NATIONAL INFRASTRUCTURE ADVISORY COUNCIL
Inaugural Meeting

Friday, November 15, 2002
11:00 a.m. – 1:00 p.m.

Truman Room

White House Conference Center
726 Jackson Place, N.W.
Washington, D.C.

AGENDA

I.	**Formal Opening of Meeting**:	John S. Tritak – *Director, Critical Infrastructure Assurance Office; Designated Federal Officer, NIAC*
II.	**Introduction of NIAC Members and Welcoming Remarks**:	Richard A. Clarke – *Special Advisor to the President for Cyberspace Security; Executive Director, NIAC*
III.	**Welcoming Remarks**:	Richard K. Davidson, *Chairman, President and CEO, Union Pacific Corp.; Chairman, NIAC*
IV.	**Briefing on rules and procedures governing Federal Advisory Committee proceedings and deliberations**:	Alice McKenna, Esquire, Arthur A. Warren, Esquire, *U.S. Dept. of Commerce, OGC*
V.	**Briefing on the draft of the *National Strategy to Secure Cyberspace***:	President's Critical Infrastructure Protection Board Staff
VI.	**Discussion of next steps to provide comments on the Strategy and deliberations concerning comments**:	Mr. Davidson, Mr. Clarke, NIAC Members
VII.	**Adjourn**	

M I N U T E S

NIAC Members present in Washington:

NIAC members: Mr. Clarke, Mr. Tritak; Mr. Berkeley, Ms. Katen, Dr. Rose, Ms. Ware.

NIAC Members attending via Conference call:

NIAC Members: Mr. Davidson, Chief Gallegos, Ms. Grayson, Mr. Hernandez, Mr. Holliday, Mr. Martinez, Mr. McGuinn, Mr. Noonan, Mr. Webb.

Mr. Chambers and Commissioner Kelly were not in attendance but had staff monitoring the call.

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 presented a brief history of the NIAC, explaining that it was established pursuant to Executive Order 13231 in October 2001 to focus on the critical infrastructures that underpin this nation. He also noted that the 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. NIAC members present in Washington and those on the conference call were asked to identify themselves (*see* list above). Mr. Tritak turned over the meeting to Mr. Clarke.

II. Introduction of NIAC Members and Welcoming Remarks

Mr. Clarke introduced himself as the Executive Director of the NIAC, serving the Chairman (Mr. Davidson) and the members of the NIAC. He observed that the first meeting was largely organizational in nature and expressed his intention to keep it brief and to scope out some proposed tasks for the NIAC to consider and a suggested timeline for the body's work.

Mr. Clarke emphasized that the importance of the NIAC cannot be overestimated, noting that Al-Qaeda has specifically identified the nation's critical infrastructures as possible targets. Mr. Clarke stated that both the President and his administration greatly appreciate the value of the NIAC members' time and effort. Mr. Clarke turned the meeting over to Chairman Davidson.

III. Chairman Davidson's Welcoming Remarks

Mr. Davidson began by acknowledging that the NIAC has an awesome responsibility and he was honored to serve as its Chairman. He observed that the nation faces a horrific challenge because so many are intent on hacking into systems and disrupting commerce. Citing his own company, Union Pacific Corporation (UPC), as an example, he noted the increasing reliance that America's critical infrastructure operators place on integrated, networked information systems. He stated that the rail industry transports 40 percent of all goods in the U.S. and one-third of that traffic travels on Union Pacific lines. No matter what the industry, he observed, rail transportation provides support to it, for example, transporting chemicals for the water systems and much of the coal used by the electrical industry; transporting the military and supplies in case of war, etc.

Mr. Davidson said that although he himself is not a technician when it comes to computer systems, he had strong staff support to assist him in his role. He then introduced Rick Holmes, UPC's head of security for cybersystems. The Chairman then asked each member of the NIAC to identify a person on his or her staff with similar capabilities who could be called upon to provide staff support for the work of the NIAC.

IV. Briefing on Rules and Procedures Governing Federal Advisory Committee Proceedings and Deliberations (Part A – Ethics Briefing)

Chairman Davidson then introduced Arthur Warren, from the Ethics Division of the Commerce Department's Office of General Counsel, to brief the NIAC members on the ethics requirements associated with their work on the NIAC. Mr. Warren summarized the ethics requirements and rules for those serving on the NIAC, recapitulating information the members have received in documents previous provided to them by the Office of General Counsel. Mr. Warren thanked the members for their cooperation in submitting the financial disclosure information in a timely manner. He explained that the purpose of the ethics rules is to allow the NIAC members to serve effectively while protecting both them and the government from possible conflicts of interest (COI).

