

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING

Tuesday, October 14, 2003
2:00 p.m. – 4:00 p.m.

AGENDA

- I. OPENING OF MEETING:** Nancy J. Wong, *U.S. Department of Homeland Security (DHS)/Designated Federal Officer, NIAC*
- II. ROLL CALL:** NIAC Staff
- III. OPENING REMARKS:** *General John A. Gordon (USAF, ret.), Assistant to the President and Homeland Security Advisor, Homeland Security Council;*
Robert P. Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection;
Richard K. Davidson, Chairman, President & CEO, Union Pacific Corporation; Chairman, NIAC; and
John T. Chambers, President & CEO, Cisco Systems, Inc.; Vice Chairman, NIAC
- IV. REPORT OF THE WORKING GROUP ON CROSS SECTOR INTERDEPENDENCIES AND RISK ASSESSMENT GUIDANCE:** *Martin G. McGuinn, Chairman & CEO, Mellon Financial Corporation; NIAC member*

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

Meeting Minutes and Briefing Materials for October 14, 2003 Meeting

Page 2

V. STATUS REPORTS ON PENDING INITIATIVES:

- | | |
|--|--|
| A. Vulnerability Disclosure Guidelines: | <i>Vice Chairman Chambers; and
John W. Thompson, Chairman & CEO,
Symantec Corporation; NIAC member</i> |
| B. Evaluation and Enhancement of Information Sharing and Analysis: | <i>Thomas E. Noonan, Chairman, President
& CEO, Internet Security Systems, Inc.;
NIAC member</i> |
| C. Regulatory Guidance/Best Practices For Enhancing Security of Critical Infrastructure Industries: | <i>Karen L. Katen, President, Pfizer
Global Pharmaceuticals and Exec. V.P.,
Pfizer Inc.; NIAC member</i> |

VI. NEW BUSINESS: *Chairman Davidson, NIAC members*

A. Questions Posed by President Bush:

1. Are we ranking areas vulnerable to cyber attacks?
2. What can we do to make the Internet harder?

B. New Items

VII. ADJOURNMENT

MINUTES

NIAC Members attending via Conference Call

Chairman Davidson, Vice Chairman Chambers; General Gordon; Mr. Berkeley; Ms. Grayson; Mr. Holliday; Ms. Katen; Mr. Martinez; Mr. McGuinn; Mr. Nye; Ms. Ware; Dr. Rose; Mr. Carty; Mr. Conrades; Mr. Kovacevich; and Mr. Webb.

Staff Designees Monitoring Proceedings on behalf of absent NIAC Members:

David Rose (for Mr. Barrett), Bobby Gillham (for Mr. Dunham), Tom Bergman (for Mr. Weidemeyer); Tom Lockwood (for Governor Ehrlich), Ed Ternan (for Mr. Hernandez) Scott Blanchett (for Ms. Marsh); Peter Allor (for Mr. Noonan); Paul Morrell (for Commissioner Kelly) Rob Clyde (for Mr. Thompson); and Bob Nabors (for Mr. Edmonds).

Members Absent:

Chief Gallegos

Other Dignitaries Present:

U.S. Government: General John A. Gordon (USAF, ret.), Assistant to the President and Homeland Security Advisor, Homeland Security Council, the Honorable Robert P. Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection, DHS; Ms. Nancy J. Wong; Ms. Cheryl D. Peace; Mr. Tom Falvey; Mr. John Gaynor

Others: Mr. F. Duane Ackerman, Vice Chairman of the President's National Security Telecommunications Advisory Council;

I. Opening of Meeting

The meeting was called to order and formally opened by Ms. Nancy J. Wong, Director of the Office of Planning and Partnerships for the Information Analysis and Infrastructure Protection Directorate and Designated Federal Officer for the NIAC. After introducing herself and welcoming Chairman Davidson, NIAC members and their staffs to the sixth meeting of the NIAC, Ms. Wong welcomed representatives from other cabinet departments, Federal Offices and the members of the press and public on behalf of the Department of Homeland Security. Ms. Wong reminded the members that the meeting is open to the public and, therefore, care should be exercised when discussing potentially sensitive information. Ms. Wong then asked Mr. Eric Werner of the NIAC Staff to call the roll to identify all present NIAC members. After completion of the roll call Ms. Wong called to order the sixth meeting of the NIAC.

II. ROLL CALL

Mr. Eric Werner takes roll.

III. OPENING REMARKS

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

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

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

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

Ms. Wong noted that the NIAC has many issues presently under consideration—significantly the matters of Cross Sector Interdependencies and Risk Assessment processes, both of which will be addressed this afternoon. Ms. Wong then turned the meeting over to the Honorable Robert J. Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection.

Assistant Secretary Liscouski began by thanking Ms. Wong, the NIAC and by extending the greetings of Secretary Tom Ridge and Under Secretary Frank Libutti. Assistant Secretary Liscouski then recognized the other Federal officials joining in on the meeting—General John Gordon, the President’s Homeland Security Advisor, and Ms. Cheryl Peace, who oversees Cyber Security issues for the White House Homeland Security Council and affirmed the importance that the President places on Cyber Security and the work of the NIAC. Assistant Secretary Liscouski expressed appreciation for the Homeland Security Council’s continued participation in the NIAC Meetings as well as their expressed interest in the working groups of the NIAC. This sustained contribution reflects the priority the President places on the issues and also reflects the coordination between the White House and the Department of Homeland Security, essential for effective policy making.

Assistant Secretary Liscouski also acknowledged other attending representatives from DHS—Tom Falvey, representing the staff of the National Security Telecommunications Advisory Committee, and Jeffrey Gaynor from the Secretary Ridge’s Homeland Security Advisory Council. Like the NIAC, both of these bodies are doing important work in areas touching upon and complementing the work of both the NIAC and one another. Facilitating more effective collaboration between these high-level advisory panels is a crucial way in which the Information Analysis and Infrastructure Protection Directorate (IAIP) of DHS can carry forward its mission involving critical infrastructure protection.

Assistant Secretary Liscouski then began to touch on the Council’s high level of engagement on various critical infrastructure protection issues, including those issues originally brought forward

by Ms. Wong in opening the meeting. The sweeping scope of these issues represents touchstones for Critical Infrastructure Protection policy.

Significantly, the Council will receive the report from its Working Group on Cross-Sector Interdependencies and Risk Assessment Guidance. Effectively managing interdependencies among critical sectors, not only from an advance planning perspective, but also during crisis response, is one of the greatest challenges facing the DHS in critical infrastructure protection. Mr. Liscouski was aware the working group's report represented five months of intensive work and incorporated contributions from many sectors represented by the NIAC and many representatives from the critical infrastructure Sector Coordinator community. Assistant Secretary Liscouski anticipated with great interest hearing both the report's findings and the working group's proposed recommendations. The Assistant Secretary then turned the meeting over to Chairman Davidson.

Chairman Davidson thanked Assistant Secretary Liscouski; he agreed that infrastructure protection is very important work and that examining interdependencies between various critical infrastructure companies was a Herculean effort. He thanked Mr. McGuinn for having the wherewithal to take on such a large task. Chairman Davidson went on to assert that any doubts or misgivings about the undertaking's pertinence should have been dispelled with the third quarter's events, namely the blackout across much of the United States' Northeastern corridor and the Blaster virus--the impact of these events were made evident throughout a large number of companies. For example, one of the nation's Eastern railroads had its signal system crippled by the widespread power outage, disrupting the flow of goods and general business between the East and West. The Blaster virus also directly affected another Eastern railroad--had the situation not been quickly fixed, the effects could have cascaded down through the system, wreaking even greater havoc. These events are true measurements of the degree of interdependency between Critical Infrastructure firms and are testaments to the value of the work being done by the NIAC. Some suggestions, such as closer cooperation between the Department of Homeland Security and the private sector to revamp the Emergency Response System are items that the Council really needs to begin moving forward with. Prior to starting on the business of the meeting, Chairman Davidson recognized and thanked Mr. Ackerman, the Vice Chairman of the National Security Telecommunications Advisory Council for joining this Council on the conference call; it has been made clear that everything involved with effectively operating a Critical Infrastructure business is directly tied to having a world-class telecommunications system. Chairman Davidson went on to welcome Vice Chairman Chambers, inviting him to make some opening comments as well.

Vice Chairman Chambers congratulated the working group on the quick yet thorough tasks they have completed; he said the four topics are very difficult and the NIAC and its members agree that the working group has put forth a high quality product. In light of recent threats to Internet-dependent infrastructure, the timing of these reports could not be any more appropriate. The Vice Chairman also applauded the Department of Homeland Security's use of technology--linking members in distant locations via teleconferencing and enabling the meeting itself. He challenged the members of the NIAC by asserting that the Council is entering the most serious phase of their work. With the presentation of the final report of the Interdependencies Working Group, it is the NIAC's responsibility to digest the material and formulate policy

recommendations to the President, considering both national and economic security. The Vice Chairman then closed his opening comments and turned the floor back to Chairman Davidson.

Chairman Davidson thanked the Vice Chairman and pushed into the working group's report, headed by Mr. McGuinn.

**IV. REPORT OF THE WORKING GROUP ON
CROSS SECTOR INTERDEPENDENCIES AND
RISK ASSESSMENT GUIDANCE:**

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

Mr. McGuinn thanked Chairman Davidson, his colleagues participating in the NIAC Working group and several critical infrastructure Sector Coordinators who also agreed to contribute to the working group. Mr. McGuinn also expressed his gratitude to Mr. Chris Terzich of Wells Fargo and Ms. Teresa Lindsey from BITS, both of whom were heavily involved with and provided a great deal of support for his colleague, Ms. Susan Vismor, Chair of the Working Group. Mr. McGuinn then turned the meeting over to Ms. Vismor to walk through the presentation in greater detail.

Ms. Vismor thanked Mr. McGuinn and then went on to outline the goals for her presentation—reviewing an abstract of the working paper provided to all attendees, the general background of the project, the working group's methodologies, key issues, recommendations and proposal of next steps in the process.

At the April meeting, a working group was established in order to provide risk assessment guidance based on cross sector interdependencies and risk assessment approaches; the group identified gaps within the process. The group initially struggled with the enormity of the task and considered building a cross-sector tabletop exercise to model interdependencies across infrastructures. However, with clarification from the DHS Secretariat, the working group determined that the group should focus on issues at the policy level. With that direction, the group was able to leverage its business perspectives and focus on capturing policy level recommendations with practical, short-term deliverables. Invitations to join the working group were sent out in May, targeting both NIAC Members as well as critical infrastructure Sector Coordinators. Mr. Terzich provided an update in July and today the working group will put forth its final recommendation.

