# NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

# MEETING

Tuesday, April 22, 2003
4:30 p.m. – 6:30 p.m. EDT

***Via Teleconference***

**Access Line for Members of the Public:**
**(Toll free) 1-800-304-8043; (toll) 1-719-955-1038**
**access code 1129948**

# AGENDA

| | | |
|---|---|---|
| **I.** | **Opening of Meeting and Roll Call of Members:** | *Nancy J. Wong*, Director, Office of Planning and Partnerships, U.S. Department of Homeland Security (DHS)/Designated Federal Officer, NIAC |
| **II.** | **Opening Remarks:** | *Robert P. Liscouski*, Assistant Secretary of Homeland Security for Infrastructure Protection, DHS;<br>*Richard K. Davidson*, Chairman, President & CEO, Union Pacific Corporation; Chairman, NIAC; and<br>*John T. Chambers*, President & CEO, Cisco Systems, Inc.; Vice Chairman, NIAC |
| **III.** | **Introduction of Possible Topics for Future NIAC Study:** | Chairman Davidson |
| | **a. Internet Protocol ver. 6 (IPv6):** | Vice Chairman Chambers |
| | **b. Cyber Vulnerability Disclosure Guidelines:** | Vice Chairman Chambers and *John W. Thompson*, Chairman and CEO, Symantec Corporation; Member of the NIAC |
| | **c. Other topics:** | NIAC Members |
| **IV.** | **Discussion of Topics:** | NIAC Members |
| **V.** | **Discussion of Possible Dates for Future Meetings:** | Chairman Davidson, NIAC Members |
| **VI.** | **Adjournment** | |

# M I N U T E S

**NIAC Members present in Washington:**

Ms. Wong; Chairman Davidson.

**NIAC Members attending via Conference Call:**

Vice Chairman Chambers; Mr. Berkeley; Mr. Dunham; Chief Gallegos; Ms. Grayson; Mr. Holliday; Ms. Katen; Mr. Martinez; Mr. McGuinn; Mr. Noonan; Mr. Nye; Ms. Ware; and Mr. Weidemeyer.

Mr. Barrett; Mr. McCarty; Mr. Edmonds; Mr. Hernandez; Mr. Kelly; and Mr. Webb were not in attendance but had staff monitoring the call.

**Other Dignitaries Present:**

Mr. Robert P. Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection, U.S. Department of Homeland Security.

## I. Formal Opening of Meeting

The meeting was called to order and formally opened by Ms. Wong, the Designated Federal Officer (DFO) of the NIAC. After introducing herself and welcoming Chairman Davidson, Vice Chairman Chambers, and all of the members and their staffs to the first meeting of the NIAC under the administration of the Department of Homeland Security, Ms. Wong welcomed the press and the public listening in on the conference line. She reminded the members that this meeting was open to the public and that care should be exercised when discussing potentially sensitive information. Ms. Wong asked Mr. Eric Werner of the NIAC Staff to call the roll to identify the NIAC members participating on the conference call. (*See* list above.) Ms. Wong set forth the agenda and introduced Mr. Robert P. Liscouski, the Assistant Secretary of Homeland Security for Infrastructure Protection.

## II. Welcoming Remarks

Mr. Liscouski thanked Howard Schmidt for his help in guiding the Federal government's efforts to secure cyberspace, first as Vice Chairman of the President's Critical Infrastructure Protection Board and, most recently, as its Chairman. He announced that Howard had recently tendered his resignation as Special Assistant to the President. Mr. Liscouski also introduced Paul Kurtz, Special Assistant to the President and Senior Director for Critical Infrastructure Protection for the Homeland Security Council.

Mr. Liscouski welcomed everyone, on behalf of the Under Secretary, to DHS, and to the Directorate for Information Analysis and Infrastructure Protection (IAIP), and explained how the IAIP integrates for the first time in our nation's history an end-to-end capability to identify and assess current and future threats to the homeland; map those threats against our vulnerabilities; communicate in a coherent and efficient way timely threat and warning information; and prioritize protective measures to prevent attacks, reduce vulnerabilities, minimize damage, and

assist in the restoration of critical services and functions following a crisis event. He characterized as equally important the fact that IAIP will provide a single point of contact for State and local government, and for the private sector, to communicate and coordinate protection activities with the Federal government, including vulnerability assessments, strategic planning efforts, and exercises.

Mr. Liscouski acknowledged the Federal government's recognition that protecting America's critical infrastructure is a shared responsibility that Federal, state, and local government must undertake in active partnership with the private sector. Mr. Liscouski stated that, within DHS, the IAIP Directorate reflects the President's commitment to holding up the Federal government's end of that partnership. He further emphasized that the ultimate effectiveness of these structures, though, depends on effective communication among all of the stakeholders in this partnership, ensuring that those partnerships are robust, and using the time and expertise of the NIAC wisely and in the best possible way we can. He turned the meeting over to Chairman Davidson.

