CEO
Symantec Corporation

January 13, 2004

1

Presentation Outline

- Charter
 - Methodology
 - Findings
 - Key Guidelines
 - Conclusions
 - Proposed Recommendations
 - Next Steps
 - Requests of the NIAC
-

2

Charter

- NIAC established Vulnerability Disclosure Working Group in December 2002
- Goals:
 - Develop global guidelines for handling security vulnerabilities from initial report to final resolution
 - Derive specific policy recommendations for the President
- This framework covers:
 - Notification
 - Investigation
 - Disclosure
 - Resolution

Methodology

- Formed inclusive Working Group representing all key stakeholder functions
- Conducted extensive literature search for best practices and white papers
- Surveyed WG members to further define problem and articulate stakeholder perspectives
- Developed key definitions and scope
- Wrote, reviewed, discussed
- Conducted two external reviews to ensure broad stakeholder representation
- Submitted final report to NIAC Members on Dec 19, 2003

Findings

- Framework requires common definitions
 - Vulnerability
 - Vulnerability life-cycle
 - Stakeholders
 - Scoring process
- Multiple perspectives are necessary; enrich solutions
- Communication is key to resolution; barriers exist
 - Inconsistent reporting procedures
 - Inconsistent use of encryption
 - Lack of assurance regarding protection of sensitive information
 - Confusion regarding authority of reports
- Legal landscape is complicated
 - Possible unintended consequences of privacy and security laws
 - Conflicting domestic and various national laws and regulations

Key Guidelines

- Definitions
 - Vulnerability
 - Vulnerability life-cycle
 - Stakeholders
- Stakeholders
 - Discoverers
 - Vendors
 - Users
 - Coordinators
- Communications
 - Suggestions for web sites
 - Suggestions for e-mail addresses
- Stakeholder roles and processes

Conclusions

1. Discoverers and vendors often disagree; but not regarding goal of improving security
2. Common terms and procedures are fundamental
3. Compatible encryption schemes are necessary
 - So all stakeholders can participate
 - To protect sensitive information

Conclusions (cont.)

4. Common threat scoring method may build common understanding
5. Robust information sharing is key to minimizing threats to critical infrastructure networks
6. Legal and regulatory frameworks at all levels need review to support secure sharing of vulnerability information

Proposed Recommendations

1. Support development of a common vulnerability management architecture
 - Common terms
 - Universally compatible procedures
 - Standardized e-mail addresses for reporting
 - Standardized web site locations and content

Proposed recommendations (cont.)

2. Provide trusted environments to protect vulnerability information and ongoing investigations

Proposed Recommendations (cont.)

3. Promote universal use of multiple compatible encryption methods
 - enables US Federal government to participate effectively in global vulnerability management process
 - compatible encryption benefits go beyond vulnerability management
 - key to improving communications

Proposed Recommendations (cont.)

4. Conduct a regulatory framework review

Proposed Recommendations (cont.)

5. Support robust voluntary information sharing through policy and funding. Set up or support neutral clearinghouses for vulnerability management

Proposed Recommendations (cont.)

6. Support a robust infrastructure for international coordination

Proposed Recommendations (cont.)

7. Promote and fund advanced university and industry security research and education

Next Steps

- NIAC approve report
- Threat scoring research task ongoing
 - Developing two-tiered methodology
 - First tier represents "base" or "raw" score
 - Second tier allows for site-specific or operational modification of base score
 - Weighted metrics and formula being developed
- Guidelines applicable to other NIAC working group efforts
- Need vehicle for updates

Requests of the NIAC

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