The working group met in weekly teleconferences. The first step was to ask DHS to provide an inventory on existing studies—the group was pleased to see that there were already 37 studies existing in the public domain. After reviewing the research, an abstract was created and is included in the working report distributed to the members of the NIAC. It is clear that there has previously been a large body of work in this area.

After the July 22nd Meeting of the NIAC and the review of these studies, the working group met with the Director of the DHS Homeland Security Operations Center, Matthew Broderick, John McClaren from DHS/IAIP, Jeff Gaynor, supporting the Common Lexicon Project at the Homeland Security Advisory Council of DHS, and Phyllis Scheck, Infragard's National Executive Board Chair. The group also invited Sector Coordinators to share their sector-specific incident response plans and received briefings from Lou Leffler of the North American Electric

Council (NERC), Nancy Wilson of the American Association of Railroads, Peggy Lipps from Bank of America and Teresa Lindsey of BITS, Ms. Lipps and Lindsey to describe the financial services industry's Incident Recovery plan. Based on the working group's research, the prospect of modeling interdependencies was estimated to be a multi-year, multimillion-dollar effort. For example, a Department of Defense and Emory University-funded project called the Complex Interactive Network Systems Initiative is a five-year, \$30 million study that began in 1999 to examine this issue. Consulting with DHS, the working group determined that this type of effort was beyond the scope of the Advisory Council itself. The group determined that the best way for it to add value was to improve the Cross-Sector Crisis Management Process; regardless of the actual event, any large-scale event is going to require the ability to recover across all sectors.

To that end, the working group identified nine issues and recommendations that can bolster Cross-Sector Crisis Management Coordination.

During the review, the working group was also struck by the slow progress of many of the projects in the study—the group acknowledges that coordinating national projects is a huge task and, therefore, it is necessary to suggest fundamental principles in order to ensure quantifiable, measurable results.

The Working Group recommended that for each Critical Infrastructure, a consistent organizational structure be installed with a Sector Coordinator, an Information Sharing and Analysis Center and a NIAC representative. This configuration is only a minimal alignment. This resembles structures that Council members have in place within their own firms. A hierarchical structure or organizational chart should be created to cover all of the required major roles and to accomplish the desired critical infrastructure protection objective. A tool for measuring progress might be the use of a Red-Green-Yellow Report constructed to outline the current representation status of various Critical Infrastructures. The color red designates required roles that are presently unfilled; yellow represents a role currently in development and green means that the role is filled. All gaps in this red-green-yellow report should be filled.

1. The group recommends structured projects to provide more short-term measurables to address the most pressing issues. An example would be in the DHS Homeland Security Operations Center, a private sector seat is not planned for two years; the group is aware that logistically it might take that long. In order to implement the project at that level, the group came up with some recommendations for an interim solution.
2. As a deliverable from this meeting, the group will produce a kind of report card for presentation back to the NIAC Members for their use to track the effectiveness of their recommendations to the President, to ensure that progress is being made. DHS has a great vision for working together with the private sector to shore up critical infrastructures' resiliency. .
3. There needs to be a continuing dialogue between the public and private sectors and input must be solicited from the private sector to ensure buy-in and ultimately result in engendering trust between the two spheres. An example of this is how the Treasury Department worked with the financial services industry on the white

papers to strengthen the U.S. financial system's resilience. Treasury solicited private sector input for over a year and met with companies to receive feedback on their white papers. It is the working group's opinion that this was an excellent process between private and public sectors to reinforce critical infrastructures.

4. There needs to be a common, universally recognized definition of Critical Infrastructure. The group was initially asked to provide a common definition of Critical Infrastructure; in looking at the National Strategy For Homeland Security, it became clear that this had already been completed. The USA Patriot Act is cited and Critical Infrastructures are defined as "systems or assets, whether physical or virtual, so vital to the United States, that the incapacity or destruction of such assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters."
5. The second issue dealt with by the working group was private industry's unfamiliarity with the Sector Coordinator role. Sector Coordinators are not viewed as focal points for Crisis Management Coordination within and across the sectors. After the July 22nd Meeting of the NIAC, the working group worked with DHS to see their vision of the Sector Coordinator role. DHS provided this information, based on a previous Presidential Decision Directive and best practices of various sectors. It is included in Chapter Two of the working paper. It also described the Federal Government lead agency's role as Sector Liaison. Sector Coordinators should provide a central conduit to the Federal Government and develop an active understanding of the nation's infrastructure from a strategic level with regard to Critical Infrastructure Protection activity. This includes organizing sector leadership and engagement on infrastructure protection, serving as a coordination point for the sector's owners and operators in discussions with other sectors and acting as a coordination point for the sector with the Federal Government. The group supports the concept of Sector Coordinators with a few modifications: the roles and responsibilities of the Sector Coordinators to be publicized to CEOs, CIOs and Crisis Managers of the private industries within the sectors. In terms of action items, the group recommends the following modifications to the current description of Sector Coordinator.
 - Sector Coordinators need to be identified for all Critical Infrastructures; currently, there are no Sector Coordinators for agriculture, food, chemical and hazardous materials, government, defense industrial base and postal and shipping.
 - DHS needs to create a communications plan to publicize the role of Sector Coordinator and introduce them to their constituents.
 - Each sector should have a consistently appointed and consistently funded Sector Coordinator. At the present time, some Sector Coordinators have full time jobs, as well as serving in this role. Realizing the importance and magnitude of the Sector Coordinator role, the role should be housed within

industry associations, if possible, and be full time. The government should provide grants to each sector to help defray the cost of this resource.

- Each Sector Coordinator should be responsible for ensuring that a Crisis Management Plan exists for their sector.
 - Each Sector Coordinator should provide cross-sector liaisons for their respective sectors—this is a crucial link for expediting recovery time.
6. Crisis Management Plans do not exist for each sector and are not tested end-to-end across the sectors. In much of the private sectors, businesses are required to have Crisis Management processes in place for all critical functions; this includes development and maintenance of Business Recovery plans and the annual testing of these plans. There is a growing realization that these plans need to encompass not only internal processes, but also any dependencies with suppliers and/or customers for end-to-end connectivity. This crisis management discipline needs to be applied to national critical infrastructures.
- In terms of short-term action items, the creation of calling trees as an automated notification system is highly recommended. A call tree should, at a minimum, include sector liaison, sector coordinator and ISAC contacts. In chapter three of the working paper, there are samples of these call trees—right now, it really is a manual process. There is an automated call tree system at Mellon Bank called Communicator, for example—there are call tree automation system products out there.
 - Sector Coordinators should establish virtual command centers with open bridge lines for use in a crisis. This is an 800 number that should be available to appropriate contacts in private industry, including the liaison, coordinators and ISAC contacts for other critical infrastructures.
 - Each sector needs to have a clearly defined recovery plan that can be shared, if appropriate, with other sectors that are users or suppliers of that infrastructure. It is crucial that these plans be tested and validated.
 - Over the long term, a crisis management plan should be developed for each sector. This plan should be annually tested and should include validation of cross-sector coordination. Consideration should be given to establishing common terminology, resource management and communication protocol.
7. There is no National Command Center to act as a private sector confluence point during a crisis. The working group received a briefing from Matthew Broderick, Director of the DHS Homeland Security Operations Center. The Center's responsibilities include maintaining and sharing continuous domestic situational awareness, conducting initial information assessment and threat monitoring to

detect, deter and prevent incidents, and coordinating and monitoring incidents. The working group agreed that this is an important charter; however, when plans to include the private sector within the operational center were proposed, the group was told that this was not possible for another two years. Until plans including the private sector are implemented, the Homeland Security Operations Center should work with the private sector's Virtual Command Center and reach the Critical Infrastructures as appropriate. This can be done through call centers or via some other communication mechanism, it is essential that there be some type of communications mechanism available alerting Sector Coordinators to a crisis situation. If practical, each sector should be assigned a seat within the Homeland Security Operations Center.

8. Government sponsored exercises do not actively solicit private industry participation. In private industry, critical business functions are required to be tested annually and it is recommended that regional cross-sector exercises be held annually in major U.S. cities. Since these exercises are resource-intensive, lessons learned should be made available and shared with the private sector, as appropriate.
 - In terms of action items, it is recommended that DHS devise and sponsors crisis management exercises—lessons learned from such events need to be extrapolated and shared with the private sector, as appropriate. Included in Tab 5 of the working paper is a final report on an infrastructure interdependency tabletop exercise named Blue Cascades. The exercise was conducted by the Pacific Northwest Economic Region and co-sponsored by the U.S. Navy, FEMA and the Canadian Office of Critical Infrastructure Protection. Blue Cascades is a prime example of value added from these exercises, as well as the lessons learned and recommendations. For example, the key findings were that participating organizations, over 70 companies with 150 people participating, demonstrated only surface level understanding of interdependency and little knowledge of the critical access of infrastructures, vulnerabilities and operational dynamics of regional interconnection. Many participants assume their organizations' contingency plans for natural disasters or isolated emergencies would be adequate in responding to terrorist acts and disruptions. Eventually, it became clear that this was not necessarily true. There was minimal recognition of the overwhelming dependency on IT-related resources and the need for contingency plans in the event of damage to electronic systems. It provided additional detailed findings and recommendations that would help strengthen our critical infrastructure protection.
9. Most organizations tend to underestimate their reliance on the Internet. Another finding from the Blue Cascades exercise was that participants had difficulty in situations in which they lost telephone and Internet communication; there were no contingency plans intact to work around the situation. There are different reasons

for this underestimation--organizations assume they have efficient fallback processes to resume operating on a pre-internet business model. Over time, legacy fallback systems are not properly maintained, essentially rendering them ineffective. Another issue is the Internet's susceptibility to viruses and worms. Consequently, there is a pressing need to determine the best line of approach for cyber attacks. Sector Coordinators felt this was an enormous task to ask at the sector level and not one that they could easily do across the sector and consolidate. The working group has provided these same questions to the members of the NIAC so they can think about their respective companies' contingency plans.

10. Richard Pethia, Director of the CERT Coordination Center at Carnegie Mellon, testified before a House subcommittee on how to protect the nation's computers from the threat of worms and viruses. The needed actions can be determined by the answers to three questions:

- What can private industry do?
- What can industry vendors do?
- What can the government do?