## III. Introduction of Possible Topics for Future NIAC Study

Chairman Davidson thanked Mr. Liscouski. He then introduced the discussion of potential new topics for NIAC study and consideration. He mentioned that the NIAC already had two projects underway: (1) the Task Force concerning the transition to Internet Protocol version 6 (IPv6), headed by Mr. Chambers, and (2) the Working Group on Vulnerability Disclosure Guidance, co-chaired by Mr. Thompson and Mr. Chambers. The Chairman noted that, since the last meeting of the Council, a number of the members had submitted suggestions for additional topics that they considered to be worthy of study. Mr. Davidson stated that these recommendations were reviewed to isolate points of commonality and consensus to determine the highest common priorities. As a result of this process, he reported, two or three major points had been identified.

Before opening the floor to discussion of these issues, however, Mr. Davidson asked Mr. Liscouski to explain how the NIAC and its functions were to transition into DHS. Mr. Liscouski explained that President Bush has nominated General Frank Libutti to be the Under Secretary for the IAIP. He further stated that the Department's goal is to connect, at the national level, the expertise of those who own and operate the critical infrastructures and implement the ideas recommended by the NIAC. Vice Chairman Chambers remarked that someone needs to coordinate all of the advisory committees to avoid overlap; he also suggested long-range planning of the NIAC meetings so allow more members to attend. Mr. Davidson agreed.

### a. Internet Protocol Version 6 (IPv6)

Returning to the issue of topics for NIAC study, Chairman Davidson next asked Mr. Chambers to share his recommendations on the IPv6 issue. As background, Mr. Chambers noted that the question of whether and how to make the transition from the existing Internet operating protocol, IPv4, to a new protocol, IPv6, is driven to a large degree by the fact that the Internet is running out of addresses. Moreover, IPv4 and IPv6 are not compatible with one another. The transition issue has become important for the U.S. because a number of other regions of the globe, most notably Europe and China, have already started their conversion to the new protocol. The current strategy is to migrate systems to IPv6 while still using IPv4.

Mr. Chambers recounted that in November 2002, the President's Critical Infrastructure Protection Board (PCIPB) originally asked the NIAC to review IPv6 from a security perspective.

After further discussion and study, the NIAC subcommittee realized that the fundamental issues associated with the transition to IPv6 are economic rather than security related. The security concerns associated with certain aspects of IPv6 are offset somewhat by other security advantages that the protocol presents. More important that these concerns are the implications that the transition to IPv6 would have for the U.S. economy because of the impact (cost and otherwise) on U.S. businesses and its relevance for U.S. global competitiveness *vis a vis* nations that have already moved forward with the conversion.

Mr. Chambers urged that the United States should study these potential economic impacts in order to determine the best policy approach to take to address the many issues that such a transition would present. It was noted that the President's *National Strategy to Secure Cyberspace* contemplated such an approach, containing a recommendation that the United States Department of Commerce convene a task force to examine these issues. In light of this fact, Mr. Davidson asked the NIAC members if they supported the proposed approach. A motion was made, and seconded, on a resolution stating that:

> The NIAC endorses the recommendation to organize a task force by the Department of Commerce to examine the issues related to IPv6 implementation. We would recommend the inclusion of private sector representatives in that task force. We encourage the task force to move forward as soon as possible.

The resolution was read and, without further discussion, was adopted by a unanimous vote.

**b. Vulnerability Disclosure Guidelines**

Following completion of the vote, Chairman Davidson turned to Vice Chairman Chambers and Mr. Thompson for a report on the work of the Vulnerability Disclosure Working Group. Mr. Thompson and Mr. Chambers, in turn, asked Rob Clyde to discuss the Status Report and Update. *See* copy of briefing: "*NIAC Vulnerability Disclosure Working Group Status Report & Update April 22, 2003*" attached hereto (item 1).

Mr. Clyde began by defining the problems the working group addressed:

- How does one share information about a vulnerability with the appropriate parties without compromising others or the critical infrastructure?
- How do the participants become aware of all of the considerations so as to make the best decisions, possibly in an emergency?
- What does full disclosure mean?
- What are its variations?

Mr. Clyde reported that industry agrees that it can and will solve this problem, and is aware of the urgency. He indicated that the consensus among those in the working group is that no "one size fits all" solution exists, and the focus should be on processes to avoid surprises and make decisions with complete awareness.

Mr. Clyde reported that the working group has been meeting since early March and expects to have a draft framework for group review by April 28th; an external draft approved by the group on May 20th; an external review period from May 23rd through June 20th; and, on June 24th, a

final version submitted for executive approval, with submission to the next NIAC meeting to follow.

Mr. Davidson asked for comments from the NIAC. The members of the NIAC complimented the working group for its efforts. As there were no further comments, Mr. Davidson moved on to possible topics of future NIAC study suggested by the members of the NIAC.

### c. Introduction of Other Topics for Potential Study

Mr. Davidson explained that the members' recommendations were analyzed and consolidated into categories for ease of discussion. Recommendations that were made by more than one member/had a common interest among members were placed in the "A" list; all of the others were placed in the "B" list. Mr. Davidson suggested that the members pick two or three topics from the "A" list to pursue in order to keep things manageable in scope so as to facilitate constructive action on the issues and "accomplish something." He turned the discussion over to Mr. Rick Holmes to explain the proposed topics and the commonalities analysis of the proposed topics for NIAC study and consideration. Mr. Holmes referred to the Memorandum to Members of the Council that Mr. Werner sent out on April 17, 2003, attached hereto (item 2). He noted that the memo should also have included an item from Ms. Margaret Grayson.

