NATIONAL INFRASTRUCTURE ADVISORY COUNCIL
MEETING

Tuesday, November 26, 2002
2:00 p.m. – 4:00 p.m.

1088 G Street, N.W.
10th Floor Conference Room
Washington, D.C.

AGENDA

I.	**Opening of Meeting/ Roll Call of Members:**	John S. Tritak, *Director, Critical Infrastructure Assurance Office; Designated Federal Officer, NIAC*
II.	**Welcoming Remarks:**	Richard A. Clarke, *Special Advisor to the President for Cyberspace Security; Executive Director, NIAC* Kenneth I. Juster, *Under Secretary of Commerce for Industry and Security, United States Department of Commerce* John T. Chambers, *President and CEO, CISCO Systems, Inc.; Vice Chairman, NIAC* Richard K. Davidson, *Chairman, President and CEO, Union Pacific Corp.; Chairman, NIAC*
III.	**Discussion of NIAC comments on the draft of the *National Strategy to Secure Cyberspace***	Mr. Davidson, Mr. Clarke, NIAC Members, PCIPB Staff
IV.	**Adoption of NIAC comments**	NIAC Members
V.	**NIAC Priorities**	Mr. Davidson, Mr. Clarke
VI.	**New Business**	Mr. Davidson, Mr. Clarke
VII.	**Adjourn**	

M I N U T E S

NIAC Members present in Washington:

Mr. Clarke; Mr. Tritak; Chairman Davidson; Dr. Rose; Ms. Ware.

NIAC Members attending via Conference Call:

Vice Chairman Chambers; Mr. Carty; Mr. Conrades; Mr. Dunham; Chief Gallegos; Ms. Grayson; Ms. Katen; Mr. Martinez; Mr. McGuinn; Mr. Webb.

Mr. Barrett; Mr. Hernandez; Mr. Holliday; Commissioner Kelly; Mr. Noonan; and Mr. Weidemeyer were not in attendance but had staff monitoring the call.

Other Dignitaries Present:

Kenneth I. Juster, Under Secretary for Industry and Security, U.S. Department of Commerce

I. Formal Opening of Meeting

Mr. Tritak, as the Designated Federal Officer (DFO) of the NIAC, called the meeting to order and formally opened it. After introducing himself, Mr. Tritak reminded the members that this meeting was open to the public and that any interested party and members of the press could be present or listen in on the call.

Mr. Tritak noted that the meeting was originally to be held in the Truman Room at the White House Conference Center, 26 Jackson Place, N.W., a few blocks away and the same place where the inaugural NIAC meeting was held on November 15, 2002; however, due to the protest in Lafayette Park, the Secret Service had urged that the meeting be held in another location. Signs were posted at the Conference Center to direct attendees to the 10th Floor Conference Room at 1800 G Street, N.W., and the start of the meeting was delayed by fifteen minutes to allow those interested in attending to reach the new location.

NIAC members present in Washington and those on the conference call were asked to identify themselves. (See list above.) Mr. Tritak turned the meeting over to Mr. Clarke.

II. Welcoming Remarks

Mr. Clarke requested that the members discuss and provide comments on the six questions pertaining to the *National Strategy to Secure Cyberspace* that were posed during the last NIAC meeting (Attachment 1), as well as the Strategy's five proposed priorities (Attachment 2).

Mr. Clarke turned the discussion over to Mr. Davidson, who immediately introduced Mr. Chambers. Mr. Chambers stated that he was honored to be on the NIAC and serve as its Vice Chairman; he thanked all of the members and asked them to consider how the NIAC can use its time most effectively and keep the partnership headed in the right direction.

Mr. Davidson then told the members that the responses received "looked quite good and thoughtful," and he thanked Rick Holmes and Ken Watson for their work compiling and distributing the responses to the NIAC members. Mr. Davidson requested that Mr. Holmes and Mr. Watson walk the members through the memo they prepared and stated that, at the end of their presentation, he would open the floor for comments from the members. A draft proposal

based on the committee's conclusions would also be circulated to all of the members for review and approval prior to submittal to the President. Mr. Davidson turned the floor over to Mr. Holmes.

III. Discussion of NIAC Comments on the Draft of the National Strategy to Secure Cyberspace

Mr. Holmes presented the questions, and summarized the responses received for each, which were captured in the letter from Chairman Davidson to Mr. Clarke dated November 25, 2003 (copy attached):

Question #1 – Is the Strategy on track?

The overwhelming response was yes; however, one dissenting member stated that the Strategy did not address real threats or identify actions, and has unclear linkage from the national priorities to the objective, although there is a feedback loop that may help address the gaps.

Question #2 – Role of Federal Regulation?

In this area, the members' responses were split between vendor accountability and holding critical infrastructure providers accountable for reliable hardware and software.