In terms of private industry, Mr. Pethia suggested verifying that security practices are being adopted and that senior management supports them to ensure proper resource dedication. People need to maintain their skills and knowledge because viruses continue to advance and it is crucial that people keep pace with programming capabilities, while end users must be educated around proper security practices.

In terms of the technology vendors, Mr. Pethia testified that if there is not enough effort in applying lessons learned guarding against vulnerabilities, the same weaknesses would appear repeatedly. Writing software constraining imported code execution would also retard virus replication. Reducing implementation errors with software flaws would benefit security as well—vendors should fix flaws before they release the product. Vendors should release products with out-of-the-box, high security default configurations in order to prevent non-secure windows from being open at first use. The government can leverage its buying power to demand higher quality software and upgrade the skills of workers buying these products. Also, investing more research on systems and operations techniques would allow software to be better able to survive cyber attacks. The federal government could encourage more technical specialists through scholarships and a Cyber Security Center of Excellence. It can provide more awareness training for end users; developing educational material as well as supporting programs that can provide early training for Internet use.

11. Coordination, planning, and response between public emergency management and private infrastructure owners and operators are inadequate and inconsistent. Referring back to the Blue Cascades research, findings around coordination suggested

that there were no region wide strategies for preparedness or early response coordination within and across sectors and jurisdictional boundaries. Generally speaking, crises occur as regional events. The ability to coordinate within and across sectors and with the government on a local or regional level must be established. In the short term, there is a system called the National Incident Management System (NIMS), a program being developed by DHS looking to establish formal Incident Management protocol throughout the United States. NIMS should be reviewed to ensure private sector's participation, and to provide for the following:

- Identification of private infrastructure within the discussed region or planning area
- Credentialing infrastructure company staff for interaction with the emergency functions
- Providing access for an infrastructure company to return to their site within a disaster area to perform critical operational functions
- Priority designation of resources to aid cross-sector critical infrastructure recovery and reconstitution
- Ensuring no effort duplication between Infragard and DHS.

The FBI-sponsored Infragard includes over 9,000 private companies as members and is more of a local-level, information-sharing mechanism. Due to the information-sharing nature of the group, Infragard needs to be integrated with the ISAC concept. The working group recommended that Infragard be encouraged to provide educational overviews to private firms. In the longer term, DHS should develop a national framework for information sharing and management; while developing, in the short term, a regional component.

12. Another issue is the lack of incentive to defray expenses resulting from strengthening the Critical Infrastructures' resiliency. Clearly, the increase in focus in the resources around strengthening the private sector's companies that comprise the nation's critical infrastructure is an increased expense burden for these firms. A working group should be put together to study this issue—there could possibly be tax or other incentives for these companies to further enhance infrastructure resiliency, beyond what their natural business interests may bear.
13. The final issue surrounds modeling. Sophisticated modeling abilities exist at National Labs and multiple research and development studies on cross-sector interdependencies have been completed. Jon MacClaren provided an overview from the National Infrastructure Simulation and Analysis Center (NISAC)--apparently, most data collected today centers on the West and Northwest regions of the United States. The working group believes that efforts should be focused on regions and sectors whose failure would have the greatest economic and national security impact. The private sector should be brought into these efforts early on to test assumptions while models are still being built.

The reliance on telecommunications is very critical and needs to be modeled. Numerous sectors recognize that dependence on this critical infrastructure requires further study. In the breakout of the different studies, there were eleven sectors covered.

- Energy was studied in twenty-two of the studies
- Water was in six studies
- Telecommunications was in five of the studies
- Transportation was evaluated in three of the studies

Clearly, when looking at the Northeastern power outage of summer 2003, it was obvious that people do have generators. Power supply can be controlled independently for some amount of time. Telecommunications sources cannot be independently managed and, therefore, is one of the most critical infrastructures—it must be modeled and understood. Where appropriate, any and all lessons learned and key findings should be shared with members of the private sector.

14. As for the action plan, the working group recommends focusing efforts on the most critical interdependencies like telecommunications and electricity and then indexing and cross-referencing this research to avoid redundancy.

The working group then presented a sample report card to the NIAC for its use to track the effectiveness of its recommendations to the President. The example is just a sample tracking mechanism that upon initial use would likely be modified to provide information in greater detail. For example, in Item 1, reporting may be broken into various sectors and communicated by sector whether or not these roles are actually filled. The appendix contains the names of working group members. The tabs in the working paper include the following topics as deliverables:

- Critical Infrastructures
- Sector Coordinators
- Crisis Management Coordination
- National Command Center
- Government-sponsored exercises
- Internet Dependency
- Lack of Incentive
- Incident Management Planning

- Research and Development of Modeling Capabilities.

Ms. Vismor then asked the audience if there were any questions.

Chairman Davidson lauded the working group's report as very well done and thoughtful.

Vice Chairman Chambers also congratulated the working group for their excellent work and said that the NIAC would be supportive of all their recommendations. Chambers suggested that as Sector Coordinators are selected, they be allowed to organize their various sectors while the NIAC and DHS encouragement and support. Mr. Ackerman from NSTAC then made a few comments to Vice Chairman Chambers about Sector Coordinators. He indicated that the structure referenced in the report has been in sort of an operational mode from a Crisis Management perspective for a number of years—there is an established National Coordinating Center (NCC) for the telecommunications sector. As the group looks at Sector Coordinators, DHS and the Department of Defense would be directly interfacing with the NCC in the event of a crisis. Mr. Holliday volunteered to assist in organizing his sector and developing a sector coordination mechanism. While USTA, one of the designated sector coordinators for the telecommunications sector, has a useful policy role, it is not clear that in a crisis they could necessarily coordinate the sector—the NCC already does this. As the sectors return and provide feedback to the working group, one may see some diversity emerging from specifics by sector; the overall outline is a good one and processes may be able to be streamlined.

Assistant Secretary Liscouski then joined in, saying he appreciates Mr. Ackerman's comments. It seems there was one component not addressed during the course of the presentation—the Infrastructure Coordination Division, part of the Infrastructure Protection Office for Infrastructure Assurance and Infrastructure Protection. The Infrastructure Coordination Division has actually begun implementing many of the working group's recommendations already. There needs to be a review at some point of the progress of this division so that the working group can be assured of having the most accurate information on moving forward on the recommendations.

Chairman Davidson then addressed Assistant Secretary Liscouski, seeking clarification on what Mr. Ackerman had spoken of earlier— Mr. Davidson had briefly lost telephone contact. He went on to say that it would be very helpful if Mr. Ackerman would formalize this information to his committee for input as well. Assistant Secretary Liscouski summarized Mr. Ackerman's input--the working group identified many items that depend on and may already be covered by IAIP as it rolls out its organization and creates an organizational design for meeting its responsibilities. Many of its recommendations reaffirm the direction that DHS will be taking. Mr. Ackerman picked up on the same theme—for instance, the NCC is the coordination center for Incident Management and the Infrastructure Coordination Division has a similar role for other sectors. Assistant Secretary Liscouski said that he thought that he would be able to respond to some of the working group's recommendations by providing a briefing for the working group on the Infrastructure Coordination Division.

Chairman Davidson asked that all interested parties in the NIAC, NSTAC, and the government would make their input to the working group in finalizing the recommendation. Mr. Ackerman said that he had that understanding and that NSTAC would provide input formally to the NIAC.

Mr. Ackerman told Assistant Secretary Liscouski that the NSTAC would provide input directly back through Ms. Vismor's working group.

Chairman Davidson said that any other members with input on this issue would certainly be encouraged to offer their thoughts on this, as well. He asked who the central contact for this should be. Ms. Wong answered that she or Mr. Werner in the Secretariat's office would act as the collection point for feedback to provide to Ms. Vismor and her working group.

Chairman Davidson said that if there were no further thoughts, he would turn the floor over to Vice Chairman Chambers and Mr. John W. Thompson's representative from Symantec, Mr. Rob Clyde, for their working group status update. Mr. Holliday and Ms. Ware volunteered to assist in organizing his sector and developing a sector coordination mechanism.

V. STATUS REPORTS ON PENDING INITIATIVES

- | | |
|---|--|
| A. Vulnerability And Disclosure Guidelines | <i>Vice Chairman Chambers; and John W. Thompson; Chairman & CEO, Symantec Corporation; NIAC Member</i> |
| B. Evaluation and Enhancement Of Information Sharing and Analysis | <i>Thomas E. Noonan, Chairman, President & CEO, Internet Security Systems, Inc.; NIAC Member</i> |
| C. Regulatory Guidance/Best Practices for Enhancing Security of Critical Infrastructure Industries | <i>Karen L. Katen, President, Pfizer Global Pharmaceuticals and Exec V.P., Pfizer, Inc.; NIAC Member</i> |

Vulnerability and Disclosure Guidelines

Vice Chairman Chambers greeted the attendees in the room. He stated that he was happy to provide a status report on the complex task of disclosing security vulnerabilities--developing a consistent way of thinking about this will benefit everyone that uses computers and networking equipment.

He then said Rob Clyde, Symantec's Chief Technology Officer, would ably present for John Thompson. The presentation will update the NIAC on the working group's current progress, some of the remaining key issues, and presented with a proposal for a related research task.

The working group members include:

- Internet Security Systems (ISS) representing the Information Technology-Information Sharing and Analysis Center
- Computer Emergency Response Team Coordination Center
- Carnegie Mellon University
- Verizon representing the Telecommunications Information Sharing and Analysis Center
- Fannie Mae representing the Financial Services Information Sharing and Analysis Center
- Microsoft representing the Organization for Internet Safety
- Internet Software Consortium (ISC),
- University of California at Davis
- Department of Homeland Security
- Forum of Incident Response and Security Teams (FIRST)
- North American Network Operators Group (NANOG)

The working group has made great strides—they have taken the right approach by including the research community, vendors, telecommunications and other users, and by leveraging their own peers within their group. Balancing vulnerability disclosure needs with real requirements to protect customers is the challenge and primary reason that universally understood guidelines are needed. The group overcame representation deficiencies from the Incident Response and Service Provider communities by involving them in an external review of early drafts—this level of participation appears to be adequate.

The working group also addressed the secure communications issue--different stakeholders in the process use different encryption schemes. Obviously, sensitive communications about threats and attacks must be protected, but compatible ways of protection must be developed.

Developing common threat scoring methodology is an area with room for improvement. The working group examined several methodologies of assessing threat severity and determined that disparate methods yield different results. Later in the presentation, a research project developing a common threat scoring methodology to enhance understanding across various stakeholder communities will be recommended. This effort targets researchers, reporters, vendors, customers, users, and governments. Vice Chairman Chambers then yielded the podium to Rob Clyde.