Mr. Holmes the referred to the "commonalities" document, attached hereto (item 3), and explained that the analysis sorted the topics into three "buckets": a) projects that are in progress; b) potential projects with common interest (the "A" list, with five topics); and c) other project suggestions ("one-offs", with seven topics). Mr. Holmes walked through each of the topics on the "A" list: (1) Cross-sector interdependency identification and risk assessment; (2) Coordinating restoration of service of critical infrastructure services; (3) Defining the role of NIAC and coordination with other advisory councils; (4) Regulatory guidance on best practices for enhancing security of critical infrastructure industries; and (5) Evaluation and enhancement of Information Sharing and Analysis. *See* attached item 3. Mr. Holmes concluded his explanation and turned the meeting back to Mr. Davidson.

## IV. Discussion of Possible Topics

Upon completion of the introduction of topics, Mr. Davidson opened the floor to discussion of them.

On the first topic (sector interdependencies), no members interposed any comments or questions, and there was general consensus that the NIAC should take on work in this area. Mr. Davidson suggested that the second issue (coordination of restoration of critical services) seemed to flow logically from work on sector interdependencies and could, therefore, be a by-product of that working group effort. There was general consensus among the member to conjoin these issues as Mr. Davidson suggested. On these points, Mr. Dunham added that he assumed that the working group would also consider issues associated with the physical facilities as well as cyber, noting that a lot of work is needed on physical issues, especially for facilities based infrastructure services providers like those in the energy and oil and gas sectors. Observing that three of the six proponents of this topic came from financial institutions (Mr. McGuinn, Mellon Financial; Mr. Kovacevich, Wells Fargo; and Mr. Martinez, Sterling Bank), Chairman Davidson asked if one of them would be willing to take leadership of this initiative. Mr. McGuinn accepted this responsibility. Mr. Davidson committed his support to the effort.

Turning to the third topic –"Defining the role of NIAC and coordination with other advisory bodies" – Ms. Katen inquired about the specific objectives of this effort. Was it to understand the consequences of the various efforts, to eliminate overlap among panels, or simply to gather information on for NIAC members on what other panels are doing? Ms. Ware, the proponent of the topic, noted that eliminating overlap among the various panels would expand the range of activities for all of them.

Mr. Kurtz from the Homeland Security Council staff noted that members of the National Security Telecommunications Advisory Committee (NSTAC) had raised expressed a similar interest in this topic. Ms. Wong, with Mr. Kurtz's concurrence, added that the identification of roles and responsibilities of the various advisory bodies working on critical infrastructure assurance issues, and "mapping the lanes" among them, are responsibilities that properly rest with the government. Ms. Wong and Mr. Kurtz committed undertake responsibility to examine the landscape of advisory panels in an attempt to uncover any unproductive redundancies in jurisdiction and to report back to the Council on their findings.

Ms. Ware agreed to serve as their liaison to the Council. Mr. Dunham expressed the view that the issue was "great" for study, and Mr. Noonan similarly indicated "strong support" for the effort and offered to assist with it.

Discussion then turned to the fourth topic – "Regulatory guidance on best practices for enhancing the security of critical infrastructure industries." This subject generated the greatest amount of interest and discussion among the members. Ms. Katen expressed the concern that adding an additional layer of regulation on already highly regulated sectors (like pharmaceuticals) could "make it too difficult to get things done." In contrast, Mr. Davidson observed that there is a sense that in some sectors (*e.g.*, water and certain segments of the power generation sector) operated by governmental or quasi-governmental bodies, movement to adopt appropriate infrastructure assurance practices is slow because customary market-based profit motives are not as powerful an incentive for these operators. In such cases, Mr. Davidson asked, does regulation become necessary to drive action? Ms. Katen agreed, but asserted that regulations would have to be developed to be industry specific.

Ms. Ware also agreed with Chairman Davidson's point, observing that, sometimes, smaller sectors (or smaller operators within sectors) tend to wait for government to provide leadership in an area before taking action. Mr. Noonan added that corporate security officers have often told him that they would welcome greater government regulation because it would create an incentive for senior managers to respond to the security officers' concerns and engage them in the issues. Ms. Ware suggested that the NIAC should raise awareness of this issue.

Mr. Berkeley expressed reservations about direct Federal regulation in the CIP area and suggested that perhaps a better answer could be found in the self-regulatory model used in the securities industry under the 1937 amendments to the Securities Act of 1934.

Mr. McGuinn noted the phenomenon that almost every sector feels that it is adequately regulated but views more regulation as necessary in <u>other</u> sectors to ensure a minimal level of adequacy to reduce or eliminate cross-sector vulnerabilities arising from sector interdependencies. Ms. Katen agreed that this was a "fair point," stating that each sector can always learn from others' best practices; however, she cautioned that a "one size fits all" approach should be avoided.