Question #3 – Citizen Awareness Program and Role of Home User?

The members believed that these programs were useful and should exist but the responsibility should not be on the Home User. Instead, Internet providers should be responsible to ensure the security of their products.

Question #4 –What the NIAC liked about the Strategy:

1) Multi-tiered scope and the focus on five sections.
2) The market-based approach, in conjunction with the Federal government's procurement power. If unsuccessful, only then consider the use of regulation.
3) The NIAP process encouraged for use beyond DoD.
4) The emphasis on public-private partnership.
5) The on-going Vulnerability Assessment Program; the same approach should be used throughout the government and industry.
6) Overall support for an Awareness Program.

Question #5 – Any major gaps? Suggested enhancements?

1) Strengthen vendor recommendations. Spell out their role(s).
2) Remove barriers to information sharing, whether real or imagined (e.g., FOIA). Also, different models are being used for the ISACs – more consistency is needed.
3) Mandates for product liability.
4) Education and awareness in public schools; there are no ethics programs in place.

5) Stress risk management process; ensure that the Government's $20B investment makes sense.
6) R&D roadmap – needs to be prioritized.
7) Best practices/accepted practices/guidelines could be included.
8) Human element has not been really addressed. Background investigations vs. civil liberties; telecommuter risk.
9) Internet service providers – enhance their offerings.
10) Interdependency issues between sectors.
11) Penalty phase and punitive damages – increase capabilities and follow-through.

Some unique themes (raised by one or two members):

1) At the university level, support for advanced degree programs. Also, there is a void of qualified professors; the CyberCore may be "decapitating" the pool.
2) Enhance universities' security programs.
3) An Emergency Response Program is a sensible idea because we can't prevent every attack.
4) Emphasize the role of the National Infrastructure Protection Center (NIPC).
5) A real cyber assessment of industry is generally opposed because of the potential for disruption, and because it is not known how the information gathered will be used.

Mr. Watson mentioned that he and Mr. Holmes attempted to identify the common themes from the members' comments. The multi-tiered approach of the Strategy had the most support (6 of the 9 members who responded supported it). Others were: 1) the need to strengthen vendor recommendations; 2) market-based solutions rather than regulation-driven; and 3) removing barriers to information sharing (developing FOIA exemptions and a National Responsible Disclosure Plan that would ensure that information would not be disclosed prematurely and would be disclosed without harm to the companies who are disclosing). Mr. Watson and Mr. Holmes turned the meeting back to Mr. Davidson.

After Mr. Davidson opened the floor for comments, the NIAC members raised the following questions/issues:

- Government regulation is necessary to catch the bad actors if other approaches fail.
- The quality and quantity of computer professionals in both the government and private sector are cause for worry. Perhaps the private sector could be "deputized" to help the government.
- The consensus was to avoid regulation, although regulation can move an "inert group" to action. Mr. Clarke opined that the regulation issue is not "black/white": Congress has already provided regulation for banks and health care. Federal regulation is not a major policy vehicle/primary thrust, although perhaps it should be. Mr. Tritak explained that the objectives of regulation are to ensure the security of cyber systems related to primary matters, and to secure cyber systems to assure the functioning and protection of the

critical infrastructures. To protect these cyber systems, one must first determine where the markets will fail and, where there is the potential for failure, regulation should be examined and considered. Another cautionary note raised by the members was that we must be careful to avoid over-regulation, and also must compare how state and local governments interact, including how information to protect vital infrastructures is exchanged throughout the country. There are many vulnerabilities and many different systems to examine. Mr. Juster summarized the discussion by observing that the different markets require different approaches to regulation; Mr. Chambers agreed that we should recommend removing some of those impediments that inhibit the exchange of information between state and local governments. In addition, Mr. Chambers concurred that regulation will work best in those instances where market forces do not affect that sector, or where the sector/market is predictable.

In response to a question regarding a member's previous comment on "deputizing" IT professionals, it was explained that since there are not enough IT professionals in the government, perhaps the government could leverage the private sector to help pursue these issues, help with enforcement, and fill the current void. Mr. Schmidt replied that the Secret Service's new Crime Enforcement program is doing just that.

A NIAC member wondered whether anyone had asked the Standards groups about its plans to address cyber security; Mr. Clarke mentioned ICAN and the DNS system and directed the NIAC to the section of the Strategy that discusses securing the mechanisms of the Internet, as well as the initiatives to increase the dialogue with these international groups.

In response to another comment on the Strategy's focus and the importance of the public-private partnership approach, Mr. Clarke reiterated that the emphasis is on awareness – we need to inform the public and industry of the risks so we can advise them on what they need to do to protect the nation's critical infrastructures. However, as another NIAC member reminded the committee, the Strategy's recommendation of not publishing known vulnerabilities runs counter to what is currently practiced in the community, and is not consistent with the Strategy's emphasis on awareness and alerting the public.