Mr. Clyde began with briefly reviewing the working group's two main tasks. Firstly, developing guidelines for managing security vulnerabilities for discoverers, vendors, governments, and users around the world is a crucial undertaking. Although there are several approaches to vulnerability management, there is no common one. Vendors and vendor organizations, including Microsoft and the Organization for Internet Safety, have published guidelines that help articulate their role. Coordinators like the Computer Emergency Support Team Coordination Center at Carnegie Mellon have published guidelines, providing assistance from a vendor-neutral coordinator's perspective. Security companies like ISS and Symantec have produced guidelines highlighting the research perspective, and there are numerous articles and white papers looking at the issue from different angles. All of these perspectives have been included in the working group's approach, and the group is developing a decision support framework that embraces all of the perspectives.

Secondly, the NIAC is primarily tasked to develop policy recommendations for the President. Those recommendations are emerging as government's role in the overall process is considered. There will be a comprehensive list of suggestions for the US Government as the project is completed.

The aim of the working group has been to be as inclusive as possible--the group includes a broader perspective than even the NIAC. Additionally, input has been solicited from an even broader group of reviewers representing researchers, incident responders, and network operators worldwide. The feedback has been tremendous, both in volume and quality. The group will not be able to outline everything received during this update, but there are three consistent themes we see in reviewer comments.

Firstly, the reviewers agreed with the draft report that a common scoring method is needed; none of the existing scoring methodologies apply to all stakeholders, and neither did the combined results in the draft report. There is a clear business case for a common scoring method. For example, if a discoverer and a vendor consider an issue to be a major hazard and another vendor dismisses it as unimportant, motivating the second vendor to treat the issue appropriately becomes difficult, and threatens safe handling by the first vendor. With a common scoring method, it would be more difficult for these vendors to disagree.

The communications section states that redundant communications are desired but not always available, affordable, practical, or established worldwide. Encryption is inconsistently applied to incident response communications; the worldwide incident response community uses PGP to encrypt e-mail while government stakeholders use other encryption schemes. PGP is also a legacy standard—newer, scalable encryption like S/MIME may have longer life.

Since the Internet is borderless and its vulnerabilities affect researchers, users, vendors, and governments around the world, reviewers agreed with the global scope outlined by the Working Group. Reviewers also endorse stakeholder roles for both government and industry. Mr. Clyde turned the meeting back over to Vice Chairman Chambers for the next part of the presentation.

Vice Chairman Chambers thanked Mr. Clyde and began his portion of the briefing. The challenge is that everyone wants to share information on vulnerabilities—customers need to know what they're facing and how to protect themselves. However, it is exceedingly difficult to decide when sharing might provoke an attack. This is the most challenging issue the group is addressing. The Working Group is including both sides of this argument, and including many in the research and user communities in additional external review. The aim is to develop a comprehensive decision support process that provides a range of options, depending on issues like severity, potential impact, general knowledge of a threat, and ease of exploitation.

The Working Group established a scoring subgroup to look at various scoring methodologies and develop something that could be commonly used. The scoring subgroup of the Working Group ran a series of past worms, viruses, and software vulnerabilities through existing methodology and showed that they all produced wildly different results. Each of the methods is useful for

their own purposes, but there is not one way of scoring the severity of a threat that everyone understands.

A common scoring method promotes global understanding among all stakeholder groups, and will underpin the rest of the vulnerability disclosure framework. This is such an important issue that we recommend today that NIAC reinstate the Scoring Subgroup of the Working Group to conduct necessary research to develop a consistent, common scoring methodology, reporting its results separately to the NIAC. The Working Group believes this task should take 6 months or less.

It is important to finish the general vulnerability disclosure guidelines, and not wait for a scoring methodology. Recent threats illustrate that we all need a consistent way to manage incidents and vulnerabilities sooner rather than later.

Vice Chairman Chambers turned the briefing back over to Mr. Clyde for him to provide the NIAC the timeline for the rest of the work.

Mr. Clyde continued with the presentation. As we indicated in the July NIAC meeting, the Working Group anticipated that the presented schedule might need to be revised if it received extensive reviewer comment. Indeed it did receive gratifying, strong reviewer participation and because of the volume of reviewer comments, the final draft will be significantly different than the first draft. Therefore the Working Group plans to send the new draft back to the original reviewers for a short second look as outlined in this schedule. We will then incorporate comments from the second review and the proposed document will be sent to the NIAC for review from November 10 to December 5. After this we will make final changes and send the document to the NIAC for final approval. This timeline provides ample opportunity for NIAC members to review, modify, and approve the final product before delivery to the President in January 2004.

Ms. Cheryl Peace of the Homeland Security Council informed the NIAC that General Gordon had arrived and was prepared to go forward with his opening comments. General Gordon was introduced and began his remarks. He said that because of his late arrival, he would keep his comments brief. He said he has appreciated what he has heard over the past few moments as a silent observer. The only thing he sought to add was a sense of urgency that the NIAC clearly already possessed. He thanked Chairman Davidson, Vice Chairman Chambers, and the other members of the NIAC for continuing their important support for the President and for the Department. He also welcomed Mr. Ackerman from NSTAC to this session as well. He said he greatly looked forward to receiving these reports. The NIAC's work is important to the Department and it is important to the President. The General offered his help to make things more efficient or reinforce the sense of urgency already present at this meeting.

Chairman Davidson said that the NIAC appreciated General Gordon's participation in the meetings and it exemplified how important the administration considers the effort. The Chairman asked the Council if any of them had any questions for the General, thanked the General, and then passed the floor back to Vice Chairman Chambers.

Chairman Davidson said, from his vantage, that the interest in projects such as Mr. Chambers' and Mr. Thompson's had accelerated as a result from the recent spread of malicious computer viruses like Blaster. Hackers respond when they recognize vulnerability and that the response time is far more rapid than it was a few years ago when businesses first began dealing with cyber security issues. Vice Chairman Chambers agreed, saying that he sees a quicker focus especially in how vulnerabilities and weak links have been expediently shored up to prevent hacking. As the Chairman alluded, there is about a 48 hour window, depending on the complexity of the vulnerability itself and how easily exploitable it is once people are aware of it.

After being asked for clarification on the reinstatement of the Scoring Subgroup of the Working Group by the Chairman, Mr. Chambers stated that he was not pushing for an entirely new effort but a reconstitution of the old one. He thought that in order to get this done correctly, four to six months of work would be required. There is surprising diversity depending on what each group considers a threat and this will underpin the ways the working group approaches this. Vice Chairman Chambers recommended the reinstatement of this subcommittee group. Chairman Davidson asked Vice Chairman Chambers if he and Mr. Thompson would take this on in addition to the work they have already committed to. Mr. Chambers answered that he is very confident that he could continue the subcommittee and reconvene the working group. He then asked Mr. Clyde if he agreed. Mr. Clyde affirmed the desire to continue on and take on the reconvening of the Scoring Subgroup.

Chairman Davidson asked Assistant Secretary Liscouski if he thought this was a good idea. Assistant Secretary Liscouski replied that he did indeed think this was a good initiative and referred the NIAC to Ms. Nancy Wong and her team to ensure no effort redundancy. IAIP would certainly find the deliverable of assistance to its mission.

Mr. Carty sought clarification from Vice Chairman Chambers on the timelines needed to reimplement the Scoring Subcommittee. Mr. Chambers reiterated that it would take six months starting now to produce a deliverable. There are more conflicting opinions than initially anticipated. It is very important to do this right and to get a number of groups to input into the effort. Vice Chairman Chambers said that the working group would go ahead and complete their tasks, then reform as a scoring group and report those results separately. Mr. Carty was in agreement about getting this done right. Chairman Davidson thanked the Vice Chairman and said the result of some of this research may greatly benefit customers. Mr. Chambers agreed that customers and the service-provider side are a broad group and, therefore, a number of different groups would need to be called upon to provide input for this undertaking. A very healthy give-and-take is expected, but the group is in search of one, universal scoring system that resounds with numerous different groups.

Mr. Maynard Webb offered his assistance on the Scoring Subcommittee—Vice Chairman Chambers accepted.

Chairman Davidson said the next item on the agenda is the evaluation of ISACs. Mr. Noonan, who could not attend this meet will have Mr. Allor present for him. Chairman Davidson passed the meeting over to Mr. Allor.

Evaluation and Enhancement of Information Sharing and Analysis

Mr. Allor stated that as a result of required business travel, Mr. Noonan regretted that he could not attend the meeting. There were four original paths within the full scope of the working group's task; these were broken down into objective focus groups for

- Business models for sharing information
- Financial modeling for financial support of the project
- Information analysis—what kind of information is coming in? How is it analyzed? How is it done from within an ISAC and/or how is it done across sectors
- Dissemination, breadth and coverage

To accomplish the objectives appropriate for the NIAC, an approach was taken to avoid heavy modeling, clearly a task outside the working group's scope. The group looked across several different levels in private industry, ISACs, and the government in order to leverage past work. The group searched for organizations participating in information sharing as well as the specific models used by these groups. Additional information was culled from the GAO, from testimony before Congress, other reports, and other specific research items out there. One of the goals was identifying funding options to make private sector models work better. Upon completion, the working group looks to go to several stakeholders throughout the private sector community, specifically from the ISAC Council, sector coordinators, and the individual ISACs themselves.

The current project team believed that it was currently nearing completion on several of these objective areas, bringing closure to information collection for the white papers, final draft development on the business model, information analysis, and aggregation model. The papers still require additional inputs to complete the final draft, financial models, and the dissemination, breadth, and coverage. The group performed multi-level literature searches to include GAO reports, testimony before Congress, and ISAC reports that involve news articles and other publicly published items. The path is quite complex due to the full range of information sharing within scope. Information from current ISACs and the ISAC Council is still being evaluated with the Department of Homeland Security's support and representation. Additionally, the group intends to gather and examine information gathered from the financial services sector—a study combining the services industry, the Department of Treasury and the Boston Consulting Group on a financial model. Lastly, as Assistant Secretary Liscouski noted, it is crucial to define the roles at DHS that may be performing new functions that may impact the working group's study. This data is to be incorporated into a larger study covering our larger objectives. One of the items the group has identified as a vulnerability for its work is the lack of a common lexicon; people define critical infrastructures and key assets differently. They define ISACs differently and, consequently, work at different levels. The working group is trying to find a way to approach and further define an approach to develop a common language and speak on leveled ground. The next steps would be to finalize input to be completed by the end of the week of October 24 and then draft preliminary assessments for review, comments from various stakeholders including sector coordinators, ISACs, the ISAC Council, and DHS. The entire comment period is slated for an early December conclusion. That will be the working group's final report for ISAC consideration. Mr. Allor then opened the floor for comments and suggestions. He offered himself as a link to any of the members on the working group.