Noting the lively interest among the members, and the apparent agreement that the subject was one worthy of further examination, Chairman Davidson asked Ms. Katen if she would take the lead on the effort and bring together a group with a balance of "pro" and "anti" regulation members. Ms. Katen agreed to undertake this responsibility. Ms. Ware, Mr. Noonan, Mr. Martinez, and Mr. Dunham all expressed willingness to contribute to the effort. Mr. Berkeley committed to provide background information on the self-regulation model used in the securities industry.

Next, Mr. Davidson opened discussion on the fifth topic – "Evaluation and enhancement of Information Sharing and Analysis" – observing that work in this area could really benefit all sectors if it was done correctly. There was a general consensus of the need to undertake this project. Ms. Ware stated that she sees wide disparities in quality among the existing ISACs.

Mr. Noonan stated that he has first-hand experience running the IT-ISAC, and he volunteered to chair this effort. Mr. Dunham noted that Bobby Gilham of ConocoPhillips serves as a sector coordinator for oil and gas, and Mr. Dunham offered his support to this project. Likewise, Chairman Davidson, Vice Chairman Chambers, and Ms. Ware indicated that they would contribute support to this working group. Ms. Grayson also added her support, noting that her concerns regarding interoperability issues fit well into this initiative.

Mr. Davidson thanked the NIAC members for their willingness to take on the responsibilities for the topics of interest.

## V. Discussion of Possible Dates for Future Meetings

Mr. Davidson asked the members if they would be willing to schedule future NIAC meetings as far in advance as possible, perhaps two meetings a year in person, with another two (no more than one a quarter) by telephone. The members thought that once or twice a year face-to-face was a good idea, but they liked the conference call meetings. It was agreed that they need as much time as possible in advance to schedule their calendars for the NIAC meetings. The suggestion was made to schedule eighteen months in advance, since it is easier to cancel than it is to schedule meetings. Based on this discussion, the NIAC staff was asked to prepare a notional schedule of future meeting dates and coordinate with the Chairman and Vice Chairman.

Mr. Davidson hoped to try for July for the next meeting. Mr. Paul Kurtz stated that the White House was seeking to reschedule the President's meeting with the NIAC members for sometime in July and would get back to the members with possible dates.

## VII. Adjournment

Mr. Davidson, Mr. Liscouski, and Ms. Wong thanked the members for their time, and Ms. Wong 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: /s/ Richard K. Davidson_____ Dated: 7/21/2003
Richard K. Davidson, Chairman

# NIAC Vulnerability Disclosure Working Group

## Status Report & Update

**April 22, 2003**



## Mission & Scope

- Guidelines for handling a network security vulnerability from initial report to final resolution
- Audience includes government, education, private industry, the public, and other stakeholders
- Builds on existing best practices and wide range of experience from working group members
- Derive specific recommendations for the President and the Federal Government from those guidelines



## Background

- Vulnerability reports continue to increase
- Great diversity of practice, goals, and values among those who handle vulnerabilities
- The Internet is global, but stakeholders have obligations to their own constituencies
- NIAC charged by Executive Order to provide recommendations which will improve sharing between ISACs, DHS, and other agencies

## Working Group Members

- Co-Chairs:
  - John Chambers, Cisco Systems
  - John Thompson, Symantec
- Participants include ISS, Mitre, CERT/CC, Verizon, Counterpane, Fannie Mae, UC Davis, Microsoft, IT-ISAC, Telecom-ISAC, FS-ISAC, ISC, DHS/IAIP



## Problem Definition

- How does one share information about a vulnerability with the appropriate parties without compromising others or the critical infrastructure?
- How do the participants become aware of all of the considerations so as to make the best decisions, possibly in an emergency?
- What does full disclosure mean? What are its variations?



## Initial Input for Content

- Vulnerability disclosure practices from working group members
- CERT/CC Vulnerability Questionnaire
- Other submitted industry best practices
- Various contributing research papers, articles, and case studies

## In Agreement

- The Internet has no physical boundaries; thus consideration has to be global but with an obvious focus on national constituents.
- Limit working group activity to vulnerability disclosure.
- Those with a plan survive; write it down now
- Industry agrees it can and will solve this problem, and is aware of the urgency.



## In Consensus

- No "One size fits all"; focus on processes to
  - Avoid surprises, and
  - Make decisions with complete awareness
- Similar efforts do not directly overlap
  - OIS, INCH (IETF), FIRST Vendor Group
- Consider varying missions and constituencies
  - Manufacturers and vendors of products and services
  - Consultants who provide warnings to customers
  - Coordinating agencies for the common good
  - Other critical infrastructure sectors



## Timetable

- Group has been meeting since early March
- April 28: Draft framework for group review
- May 20: External draft approved by the group
- May 23 – June 20: External review period
- June 24: Final version submitted for executive approval with submission to the next NIAC meeting to follow

## Deliverables

- Full report due by the end of June, 2003
- Various status reports in the interim, including presentations to other groups during the external review period
- More information is solicited, but the authors have enough information to begin writing the basic framework