The "common criteria" and the NIAP process comprise another concern – the expense and the burden of the process could preclude early-stage entrepreneurial-type organizations from becoming involved. We must "wind-down" the process and make it less costly. Mr. Clarke agreed "one-hundred percent." It was suggested that perhaps a cost-sharing or sliding scale of assessment could be developed: for example, if a small company develops a product, the government would pay 100 percent of the cost for certification.

On the issue of responsible disclosure, Mr. Chambers stated that disclosure should be more conservative, rather than favoring immediate and complete disclosure of every vulnerability, because the "bad guys" are operating at the same pace as the good guys, if not faster. Mr. Clarke felt that it was necessary to mediate this issue to find middle ground. If we have learned about a vulnerability that would be damaging if used, and if the information is spreading like wildfire, we should tell everyone to shut down his or her systems. However, if sitting on the information means that a patch can be developed, withholding the information is more sensible.

The view was expressed that a need exists for a system to make these judgments on a case-by-case basis with the vendors. The government has not had that role before (it has been handled by FedCERT at Carnegie Mellon); however, it was noted that perhaps this could be a task for the

new Department of Homeland Security. The NIAC members felt that they should do more to "wrestle this to the ground" for the group, especially in identifying exploitation technologies and the delivery of protection technologies, rather than waiting for the large infrastructures to react.

The idea of a small group within the NIAC to research, build an ongoing process and encourage debate among the NIAC members was discussed. Mr. Davidson agreed that this could be the first *ad-hoc* committee and asked Mr. Chambers and Mr. Thompson to co-chair the subcommittee; flesh out the approach with the various members of the NIAC; and develop a consensus viewpoint.

Mr. Davidson suggested that the members' delegates speak to Rick Holmes to get the owners/operators to work with them; Mr. Clarke offered his and Mr. Tritak's assistance. Mr. Tritak added that he would ask that staff from the new Department of Homeland Security and each company's corporate counsel look at the information to be shared to encourage information sharing under the new legislation, as the legislation was designed with these problems in mind.

IV. Adoption of NIAC Comments

After asking whether there was any further input from the members, Mr. Davidson asked the group to put together the summaries and work with Mr. Clarke's staff to draft the report for the NIAC's review before submitting the final report to the President. Mr. Clarke advised the NIAC that it was not appropriate for his staff to help the NIAC with this, and he asked them to also include any dissents.

Mr. Tritak hoped that the NIAC would be able to get the draft out to all members by the end of the first week in December. No report from the new ad hoc committee would be included in this report to the President. In response to Mr. Chambers' query, Mr. Clarke reiterated that the NIAC report was the committee's own work product and that he, his staff, and Mr. Tritak were available to "facilitate but not filter". Mr. Tritak noted that the CIAO would channel the report for the record.

Mr. Davidson informed the NIAC that no other meetings have yet been scheduled. Mr. Clarke said a third meeting would be held to review final comments to the draft report. Another meeting with the President may be scheduled in January. Mr. Clarke requested members to provide to his staff and Mr. Tritak's with a list of any dates in January on which the members would be unable to attend a meeting. Mr. Davidson asked each "principal" to designate a lead person who will be doing the "heavy lifting" in order to begin the Conflict of Interest (COI) clearances, if necessary. Mr. Tritak asked that the information be provided to Mr. Eric Werner at the CIAO.

V. NIAC Priorities

Mr. Clarke reiterated the request for the members to provide comments to the 5 priorities so that the priorities are clearer. Another issue that has been voiced by the public in its comments to the Strategy pertains to Internet Protocol Version 6 (IPv6) conversion problems, and the necessity for the U.S. to develop a national policy addressing this in relation to security and interoperability issues. Mr. Clarke suggested this as a possible subject for the NIAC to place on its agenda in the future. Mr. Chambers said he would prefer to include, as an NIAC agenda item, the development of a "straw person" approach before the meeting rather than having a freewheeling discussion. He also thought that adding another member to the NIAC from a large service provider would add value.

VI. New Business

Mr. Davidson remarked that perhaps the NIAC should also look at including comments on physical security since many cyber and physical security issues are intertwined. Although some of the members were interested in pursuing this, Mr. Tritak reminded them that the Department of Homeland Security was looking into a comprehensive, integrated approach, and asked the NIAC's forbearance to only work on those issues that pertain to cybersecurity. He promised to provide more input on the new Department's process and progress on the integrated approach in the future.

Mr. Davidson again thanked Mr. Chambers and reminded the NIAC that they would be following up with each member. At this time, he 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: 2/24/03
Richard K. Davidson, Chairman