Chairman Davidson stated that either Assistant Secretary Liscouski or the President's Homeland Security Adviser Gordon might be able to help--the DHS' Homeland Security Advisory Council (HSAC) has also addressed the issue of a common lexicon. By leveraging HSAC, there is a possibility of gaining knowledge and short-circuiting the process. Mr. Allor responded that Mr. Werner has already put him in touch with Mr. Jeff Gaynor of the HSAC.

Assistant Secretary Liscouski commented that he thought the group was really on the right track and that he is looking forward to gaining insight from the report. He continued with his comments that as the group was aware, implementing the new IAIP organization in any way by using any gained insight from this study would be very helpful. The organizing is being done on the fly, so if there were room for process improvement, it would be better to incorporate that sooner than later. Mr. Allor thanked Assistant Secretary Liscouski for the input and said that the hardest part was defining all the literature and other items out there, analyzing, categorizing it and then coherently arranging them. Allor thought the group was ready to have others provide additional input and perspectives that may have been initially missed. Mr. Liscouski asked if there was a great deal of crossover between the first group, Critical Infrastructure dependencies, and Mr. Allor's. According to Mr. Allor, the working group was awaiting the report that had just been completed—the working group was aware that the first report was going to impact them; they also believed that the vulnerability disclosure report would also have an impact. The time delay for this report was introduced—because of those dependencies and to account for all of that information and leverage it properly. In short, the other working groups' input is exceedingly important and the group is just now beginning to take that in. They are waiting for it in its final form.

Chairman Davidson again thanked the working group for its presentation, saying that the task is difficult but that the potential for it to be beneficial is there. He steered the meeting towards its next topic—Regulatory Guidance and Best Practices for Enhancing Security of Critical Infrastructure Industries under the leadership of Ms. Karen Katen. Chairman Davidson then introduced Ms. Katen and thanked her for attending the meeting.

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

Ms. Katen began her presentation. Since the last NIAC Meeting, as mentioned by Mr. Davidson, problems created by the electrical grid failure in the Northeast and the Blaster virus has shown exactly how interconnected and interdependent the national infrastructures really are. These events served to remind the NIAC just how important their work actually is and speaks to the urgency of the task. In this meeting, there is a plan to report back on the Regulatory Sub-team's progress, in support of this committee's goals. Ms. Katen reminded the group that at the last meeting, as discussed in length, that the appetite and the perception of the regulation varies widely even among members of the working group. Ms. Katen began by pointing out that change is already happening as awareness of infrastructure risks increase. Public and private sector organizations are responding within their own organizations and across industry and sector boundaries. These changes are driven by the need to secure their own organizations and protect business relations with customers and trading partners.

The question now is whether or not these changes will be sufficient. The NIAC asked the working group to review the role of possible government regulation in expediting a more effective response. At prior meetings, the group discussed the need to assess the impact of focused regulation, raise awareness on the scope of regulation to mitigate risk, and identify the most effective drivers of security improvement. The key messages Ms. Katen aimed to leave the audience with were:

- This is an immensely complicated issue playing out differently in different sectors and subsectors as a result of very complex market dynamics and legacy regulatory environments.
- Blanket recommendations are likely to be ineffective at best and potentially damaging.
- There is a marked need to tread carefully and to be judicious.
- While market forces remain the most powerful force for effective change; targeted regulation can actually increase an institutions' ability to drive better solutions.
- In some sectors, intelligently applied regulatory change is likely to be a part of the answer.
- There have also been many instances uncovered that point to regulation doing more damage than good. Consequently, when markets are not yet operating efficiently, the question should not be what does government need to do but can regulation improve the situation and, if so, what best practices and past experiences can be used to guide the effort?

The last time the working group reported to the NIAC on the need for regulation in general terms and principles, and in several sample sectors. Since then, the group has done extensive additional analysis on this subject. In addition to discussions with many NIAC members, a much broader information-gathering exercise has been conducted. In total, there has been input from 74 different institutions and industry associations. The group further reviewed existing studies on cyber security and regulatory efforts in many of the critical infrastructure sectors. In particular, there have been coordinated deep dives into the issues surrounding the financial services and IT sectors. These were chosen because they are very different challenges—one is an established sector with a complex mesh of working regulatory bodies, and the other is an emerging sector where entrepreneurship and the freedom to innovate are highly prized. Only top-level findings are being presented today. The working group needs to consider how different recommendations may operate at the sector level so that the subtle interactions of markets and regulatory guidance can be properly addressed. Ms. Katen thanked Mr. Jonathan White from Pfizer who did most of the coordination of this very extensive research project. In summary, the analysis of the existing information has led to four key findings.

- A deep understanding of sector dynamics is required before action can be taken.
- Organizations are already responding to both competition and cooperation to address the issue of critical infrastructure protection
- Government regulation may still be selectively required
- Best practices do exist for government involvement, and the working group has identified these

Now the group will examine each of these practices in turn.

The need for regulation is different both within and across sectors because of differences in structure, market forces, and existing regulations. For example, the water sector is composed of local, largely independent monopolies with comparatively weak market forces. The financial services sector is an interconnected, competitive sector with strong market forces and preexisting regulations. Even within sectors there is great diversity. Like financial services, banking institutions are constructed as interconnected networks that are regulated at the Federal level whereas insurance companies are structured more independently and regulated at the state level. Securities firms are different yet again—given the extensive differences of cost within sectors, any proposed regulation would need to be designed and enforced at the most appropriate level and through the most effective agency. All NIAC Infrastructure sectors are, by definition, critical.

There are still differences in the impact of a failure. A failure in the electricity subsector can quickly impact multiple industries. Damage to a key payment system within the Federal Reserve Bank can have significant more systemic impact than damage to a small regional bank. Sectors or subsectors are critical nodes that certainly warrant higher security standards. In defining where to focus, it is essential to consider the impact of an attack on an individual player, the impact on other players within the sector, and imperatively, how the sector's damage impacts other sectors. This requires a deep understanding on both industry specific issues and of the interdependencies of the system. In all the sectors examined, a combination of market forces, government-led initiatives, and existing government regulations drive security behavior. Market forces are the most pervasive drivers of change within critical infrastructure protection, both within and across sectors. The effects of the market forces are non-uniform and hinge upon several factors—

- Are customers willing and able to switch providers based upon the providers' security? A bank's customers may well leave if an account's security is threatened or personal information is compromised. In contrast electrical utilities customers probably have few options. A chemical company's may not feel at risk from suppliers' security issues, but in most cases, they would have alternative supply sources.
- Peer pressure within the sector drives security concerns. In some sectors, especially financial transaction processing, people conduct security audits of potential partners to ensure that no security gaps exist that could cause their own systems to become more vulnerable.
- Are attacks expected within the sector? Banks expect thieves and take the needed precautions to prevent theft, pharmaceutical firms and information technology companies routinely expect hackers to target them and attempt to steal intellectual property—they take measures guarding against that. But even when incentives exist, it still depends on the ability of a sector to afford security.

In low margin industries and in some public sector institutions, it may be hard to justify new investment in security. In some sectors, sector-led initiatives and regulations were found to be effective in on ramping market forces. Industry groups such as the North American Electrical Reliability Council (NERC) and the American Chemistry Council (ACC) are publishing security guidelines for their sectors, but the strength of enforcement mechanisms can vary. The ACC's guidelines are self-audited while the NERC's can notify the Federal Energy Regulatory Commission of electric companies not in compliance and, therefore, trigger regulatory scrutiny. It is essential to remember that existing regulations exist and may

serve their purpose well. Indeed in financial services, regulation already drives security behaviors effectively and many parts of regulation are seen as of pivotal importance for regulating their system. At the other extreme, there is little regulation in the Information Technology sector, but most interviewees felt that when customers are in a position to switch services in a competitive environment, then market forces will eventually eliminate non-performing suppliers.

In determining the need for government involvement, the balance between impact and incentive should be considered. By impact, it is not simply whether the undertaking is costly to the firm or is locally damaging, but whether it has the capacity to spill and have broader consequences. By incentives, the group means the net effect of today's market forces, sector-led initiatives and existing regulations. The key areas to examine for potential government action are where there is a relatively high potential impact and there are comparatively weak incentives to take preventive action. An example to consider is the water system. A terrorist attack could threaten a city locally or cause systemic effects by damaging cooling mechanisms for electrical generation. Can we really rely on the constant investment of every company if market forces operate at a comparatively weak level?

It would be wrong to speculate on the final recommendations from NIAC at this time, but this is the type of analysis and discussion that should continue to take place in the final phase of this work. Whenever regulation has been introduced, it can be either a positive or a negative force for change. Many respondents pointed to the securities act and follow up legislation on the disclosure of financial information as an example of good legislation that added transparency and improved the operation of market forces—it was seen as a pillar for the stability of nation's financial services industry. Regulation can, however, be dramatically restrictive as well. FDA regulations that require pharmaceutical manufacturers to document and test all changes in process control systems, for example. This may cause some manufacturers to be disinclined to modernize some security systems to introduce better protection, as the process will need to be extensively revalidated. Consequently, before choosing to regulate, alternatives need to be explored, and the potential negative impacts of regulation should be investigated. Pre-screening questions may be useful before resolving to regulate.

- Will market forces continue to work over time? While increasing incentives today may not be strong enough to enhance security, this may change over time, and market changes may bolster companies' self-driven efforts to reinforce security measures. Increased awareness by customers of high profile attacks could drive switching, which would improve security. This driving force emerges within the IT sector.
- Can the sector answer these problems and issues independently without government aid? Sectors may be able to provide their own solutions, sector-wide collective action has been seen in the past as a response to issues. For example, the NERC was created in 1968 by the Electricity industry to promote overall reliability within the electrical system. Recent events notwithstanding, this helped avoid problems for over thirty years. If similar initiatives focus on other sectors, generating widespread participation, this may nullify the need for any regulation.
- Is regulation a valid response, can it be effectively done? It is important to understand and consider the lifecycle phase of the given sector when contemplating regulation.

Immature sectors with rapidly evolving business models, effective regulation is difficult to construct and even more difficult to apply. Conversely, the sectors that are later in their specific lifecycle phases may have more stable environments and, therefore, be more receptive to newly introduced regulations. It is also important to be sure that the regulation can achieve the desired results without also having severe, negative consequences such as stifling innovation—in such cases other options should also be explored.