## Comments and Suggestions

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

# NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

**MEMORANDUM**

TO: Members of the Council *Via e-mail*

FROM: Eric T. Werner
Office of Planning and Partnerships, DHS

RE: Compilation of Members' Proposals for Potential Issues to be Placed on NIAC Agenda

DATE: April 17, 2003

---

During its meeting on January 8th, the National Infrastructure Advisory Council (NIAC) discussed the need to develop an agenda of items for future study and consideration by the Council and agreed that such an agenda should be based on input from the members themselves. Following that discussion, in a letter dated January 22, 2003, Chairman Davidson invited you to forward to this office your proposals or suggestions for topics to be considered by the NIAC. Chairman Davidson stated that the NIAC would consider criteria to identify and rank items requiring further evaluation and proposed the following three metrics as an initial framework for discussion:

- The significance, relevance, and/or importance of the issue to the Federal Government and NIAC members;
- The ability of the NIAC to complete action on the issue and report findings or recommendations within 90 days, excluding any longer-term supporting task force or working group actions; and
- No more than three items should be concurrently pursued.

Several members have submitted suggestions for possible topics worthy of consideration by the NIAC. Pursuant to Chairman Davidson's letter, and in preparation for the meeting of the NIAC scheduled for next Tuesday, April 22, we have compiled your suggestions into the consolidated list that appears below. Most of the suggestions or recommendations speak for themselves. Where the member submitting the proposal provided additional narrative to explain the issue, we have included it in the list.

The list below presents only the topic suggestions. It does not attempt to rank or otherwise prioritize the proposals or to organize them according to topic. A separate chart, which attempts to identify points of commonality among the suggestions, is being prepared and will be sent separately in the next day or so.

In the event you have any questions concerning the information in this memo, please do not hesitate to contact me.

## TOPICS FOR POSSIBLE NIAC STUDY AND CONSIDERATION

1. Critical Infrastructure Interdependency and Prioritization of Restoration of Service. *Chairman Davidson*
2. Define the role of the NIAC in coordination with related federal advisory committees. *Vice Chairman Chambers*
3. Develop national vulnerability disclosure guidance. *Vice Chairman Chambers*
4. Recommend that the President establish an IPv6 Transition Task Force. *Vice Chairman Chambers*
5. Develop a scalable national identity management trust model. *Vice Chairman Chambers*
6. Develop a plan for public-private cross-sector vulnerability risk assessments. *Vice Chairman Chambers*
7. Recommend incentives or other retention programs for security specialists for government and service providers. *Vice Chairman Chambers*
8. Refine the role the Council will play with the Department of Homeland Security to enhance the security postures of the nation's critical sectors. *Ms. Ware*
9. Sponsor a study to better understand the unique security issues surrounding Digital Control systems defining configuration and integration measures that can be implemented immediately to better protect these mission critical systems. *Ms. Ware*
10. Develop a proposal for the coordination and initiation of vulnerability and interdependency assessments across all critical sectors focusing on the convergence of physical and information vulnerabilities specific to the infrastructures of each sector, and the development of a common framework for cross-sector emergency preparedness and response exercises sponsored by lead sector agencies. *Ms. Ware*
11. Propose recommendations to address the inequities between critical sectors' Information Sharing and Analysis Centers (ISACs) and how all sector ISACs will coordinate among one another as peers and with the new Department of Homeland Security for integration into national efforts. *Ms. Ware*
12. Information Sharing and Analysis – Review sector and cross-sector sharing and analysis of threat and vulnerability information including physical and electronic threats. Determine which models (such as Information Sharing and Analysis Centers (ISACs) or others) are most effective. Develop action plan to address gaps. *Mr. Kovacevich*

    The importance of the critical infrastructure to National security requires effective sharing of threat and vulnerability information. The current environment is fragmented with information sharing taking place in piecemeal fashion and with little or no information shared between sectors. Improved information sharing and analysis will ensure timely and effective response to crises that threaten critical

infrastructure sectors. Additionally, threat and vulnerability detection will improve over time with a broader and deeper information base.

13. Mutual Assistance/Shared Resources – Undertake an analysis to develop opportunities for shared resources and mutual assistance. Some areas for consideration include business continuity planning (currently being explored by the Financial Services Technology Consortium), threat assessments as well as physical and data security. *Mr. Kovacevich*

    Competitive influences often result in business sectors and organizations responding to threats individually. These individual efforts result in varied effectiveness of preparedness and response to crises. September 11th demonstrated the urgent need to challenge commonly accepted norms of non-competitive coordination and push the envelop of open communication and mutual support. An analysis of opportunities to share resources or provide mutual assistance during crises can significantly reduce the risk of sector or national infrastructure impact.

14. Advanced Mobile Malicious Code Mitigation – Produce recommendations for public and private research and development of virus prevention and risk based, minimum standards by industry for timely patching. *Mr. Kovacevich*

    Increasingly, traditional anti-virus efforts need to be integrated with non-anti-virus measures (worms, etc.). Increasingly, mobile malcode are utilizing consumer systems as agents of replication and attack platforms (zombies). Critical companies with large customer bases should take a more proactive role in helping to protect their customer systems. Public and private collaboration on virus protection can produce synergy that will result in a decrease in impact and disruptions caused by viruses.

15. Leased Space Issues – Undertake a review of building-related issues in order to develop a set of best practices and policies for space leasing. *Mr. Kovacevich*

    Many companies who make up the critical infrastructure conduct business in leased office and production space. Actions taken by building owners may cause disruptions in critical services. A collaborative effort will identify a broader range of building-related risks and mitigation opportunities than can be accomplished within any single company or sector.

16. 3rd Party Services – Conduct an evaluation to determine vulnerability in use of third party staff, critical systems or services with the goal of identification of priority actions to and development of procedures to mitigate risk, particularly as it pertains to terrorism. *Mr. Kovacevich*

    Reliance on third party resources creates a constantly evolving risk for critical business sectors. This is an area that has not received significant or cooperative analysis. This effort may result in a significant reduction in overall risk to disruption.

17. Asking the private sector entities to conduct their own vulnerability assessments. This topic may be nested in the topic concerning "responsible disclosure of cyber attacks/incidents." *Mr. Martinez*

18. Improve the process for timely communication to the private sector of indications and warning information concerning emergent viruses or other cyber incidents. *Mr. McGuinn*.

    On January 25, 2003, at 6:45 a.m., Mellon was notified of the Slammer Virus incident via one of our software vendors. Later that morning, Mellon participated in a BITS (Banking Internet Technology Secretariat) crisis call, where representatives from the Government noted that they were aware of the virus and its potential impact around 3:00 a.m., well before we had received any notifications about the virus. The importance of the Internet as a critical infrastructure component, coupled with the speed with which viruses such as Slammer can spread around the world, create a need for an effective process for contacting the business sector when such incidents arise. Time is of the essence in reducing the damage such incidents can cause.

19. Improve telecommunication capability for critical financial services. *Mr. McGuinn*

    Inadequate diversity and lack of redundant services within the telecommunications network present unacceptable operational risks for the delivery of critical services, which poses a threat to national interest. Specifically, the telecommunication's industry weaknesses in the following areas in turn pose a threat to industries that are dependent upon telecommunications to operate. These weaknesses include: (1) inadequate diversity, lack of redundancy, and existence of points of failure; (2) limited information sharing ability; (3) lack of business and political processes; and (4) uncertain impact of emerging technologies and integration with existing technologies.

20. Champion sponsorship of a national Crisis Command Center that spans critical industries and could help to coordinate recovery activities in time of a crisis. The Center could also provide a mechanism for true end-to-end business continuity testing across sectors, service providers, governmental bodies and other key dependency parties. *Mr. McGuinn*

21. Gain a better understanding of cross border outsourcing and best practices regarding control, security, and business continuity issues. Gain an understanding of how companies develop processes to establish these controls, evaluate country, economic, political, and subcontracting risks, and meet regulatory, shareholder, and industry requirements. How will the US deal with the longer-term issues, such as cost of labor, quality of development, and a need to incent organizations to develop technical expertise? *Mr. McGuinn*

22. Increase the labor pool of available technical expertise. Develop a methodology to award scholarship funding to high school students with a mathematical aptitude. *Mr. McGuinn*

23. Improve the implementation of software to minimize flaws and security vulnerabilities before distribution, and improve the process for patching systems once flaws are discovered. *Mr. McGuinn*

24. In the financial services arena, regulators are in the process of providing regulatory guidance on Sound Practices to Strengthen the Resiliency of the U.S. Financial Systems. Should there not be the same amount of scrutiny and updating of best practices to reach a post-9/11 view of the world for each of our critical infrastructure industries? *Mr. McGuinn*

Alternative Recommendations

In addition to his suggestions above, Mr. Kovacevich also submitted the following items as secondary or alternative topics for consideration:

1. Telecommunications – Work with financial sector groups to identify non-redundant services within the telecommunications network. *Mr. Kovacevich*

   Inadequate diversity and lack of redundant services within the telecommunications network present unacceptable operational risks for the delivery of critical services, which poses a threat to national interest. Vulnerabilities in telecommunications were well demonstrated on September 11th, 2001. Immediate and strong support of public and private efforts is necessary to ensure the nation's economic resiliency. The issue is identified as the highest priority as it addresses a known and demonstrated problem.

2. Priority Disaster Area Access and Resource Allocation – Identify opportunities to use the CEAS and GETS models and produce a recommendation and process to be communicated at the national, state and local levels of government. *Mr. Kovacevich*

   During an emergency or crisis, there is little ability at present to prioritize access, physical and electronic, to critical areas and resources for private companies. Two examples can provide a model; 1) in New York City, public and private cooperation produced the Corporate Emergency Access System (CEAS) identification program to allow businesses access to their critical buildings in a disaster area, and 2) the Government Emergency Telecommunications Services (GETS) card allows for critical public and private personnel to gain priority access to telephone circuits during an emergency. These models can be applied to other issues including prioritization of public resources such as building inspections. Inclusion of critical private sectors in public emergency management efforts will improve the speed and effectiveness of emergency response and recovery.