If regulation is used, interviews have suggested some of the conditions in which government involvement is most likely to prove beneficial.

- Develop regulations in concert with the industry. Strong coordination with the private sector was used to manufacture the FSIC Regulatory Handbook—broadly recognized for its value to the banking industry. Regulation developed through public-private partnership in this way will build on existing best practices, recognize sector-specific rules, promoting a higher degree of buy-in from the sector.
- Mandating outcomes instead of specific actions gives companies full flexibility to achieve their desired results using methods matching their business steps. Regulation requiring specific actions and technologies may become obsolete, inhibit innovation, or produce inefficient business practices. The construction of particular firewalls may initially promote security, but eventually may inhibit security upgrades later on.
- Insuring alignment between state, local and Federal regulations—a problem in the past. With multiple jurisdictions and agencies imposing regulations over a wide range of sectors, there is a marked chance for conflict. For example, larger water systems are required by the EPA to conduct and submit vulnerability assessments. Some states' sunshine laws require public discussions of new assessments to secure funding; vulnerabilities then become public knowledge, exposing states to a greater risk of attack. This is a real consequence of the push for openness and public awareness.
- Evaluate all new and existing regulations through a security filter—roles pertaining only directly to security make up only a small portion of regulations. Other regulations, however, affect security and often in unanticipated ways. For example, EPA regulations limit the amount of fuel or battery backup power that is legally allowed to be stored at a cellular phone tower. During electricity outages, backup power is limited, causing the rapid loss of the mobile phone networks. Many items within the private sector depend upon the restoration of those services. Without some check on security implications, well-intentioned regulations may have unintended security consequences.
- It is exceedingly important to incorporate flexibility and sunset provisions. With the rapid pace of change today, regulations can quickly become obsolete. Incorporating flexibility by implementing sunset provisions such as where rules must be renewed on a regular basis, assure that the regulation remains relevant.
- Some funding may be necessary to fulfill government mandates. Unfunded mandates are a special concern in the public sector. Voters at a local level may not be willing to fund improvements if regulations are not being applied. Furthermore, costly regulations without the means allowing for the recovery of those costs, such as higher prices, will not be implemented. In some instances, the government could consider providing incremental funding to meet the mandate. There are precedents within the EPA-mandated vulnerability assessments for large water systems—improvised incremental

funds are used. In this way, large systems would not be adversely affected relative to smaller ones.

- Regulation must be implemented in phases. Depending on the scope of new regulation, implementing all provision may place a weighty burden on the industry made to comply and the agency responsible for enforcing regulation. Gradual implementation allows the industry to prepare and spread out the necessary capital investments; for example, fuel efficiency standards were implemented gradually, being increased steadily over the years, which allowed the industry more time to adjust production and develop new technologies.

A few early findings were generated by the working group's research. One of the key findings that came to light was that there is a marked need to engender a deeper understanding of sector dynamics. As mentioned before, organizations are already taking the initiative to address threats but government action and intervention may nevertheless be selectively required. Also, whenever regulation is used, identified best practices should be considered.

In order to fully accomplish the goal of determining regulatory guidelines and best practices for enhancing homeland security, there must first be a deep understanding of sector dynamics. In varying sectors, there are obviously differing structures, market forces and existing regulations. Even going beyond intersector differences, there are even dissimilarities within sectors. A possible remedy is proposing regulation to be designed and enforced at all appropriate levels using the most effective agency. Additionally, within and without sectors, there are discernible differences in the potential for systemic failure. So as to protect against catastrophic system-wide failures, the system's critical nodes must meet higher security standards. Any terrorist attack or other kind of failure, may extend beyond individual firms depending on the degree of interdependency

In order to be sure they themselves are protected from any form of attack, organizations have been forced to take a proactive stance on securing their own resiliency. Market forces tend to be the most pervasive drivers of behavioral change because of direct competition for customers, general peer pressure and the overriding desire for firms to secure themselves against any form of damage. For the most part, many of these sector-led initiatives catalyze improved security behavior and currently existing regulations are strong drivers of behavior in certain sectors.

Prior to governmental regulation, three essential principles must be considered. The working group identified best practices to leverage when regulation will be used. It is of the utmost importance to develop all regulations with the specific sector's industry. Success will be far more likely if outcomes are mandated, as opposed to specific actions. It is key to ensure proper alignment between federal, state and local regulations. All new and existing regulations must be evaluated through a security filter. Flexibility or sunset provisions must be incorporated. Obviously, with all of these changes potentially afoot, some outside funding may be needed to fulfill mandates. The only way to make regulation stick is to implement regulation in phases.

As the working group steadily continues its process, there are some next steps that have been identified that should pave the way for a smooth road all the way to completion. Firstly, it is key that the working group be more representative for the next phase—to do this, it is necessary that

the NIAC members seeking involvement in this project make their voices heard and that non-NIAC members are also identified and participate, as appropriate. It is absolutely critical that the group agrees on overall timeframe and deliverables.

Ms. Katen stated that she hopes her summary has given some insight into the issues involved and the complexity of the issues. In the final phase of this work, the interplay of market forces and regulations will be studied in different sectors and discuss where different regulations should be sector-specific or a general application across critical infrastructures as a whole. Extended working groups will be assembled to conduct these discussions and the working group is interested in getting the Council's further involvement as NIAC members. Ms. Katen asserted that the working group hopes to reach out to the Council over the next few weeks, encouraging the broadest possible discussion and debate on these issues within and across sectors. Ms. Katen closed her presentation and thanked the NIAC.

Chairman Davidson thanked Ms. Katen and began canvassing the NIAC members sitting in on the call to see if anyone wanted to assist her with going forward in this important study. The following people offered their assistance:

- Vice Chairman Chambers
- George Martinez
- Al Berkeley
- Chad Holliday
- Marilyn Ware

Ms. Katen said she was impressed by the number of volunteers, Chairman Davidson said that everyone is greatly concerned about unintended consequences of regulations. He went on to say that that is a great response and that there was a strong group of blue-ribbon people—he thought it was a tribute to Ms. Katen's leadership.

Chairman Davidson asked Assistant Secretary Liscouski if he had any thoughts from his vantage point. Mr. Liscouski replied by saying that this is one of the more critical areas that DHS is looking at and is trying to get consistency across industries by baking in long term security processes. As the group is well aware, the areas receiving the most attention from everyone are based on finding the best ways to get a good security program out there without being overly onerous on the industry. This is extremely valuable work for the DHS and the Department looked forward to the end product.

Chairman Davidson asserted that this was a very thoughtful piece of work, but he did not originally think it would come to the forefront of the NIAC's efforts, but now it appears to be timely and a good contributory effort by the NIAC to the national interests.

Chairman Davidson thanked Ms. Katen and moved on to the next issue—new business.

III. NEW BUSINESS.

Chairman Davidson began this portion of the meeting by saying that there were a couple of things that were addressed in a meeting at the Roosevelt Room with the President in the July meeting that he wanted to look at. He also canvassed the group for any other items that they felt

needed to be discussed. Mr. Holliday commented that he had noticed that as of yet, there was no chemical and hazardous material sector coordinator; he asserted that if Mr. Davidson would like someone to work on it, he would be more than glad to help. Chairman Davidson thought that that would be a great outcome of the previous conversations in the meeting.

Chairman Davidson went on by saying that many members of the Council were fortunate enough to have been invited to the White House this past summer to talk with the President, a number of the cabinet members, General Gordon, and others to discuss the work the NIAC is undertaking. The President asked a couple of very penetrating questions, Chairman Davidson was not sure he remembered them precisely, but they were essentially:

- Is the NIAC identifying the areas that are most vulnerable to cyber attacks?
- What can be done to make the Internet more secure?

Chairman Davidson asked for confirmation from the rest of the members who had been in the July meeting if those questions were the ones President Bush posed during the meeting. The Council agreed that these were the questions. Chairman Davidson said at this point, the Council had not directly addressed those areas. It seems that if the Council is going to do the work of the administration adequately, the Council should get these two items high on the agenda. Mr. Davidson said the Council had been hired on this job to work on issues exactly like this. He then sought out the group's thoughts on the best way to pursue this.

- Mr. Conrades said that he would be happy to follow up on these two issues and participate in the leadership of a working group to pursue them.

Chairman Davidson asked whether or not this should be looked upon as two separate groups or as one single research team. Vice Chairman Chambers joined in, saying he recommended two groups and perhaps a panel to evaluate preliminary answers for the first question as quick as thirty to forty-five days. He said he is averse to penalizing someone who does a good job, but given the success of the Interdependency and Risk Assessment working group, Mr. Chambers congratulated Mr. McGuinn and asks if he might want to lead this group.

On the hardening of the Internet, there were several points of views. It was seen as a very practical request stemming from the first question. Some believe that the existing best practices followed by vendors and other service providers officially harden the Internet. There may be more new technologies and practices, which can be deployed to help secure the Internet. Again, this is not an issue that any one nation has an influence over. A new NIAC working group effort to consider all the different perspectives would be the best way to approach this. So, breaking them into two pieces seems to be the best idea.

Mr. McGuinn agreed that the questions should be separated into two different efforts and said he would be willing to lead, but with the support from the team. Chairman Davidson thanked Mr. McGuinn for extending himself and again taking the responsibility for a needed undertaking. Ms. Marilyn Ware, saying just to prove how loyal Pennsylvania really was, that she would certainly like to participate with Mr. McGuinn's group. Mr. Maynard Webb offered his support for handling the second question on making the Internet harder—he is not sure that he can lead it, but he can assure strong participation. George Conrades offered his leadership for the group assembled to answer the President's second question. Ms. Grayson mentioned that in the

documents her group is working on, in conjunction with the group Mr. Noonan is leading on Information Sharing and Analysis, the group did have a great deal of information to contribute on sensitive but unclassified information passing through the Internet that might be of some value to this study. Chairman Davidson asked her if she would like to participate with Mr. Conrades. Ms Grayson replied that she would. Vice Chairman Chambers offered his assistance to Mr. Conrades' group and offered a suggestion—several of the groups are providing information that this new group can leverage. Maybe starting this group in January is an appropriate timeframe. Mr. Allor offered that there is a great deal of work still to be done on his working group and it would really aid and support a lot of other work that is going on, especially the Vulnerability Disclosure group and he thought the end product would actually set the stage for these questions to be answered. Mr. Conrades agreed, saying he thought that there would be a lot of information that comes out of the other groups that will aid in resolving these questions.