3. Critical Interdependencies – Undertake an analysis of critical interdependencies should be undertaken with the goal of a prioritized public and private risk mitigation plan as the result. *Mr. Kovacevich*

There are many interdependencies throughout the private sector. Interruptions in some sectors (such as telecommunications and transportation) may be more disruptive than others. An example of this is interruption of payment systems due to grounding of airlines in the wake of September 11th. A cross-sector analysis of interdependencies will result in identification and mitigation of risks that are most critical to the nation's infrastructure.

# NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

## Teleconference

Tuesday, April 22, 2003
4:30 p.m. – 6:30 p.m. EDT

## COMMONALITIES ANALYSIS OF PROPOSED TOPICS FOR NIAC STUDY AND CONSIDERATION

### Projects that are in progress

1. Develop national vulnerability disclosure guidance.
2. Recommend that the President establish an IPv6 Transition Task Force

### Potential Projects with common interest

1. Cross sector interdependency identification and risk assessment
2. Coordinating restoration of service of critical infrastructure services
3. Defining role of NIAC and coordination with other advisory councils
4. Regulatory guidance on best practices for enhancing security of critical infrastructure industries
5. Evaluation and enhancement of Information Sharing and Analysis

### Other Project Suggestions

25. Develop a scalable national identity management trust model.
26. Recommend incentives or other retention programs for security specialists for government and service providers.
27. Sponsor a study to better understand the unique security issues surrounding Digital Control systems defining configuration and integration measures that can be implemented immediately to better protect these mission critical systems.
28. Advanced Mobile Malicious Code Mitigation – Produce recommendations for public and private research and development of virus prevention and risk based, minimum standards by industry for timely patching.
29. Increase the labor pool of available technical expertise. Develop a methodology to award scholarship funding to high school students with a mathematical aptitude.
30. Improve the implementation of software to minimize flaws and security vulnerabilities before distribution, and improve the process for patching systems once flaws are discovered.

**Project Name:** **Cross-sector interdependency and risk assessments**

**Project Proponents**: Mr. Chambers. Mr. Davidson, Mr. McGuinn, Mr. Kovacevich, Mr. Martinez, Ms. Ware

---

**Issue:** We need to assess the critical interdependencies that exist between the critical infrastructure sectors and provide risk assessment guidance. Interruptions in some sectors (such as telecommunications and power) may be more disruptive than others. Examples include the potential impact to Emergency Services during a telecommunications failure or cascading failures in multiple sectors due to an interruption in one.

**Action:** Analyze critical interdependencies between sectors and develop risk management strategies by taking advantage of modeling efforts and regional tabletop exercises. Consider the impact, control issues, and best practices of cross-border outsourcing, 3rd party services, and leased facilities.

**Benefits:** A cross-sector analysis of interdependencies will result in the identification of risks that are most critical to the nation's infrastructures and will become the basis for a prioritized program to remediate the risks and coordinate the restoration of service.

**Project Scope:** Identify key regional dependencies with the exclusion of specific company and government vulnerabilities. Evaluate best practices related to third party services and cross-border outsourcing.

**Team Members:** NIAC volunteers and DHS staff with representation from each sector; National Infrastructure Simulation and Analysis Center (NISAC) support and key stakeholders in each region where tabletop exercises are conducted; and coordination with Partnership for Critical Infrastructure Security (PCIS) efforts to develop a risk assessment guidebook.

**Potential Approach:** Form a project team to collaborate and coordinate with applicable public and private entities to leverage current efforts in interdependency modeling efforts and regional tabletop exercises.

**Project Name:** **Coordinating restoration of service of critical infrastructure services**

**Project Proponents**: Mr. Davidson, Mr. McGuinn

---

| | |
|---|---|
| **Issue:** | There is a need to enhance crisis coordination capabilities across critical infrastructure sectors to facilitate orderly restoration of all critical infrastructure services. The Telecommunication Service Priority program exists to provide prioritized restoration of service for telecommunication services; however, an equivalent capability does not exist for other infrastructure sectors. |
| **Action:** | Leverage the results of cross sector risk assessments and evaluate existing processes to coordinate restoration of service. Make recommendations to DHS for a service restoration program to cover critical infrastructure requirements. |
| **Benefits:** | Orderly restoration of critical services and minimization of impact during crises. This would enhance the effectiveness of existing crisis coordination within the DHS. |
| **Project Scope**: | Build on dependencies identified in cross-sector risk analyses to develop restoration priority processes across the sectors. |
| **Team Members:** | NIAC volunteers, industry trade organizations, and DHS staff with representation from each sector. National Infrastructure Simulation Analysis Center (NISAC) support as applicable. |
| **Potential Approach:** | Evaluate cross-sector risk assessments, existing restoration of services programs, and industry best practices. Work with the NISAC to refine effective restoration processes. |

**Project Name:** **Defining the role of NIAC and coordination with other advisory councils**

**Project Proponents**: Mr. Chambers, Ms. Ware

---

**Issue:** NIAC is one of several Federal Advisory Committees and other organizations tasked to investigate national security and emergency preparedness issues affecting critical infrastructures. It is imperative that companies and organizations understand the scope and limitations of each advisory group to minimize duplication of effort and provide effective advice to the President.