Chairman Davidson proposed that the team leaders that have so kindly volunteered could perhaps begin assembling their teams. These questions are obviously important since it is not every day that you get a request from the President of the United States. The quicker the groups can push forward, the better. Mr. Conrades agreed, saying he thought that Mr. Chambers' recommendation was anticipating this input-in-parallel and starting the response in January is a good one, as there will be the added benefit of leveraging information from the other groups. Chairman Davidson then asked Assistant Secretary Liscouski if he thought the group is headed down the right track by dividing these tasks up. Assistant Secretary Liscouski thought that the point of convergence with the other working groups was a good one and should be pursued. These are the big issues that are trying to be studied and the more that the group can be forward-leaning on this, the more helpful, it would be. The benefit of having these advisory councils is leveraging a strong knowledge base and great talent on these teams to really make a great deal of progress on these big "think" issues. There are a lot of big think issues that the group in Infrastructure Protection has to consider. He thought this one topic in particular requires a great deal of this thinking. He just wanted to reaffirm this effort and its general importance. Chairman Davidson says that there is no question that within the members of this Board, there are some of the most qualified firms represented in America. With all due respect, a lot of great ideas are generated from private industry and the United States Government has tremendous resources when accessing its expertise. Therefore, a lot of meaningful work should come out of this.

Mr. Conrades then spoke, telling the Chairman that he would take the assignment and get started on a work plan with some of the others. Chairman Davidson again thanked Mr. McGuinn for taking on extra work in addition to the items he already has on his plate. Mr. McGuinn thanked him saying that these efforts built on previous ones and the group would report back with a timetable shortly. Chairman Davidson thanked Mr. McGuinn again and asked the group if there were any more comments before the meeting was concluded. He went on to say the NIAC is a great working group and that it was a pleasure to do business with people of such quality to work these difficult issues.

Chairman Davidson asked Assistant Secretary Liscouski if he had any comments. Assistant Secretary Liscouski said that he would like to thank everyone for their participation, their hard work and their effort—he knew they all had real jobs to do. The government is very grateful to


NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

Meeting Minutes and Briefing Materials for October 14, 2003 Meeting

Page 30

the two groups working together. Chairman Davidson called a close to the meeting and stated that the next one would be scheduled as far ahead as possible so everyone has the chance to get it on their schedules—everyone has priorities to sort through so scheduling would try to be as respectful of that as possible. Chairman Davidson then thanked everyone again and adjourned the meeting.

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

By:  Dated: 1-22-04
Richard K. Davidson, Chairman

ATTACHMENT A

*(Cross Sector Interdependencies &
Risk Assessment Guidance Briefing Materials)*

NIAC Working Group on Cross Sector Interdependencies & Risk Assessment Guidance

Proposed Recommendations

Martin G. McGuinn, Chairman & CEO
Mellon Financial Corporation

Tuesday - October 14, 2003

1

Presentation Outline

- Background
- Report on Actions to Date
- Methodology
- Key Issues and Proposed Recommendations
- Next Steps

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
 - Invitation sent to NIAC members
 - Invitation sent to Sector Coordinators
- Kick-off Meeting – May 14, 2003
- Progress Report – NIAC Meeting – July 22, 2003
- Deliver Proposed Recommendations – October 14, 2003

Methodology

- Formed Working Group comprised of representatives from NIAC member institutions and sector coordinators. The Working Group:
 - Met by conference call every week.
 - Reviewed existing interdependency studies.
 - Received briefings on the following:
 - DHS Homeland Security Operations Center
 - National Labs Modeling Capabilities
 - DHS Common Lexicon Project
 - InfraGard
 - Incident response plans from some critical infrastructures

Key Findings

- Cross-sector crisis management coordination is fundamental to the rapid restoration of critical infrastructure and integral to sustain the public's confidence in those infrastructures.
- We have identified nine issues and recommendations, that can help strengthen cross-sector crisis management coordination.

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 towards implementing approved recommendations.
- ❑ Partnership between the public and private sectors must be a two-way street in order to evolve to a “trusted” partnership.

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.

- ❑ Each critical infrastructure should have:
 - Sector coordinator
 - Information sharing and analysis center (ISAC)
 - NIAC representation

ACTION ITEM: Critical Infrastructures

Sector	Sector Coordinator	ISAC	ISAC Contact	NIAC
1. Agriculture				
2. Food - Meat and Poultry - All Other		Food ISAC	Tim Hammonds Tim Weigner	
3. Water	Diane VanDe Hei - AMWA	Water ISAC	Susan Tramosch	American Waterworks Service Company, Inc.
4. Public Health	Tim Zoph - Northwestern Memorial Hospital	HC ISAC in development		
5. Emergency Services	Dave Christler			City of Albuquerque; City of New York
6. Government		NASCIO	Chris Dixon	
7. Defense Industrial Base				
8. Information and Telecommunications	Harris Miller - ITAA Matthew Flanigan - TIA Daniel Pythyon - USTA Kathryn Dondello - CTIA	IT ISAC Telecom ISAC	Peter Allor Ernie Gormsen Lt. Col. Francis Wentworth	Akamai Cisco E-Bay EDS Intel Inter-Con Security Systems Internet Security Systems Symantec V-One Corporation
9. Energy	Mike Gent - NERC Bobby Gilham - ConocoPhillips	Electric ISAC Energy ISAC	Lou Leffler Bobby Gilham	ConocoPhillips TXU Corp
10. Transportation	Ed Hamberger - AAR Greg Hull - ACI - NA David Plavin - APTA	Surface Transportation ISAC	Paul Wolfe	American Airlines
11. Banking & Finance	Rhonda MacLean - Bank of America	Financial Services ISAC	Suzanne Gorman	Mellon Financial Corp. NASDAQ Sterling Bank & Bancshares Wells Fargo & Company
12. Chemical Industry & Hazardous Materials		Chemical ISAC		DuPont Company Pfizer Global
13. Postal & Shipping				United Parcel Service
14. National Monuments and Icons Education (Not in National Strategy)				

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

- We support the concept of sector coordinators who participate in, coordinate and support private/public and cross-sector collaborative efforts.
- Coordinator role should be defined and publicized to the CEOs, CIOs, and crisis managers of their sectors.

ACTION ITEMS: Sector Coordinators

- ❑ Modify the sector coordinator definition as follows:
 - ❑ Each "Critical Infrastructure" should have a consistently appointed and consistently funded sector coordinator.
 - ❑ The Sector Coordinators should be responsible to insure that a Crisis Management Plan exists for their sector.
 - ❑ The Sector Coordinators should also provide the "cross-sector" liaison role for their respective critical infrastructure.
- ❑ Appoint sector coordinators for critical infrastructures that currently do not have a coordinator.
- ❑ Create a communication plan to publicize the role of the sector coordinator to their constituents.

11

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.

12

ACTION ITEMS: Crisis Management Plans

□ Short-Term

- Create automated calling trees via an automated notification system.
- Each sector coordinator should establish a "Virtual Command Center" via an open bridge line to be used during a crisis.

□ Long-Term

- Develop crisis management plans for each sector
 - Test annually and validate cross-sector coordination
-

13

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.
-

14

ACTION ITEMS: National Command Center

- ❑ Establish a virtual command center that provides a call tree, alerting mechanism, and communication point for use by critical sectors during an emergency situation.
 - ❑ Assign each sector a seat at the Homeland Security Operations Center.
-

15

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.
-

16

ACTION ITEMS: Government Sponsored Exercises

- ❑ DHS devise and sponsor crisis management exercises.
- ❑ Extrapolate lessons learned from such exercises and distribute as appropriate.

17

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

- ❑ Enhance awareness of Internet dependencies, including:
 - Which products are dependent on the internet?
 - How much revenue would be lost if the above product(s) were not available?
 - What customer service products would be unavailable?
 - What internal processing supported applications would be broken?
 - What information/marketing tools would be impacted?

18

ACTION ITEMS: Internet Dependencies

- Private Industry:
 - Adopt security practices
 - Encourage users to keep skills and knowledge current
 - Help educate users
- Technology Vendors:
 - Design virus resistant-virus proof software
 - Reduce implementation errors
 - Ship products with high-security default configurations
- Government:
 - 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

Excerpts from testimony of Richard D. Pethia, Director, CERT Coordination Center 19

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.

ACTION ITEMS: Planning and Response Coordination

Short-term

- Review National Incident Management System to insure inclusion of private sector.
- Resolve any duplicative or competing objectives between InfraGard and DHS.
- Provide overview guide to critical infrastructure crisis management for private companies.

Long-term

- DHS should develop a national framework for information sharing and emergency management.
 - Ensure above model includes a regional component.
-

21

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.
-

22

ACTION ITEMS: Lack of Incentives

- Form a working group to study this issue further.

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.

ACTION ITEMS: Modeling and Existing Research.

- Focus modeling efforts on most critical interdependencies, i.e., telecommunications and electricity sectors.

- Index and cross-reference existing research to avoid redundant efforts.