**Action:** Based on a review of advisory committee and other organization charters, membership, results to date, and Department of Homeland Security needs, make recommendations regarding "lanes in the road" and cross-coordination.

**Benefits:** Each group working on critical infrastructure assurance issues will understand each other's missions, scope, and boundaries, and will be empowered to focus within defined roles. Coordination across related advisory groups will improve, minimizing duplication of effort, while providing cross-fertilization of ideas.

**Project Scope:** Since NIAC's charter covers national and economic security and covers all critical infrastructure sectors, the scope of this effort should include NIAC, National Security Telecommunications Advisory Committee (NSTAC), National Reliability and Interoperability Council (NRIC), President's Homeland Security Advisory Council (PHSAC), Partnership for Critical Infrastructure Security (PCIS), Partnership for Public Warning (PPW,) President's Committee of Advisors on Science and Technology (PCAST), and other relevant organizations discovered during the review.

**Team Members:** Volunteer NIAC Task Force and DHS support staff

**Potential Approach:** Survey existing related organization charters, membership, and recent results, with assistance from DHS staff. Identify DHS requirements for critical infrastructure protection advice from industry. Coordinate meetings and establish coordination points of contact with all relevant advisory organizations to define roles and responsibilities and develop models for cooperation. Publish a report of findings and recommendations to the President, through the Secretary of Homeland Security, by July 18, 2003.

**Project Name:** **Regulatory guidance on best practices for enhancing the security of critical infrastructure industries**

**Project Proponents**: Mr. McGuinn, Ms. Ware

---

| | |
|---|---|
| **Issue:** | The protection of our critical infrastructures is clearly a national imperative. Many critical infrastructure sector owner/operators have numerous high priority risks to mitigate based upon the new paradigm of asymmetric threats facing the Nation today. We can expect the costs for the remediation of these risks across all critical sectors to be staggering. Some critical sector owner/operators have sound commercial positions for mitigating security risks; others are heavily regulated already, yet others will be challenged to meet the risk mitigation challenges without regulation or subsidization. |
| **Action:** | Conduct a study to assess the impact of focused regulation on the security posture of each critical infrastructure sector. |
| **Benefits:** | Raise awareness of the effectiveness of regulation and other tools to improve security and mitigate risks and vulnerabilities in each critical infrastructure sector. |
| **Project Scope:** | The scope should include the investigation of the most effective drivers of security improvement in each sector. |
| **Team Members:** | Volunteer NIAC Task Force with DHS staff support. |
| **Potential Approach:** | Conduct individual studies of each sector and present results to lead sector agencies, regulatory bodies and lead sector coordinators. |

**Project Name:** **Evaluation and enhancement of Information Sharing and Analysis**

**Project Proponents**: Mr. Kovacevich, Mr. McGuinn, and Ms. Ware

---

**Issue:** Sharing information within industry sectors, across sectors, and between industry and government is critical to understanding and responding to threats to remediate vulnerabilities. Because of the rapidity of cyberspace attacks, the only way to develop timely defensive actions is by correlating events across companies and governments. Industry Information Sharing and Analysis Centers (ISACs) have been created, with mixed results and spotty participation. Sharing information with the Federal government has been hampered by barriers such as the Freedom of Information Act (FOIA), recently partially improved by language in the law creating the Department of Homeland Security. Several privately run ISACs are experiencing financial difficulty, and many are struggling to demonstrate value to prospective members. States and first responders have unique information-sharing needs that are not met within current fiscal environments.

**Action:** Champion cross-sector and public-private information sharing on critical infrastructure threats, vulnerabilities, countermeasures, and best practices by investigating funding and operational models of existing ISACs and government information-sharing organizations; developing goals and objectives to provide added value to infrastructure companies and governments; and making recommendations to the government regarding funding support, incentives to enhance inclusiveness among sectors, and research toward real-time event correlation across sectors.

**Benefits:** Scaling ISAC membership to include most infrastructure owners and operators in each sector would provide a broad base for information on threats and warnings, and an equally broad base to transmit warnings, countermeasures, and other solutions. Federal funding support may enable ISACs to bring in a greater percentage of their sectors than they do currently. Successful research toward real-time cross-sector event correlation will add significant value to threat warning, trending, and analysis. Enhancing trust models will encourage cross-sector and public-private information sharing, thereby enabling the Federal government to make timely decisions regarding possible attacks on the United States.

**Project Scope:** This initiative should include a survey of all existing ISACs, other industry and government information-sharing organizations, and DHS/NIPC analysis and warning requirements. It should also include a review of existing and planned research on real-time event correlation, identifying technical and non-technical barriers to the desired comprehensive trust model. Finally, the initiative should recommend organizational and funding models for ISACs, a cross-ISAC information sharing architecture, and public-private event correlation.

**Team Members:** Staffing alternatives: Volunteer NIAC Task Force with DHS staff support, volunteer PCIS Task Force

**Potential Approach:** Review existing ISAC organization and funding models, membership, and challenges. Review government information sharing organizations. Review GAO and other survey 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 other incentives to scale ISAC participation to include all owners/operators in each sector.