25

Sample Report Card

Issue #	Action Item(s)	Date Approved	Proposed Completion Date
1	Fill vacant roles in critical infrastructures	1/1/04	
2	Modify sector coordinator definition		
	Appoint sector coordinators		
	Create a communication plan		
3	Created automated calling trees		
	Establish sector virtual command centers		
	Develop crisis management plans		
	Test and validate plans annually		
4	Establish national virtual command center		
	Assign each sector a "seat" at HSOC		

26

Sample Report Card - *continued*

Issue #	Action Item(s)	Date Approved	Proposed Completion Date
5	Devise and sponsor cross-sector exercises		
	Extrapolate and distribute lessons learned		
6	Private Industry		
	Technology Vendors		
	Government		
7	Review NIMS for private sector inclusion		
	Resolve duplicative or competing efforts		
	Provide CIP guidance to private sector		
	Develop national framework for IS		
	Ensure a regional component in IS		

27

Sample Report Card - *continued*

Issue #	Action Item(s)	Date Approved	Proposed Completion Date
8	Form a working group to study incentives to strengthen CIP		
9	Focus modeling on telecommunications and electricity sectors		
	Index and cross-reference existing research		

28

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

Working Group Participants

□ Sector Coordinators

- Kathryn Condello, CTIA, Telecommunications *
- Matthew Flanigan, TIA, Telecommunications*
 - David Thompson, TIA Online
- 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).*

31

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

32

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

ATTACHMENT B

*(Vulnerability Disclosure Guidelines
Briefing Materials)*

NIAC Vulnerability Disclosure Working Group (VDWG)

Status Report
National Infrastructure Advisory Council
October 14, 2003

John Thompson
Symantec

John Chambers
Cisco Systems

Tasks

- Develop global guidelines for handling security vulnerabilities from initial report to final resolution
 - Derive specific policy recommendations for the President
-

Participants

- Working Group Co-Chairs:
 - John Chambers, Cisco Systems
 - John Thompson, Symantec
 - Working Group members: ISS (IT-ISAC), Mitre, CERT/CC, Verizon (Telecom-ISAC), Counterpane, Fannie Mae (FS-ISAC), UC Davis, Microsoft (OIS), ISC, DHS/IAIP
 - Additional feedback and input from FIRST, NANOG, USENIX
-

Reviewer Comments

- Consistent vulnerability scoring methodology will be a key outcome
 - Current methods do not agree—disagreements on threat severity affect handling
 - Consistent scoring would support predictable threat management choices
 - Very difficult problem, but necessary to solve
 - Communications section comprehensive and clear
 - Covers discoverers, vendors, coordinators, governments, users
 - Desired redundancy must be balanced by reality
 - Encryption differences must be resolved
 - Reviewers endorse global scope and public-private partnership emphasis
-

Task Complexity Requires Time to Complete

- Real challenge: balancing desire to disclose with need to protect
 - Developing decision support process
 - Process must include predictability, consequences, wide acceptance, and dependability
 - Meat of the report—most difficult to complete
 - January 2004 delivery
 - Recommend NIAC commission scoring research task to provide common perspective
 - Reinstate scoring subgroup of this WG
 - Conduct research concurrent with this report development—(6-month project)
 - Develop common scoring methodology
 - Report separately, but will support overall framework
-

Next Steps

- Revised schedule:
 - 07/14: First draft reviewed by working group
 - 08/13: External reviewers solicited
 - 08/22: 1st round of external comments received
 - 08/25-09/12: Additional comments and discussion
 - 10/17 External review comments incorporated
 - 10/20-11/03: 2nd external review period
 - 11/17: Incorporate comments from 2nd external review
 - 11/19-12/19: New draft presented for NIAC review
 - Mid-December: Final changes made based on NIAC review
 - Late December: NIAC-approved version delivered to DHS for final printing and preparation
 - Formal presentation to the President in January 2004
-

Comments and Suggestions

- Principal authors:
 - Adam Rak, Symantec
 - Jim Duncan, Cisco Systems
 - Additional contacts:
 - Rob Clyde, Symantec
 - Ken Watson, Cisco Systems
 - Editors' e-mail address:
 - niac-vdwg@external.cisco.com
-

ATTACHMENT C

*(Evaluation and Enhancement of Information Sharing and
Analysis (EEIS) Briefing Materials)*

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

Status Report
National Infrastructure Advisory Council
October 14, 2003

Tom Noonan
Internet Security Systems, Inc.
tnoonan@iss.net

Tasks

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

Background Approach

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

3

Participants

- ❑ Working Group Chair:
 - Tom Noonan, Internet Security Systems, Inc
- ❑ Working Group members: ISS, Wells Fargo, NYPD, EDS, Union Pacific, UPS, Inter-Con Security Systems, V-ONE, NERC, SIAC, ConocoPhillips, Cisco, Symantec, DuPont, US CoC, and IAIP
- ❑ Additional feedback and input to be processed from ISAC Council and ISACs Sector Coordinators

4

Project Status

- ❑ White Papers in final draft development:
 - #1 Business models
 - #3 Information Analysis and aggregation
- ❑ White Papers requiring final input for completion:
 - #2 Financial models
 - #4 Dissemination breadth and coverage
- ❑ Literature Search nearing completion: GAO Reports, Testimony to Congress, Numerous ISAC Reports and News Articles

5

Task Complexity Requires Time to Complete

- ❑ Gathering/leveraging of data from:
 - ISACs / ISAC Council
 - Dept of Treasury and FS ISAC – BCG Study
 - DHS Organization
- ❑ Review and incorporation of data into research
- ❑ Covering a wide spectrum in the four objectives
- ❑ Lack of common lexicon and approach

6

Next Steps

- Revised schedule:
 - 07/24: First draft of Objective White Papers
 - 10/10: Coordinating Draft Objective White Papers
 - 10/14: NIAC Teleconference
 - 10/24: ISAC Council Input – BCG FS Study?
 - 10/31: Final White Papers drafted
 - 10-31: Draft Preliminary Assessment and recommendations
 - 10/05: Start External review period
 - 12/05: Comment Period closed
 - Mid-December: Final changes made based on comments
 - Late December: NIAC-approved version delivered to DHS for final printing and preparation
- Formal presentation to the NIAC January 13, 2004

7

Comments and Suggestions

- Principal authors:
 - Chris Terzich, Wells Fargo
 - Rick Holmes, Union Pacific
 - Margaret Grayson, V-One
 - Daryl Eckard, EDS
- Additional contacts:
 - Peter Allor, ISS
- Editors' e-mail address:
 - pallor@iss.net

8

ATTACHMENT D

*(Regulatory Guidance Best Practices for Enhancing Security of
Critical Infrastructure Industries Briefing Materials)*

Regulatory Guidance Best Practices for Enhancing Security of Critical Infrastructure Industries

NIAC Working Group
Progress Report

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

October 14, 2003

Presentation Outline

- Objectives
 - Methodology
 - Early findings
 - Next steps
-

Objectives

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

Methodology

- ❑ Conducted structured interviews with 14 NIAC member institutions to identify differing perspectives
 - ❑ Conducted wider set of over 70 interviews to further flesh out issues
 - ❑ Developed preliminary findings, including framework that can be applied to sectors
 - ❑ Construct working groups to advance findings, apply framework and create policy options and recommendations for each sector
-

Early findings

- ❑ Deep understanding of sector dynamics is needed
 - ❑ Organizations are already responding to address threats
 - ❑ Government action may still be selectively required
 - ❑ Identified best practices should be considered when regulation is used
-

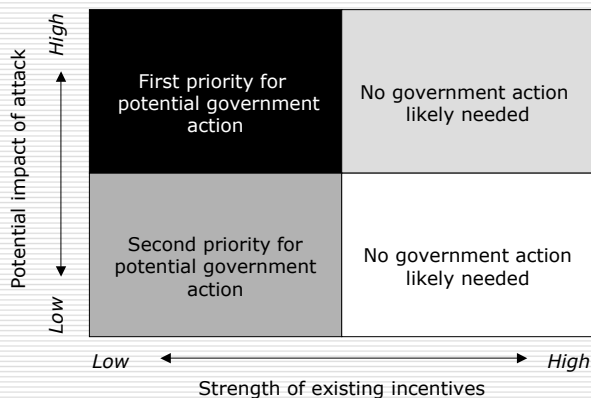
Deep understanding of sector dynamics is needed

- ❑ Different structure, market forces, and existing regulation are present
 - Even within sectors there is great diversity
 - Proposed regulation would need to be designed and enforced at appropriate levels and through the most effective agency
 - ❑ Differences in the potential for systemic failure exist across and within sectors
 - Critical nodes for the system need to meet a higher security standard
 - The impact of an attack may extend beyond individual firms because of interdependencies of systems
-

Organizations are responding to address threats

- Market forces are the most pervasive driver of behavioral change because of:
 - Customers switching
 - Peer pressure
 - Expectations of damage
 - Sector-led initiatives encourage improved security behavior
 - Existing regulations are a strong driver of behavior in certain sectors
-

Government action may be selectively required



Screening questions to consider before resolving to regulate

- Will market forces work over time?
 - Can the sector provide its own solution?
 - Can regulation be successfully applied to this sector?
-

Identified best practices should be considered when regulation is used

- 1. Develop regulations in concert with industry**
 2. Mandate outcomes rather than specific actions
 3. Ensure alignment between federal, state and local regulations
 4. Evaluate all new and existing regulations through a "security filter"
 5. Incorporate flexibility or sunset provisions
 6. Some funding may be needed to fulfill mandates
 7. Implement regulation in phases
-

Identified best practices should be considered when regulation is used

1. Develop regulations in concert with industry
 2. **Mandate outcomes rather than specific actions**
 3. Ensure alignment between federal, state and local regulations
 4. Evaluate all new and existing regulations through a "security filter"
 5. Incorporate flexibility or sunset provisions
 6. Some funding may be needed to fulfill mandates
 7. Implement regulation in phases
-

Identified best practices should be considered when regulation is used

1. Develop regulations in concert with industry
 2. Mandate outcomes rather than specific actions
 3. **Ensure alignment between federal, state and local regulations**
 4. Evaluate all new and existing regulations through a "security filter"
 5. Incorporate flexibility or sunset provisions
 6. Some funding may be needed to fulfill mandates
 7. Implement regulation in phases
-

Identified best practices should be considered when regulation is used

1. Develop regulations in concert with industry
 2. Mandate outcomes rather than specific actions
 3. Ensure alignment between federal, state and local regulations
 4. **Evaluate all new and existing regulations through a "security filter"**
 5. Incorporate flexibility or sunset provisions
 6. Some funding may be needed to fulfill mandates
 7. Implement regulation in phases
-

Identified best practices should be considered when regulation is used

1. Develop regulations in concert with industry
 2. Mandate outcomes rather than specific actions
 3. Ensure alignment between federal, state and local regulations
 4. Evaluate all new and existing regulations through a "security filter"
 5. **Incorporate flexibility or sunset provisions**
 6. Some funding may be needed to fulfill mandates
 7. Implement regulation in phases
-

Identified best practices should be considered when regulation is used

1. Develop regulations in concert with industry
 2. Mandate outcomes rather than specific actions
 3. Ensure alignment between federal, state and local regulations
 4. Evaluate all new and existing regulations through a "security filter"
 5. Incorporate flexibility or sunset provisions
 6. **Some funding may be necessary to fulfill mandates**
 7. Implement regulation in phases
-

Identified best practices should be considered when regulation is used

1. Develop regulations in concert with industry
 2. Mandate outcomes rather than specific actions
 3. Ensure alignment between federal, state and local regulations
 4. Evaluate all new and existing regulations through a "security filter"
 5. Incorporate flexibility or sunset provisions
 6. Some funding may be needed to fulfill mandates
 7. **Implement regulation in phases**
-

Next steps

- Assemble working group for next phase
 - Determine which NIAC members are interested in participating in the working group
 - Identify possible non-NIAC members that are also interested in participating

 - Agree upon overall timeframe and deliverables
-