Mr. Warren explained that COIs arise when a member works on a matter before the NIAC in which s/he or his/her company has a interest that could be impacted favorably or negatively by the NIAC's action. For example, Mr. Warren cited potential conflicts pertaining to employment interests, personal investments, and investments of one's spouse, minor child(ren), or as a trustee. He instructed that the rules forbid a NIAC member from participating in NIAC deliberations or making recommendations about matters that affecting her/his personal interests or company. He noted, however, that the ethics rules provide an exception to this general principal: Specifically, if a matter would affect a member's company as one of a group of companies so affected, then the member can participate in NIAC work on the matter. However, Mr. Warren noted that this exception does not apply to matters that specifically or uniquely affect the member's employer (*e.g.*, a lawsuit, a contract award to the member's company, etc.). Mr. Warren also noted that mutual funds and stock investments also fall under the general exemption.

Mr. Warren then briefed the members concerning the scope of the waivers they had received following OGC's financial interest review. Mr. Warren noted that the Department of Commerce had issued individual waivers to the members based on the information the members had provided in their disclosure materials. He stated that the waivers will allow members to participate on general issues affecting those interests disclosed, but would not permit members to act concerning matters potentially impacting a member's employment or personal interests. He also reported that those members who had received waivers would each receive a copy it accompanied by the member's certified financial review report.

Mr. Warren emphasized that each NIAC member still bears personal responsibility to comply with the rules; however, he explained that his office and staff will continue to work with the NIAC and CIAO to assist members with these issues. He urged the members to read the ethics rules pamphlet included with their disclosure packages and asked them to call him, or one of the

other attorneys in the OGC Ethics Division, with any questions they may have. The telephone number to call with questions is (202) 482-5384.

V. Welcoming Remarks from Governor Tom Ridge

At this time, Governor Ridge, Special Advisor to the President for Homeland Security, joined the conference call. Following a brief summary from Mr. Clarke of the proceedings up to that point, Governor Ridge, for himself and on behalf of President Bush, thanked Chairman Davidson and the NIAC members for their service. He stated that the goal of homeland security presents a significant challenge for private industry because the country depends so heavily on the private sector to protect the nation's critical infrastructures. He briefly mentioned the National Strategy for Homeland Security, and explained that Administration's goal to develop strategic partnerships between different levels of government and private industry, noting with emphasis that 85 percent of the nation's critical infrastructures are owned by private industry. He stated, "Unless we work together, we will fall short of our goal – this is absolutely critical." He noted that most of the country will benefit from the NIAC's work and expressed his confidence that the NIAC understands how critical it is to protect both information and physical infrastructure.

Governor Ridge stated the three goals of the Administration's Homeland Security Strategy, namely, to identify:

1) What we need to do to prevent disruption/destruction of our critical infrastructures;
2) How we can work together to reduce vulnerabilities; and
3) In the event of a disruption in critical service, how we can restore capability/services as quickly as possible.

He then thanked the members again, and before leaving the call, expressed his hope one day to be able to meet with the members.

VI. Briefing on Rules and Procedures Governing Federal Advisory Committee Proceedings and Deliberations (Part B – Federal Advisory Committee Act [FACA] Rules Briefing)

Chairman Davidson then turned the floor over to Alice McKenna, an attorney from the General Law Division of the Commerce Department's OGC, to brief the members on the legal rules applicable to the work of the NIAC under the Federal Advisory Committee Act (FACA). Ms. McKenna started with a brief summary of the creation of the NIAC under Executive Order 13231 and a review of the requirements set forth in the NIAC Charter.

Ms. McKenna then stated that FACA contains elaborate requirements, both substantive and procedural, for meetings of Federal advisory bodies like NIAC. Noting that neither the FACA nor the NIAC Charter create a quorum requirement for the NIAC, she then cautioned that a "meeting" of the NIAC (triggering the rules) occurs at any time two or more members meet and discuss substantive NIAC business. Ms. McKenna stated that FACA requires that all meetings must be called by the DFO. Moreover, meetings must be announced to the public in advance by publication in the Federal Register. Finally, she noted, the meetings of the body must be open to

the public unless the subject matter to be discussed at the meeting is determined, in advance of the meeting, to fall within one of the four exemptions to the open rule requirement.

Ms. McKenna emphasized that all materials, minutes, etc., prepared by or for the members of the NIAC are government documents and will available to the public for review in a reading room to be created. She explained that any information exempt from public disclosure under the Freedom of Information Act (FOIA) may be redacted from such documents before they are placed in the reading room.

Ms. McKenna then addressed the issue of work by subcommittees or other subgroups or subordinate groups of the NIAC. She noted that, although meetings of such subordinate groups are not subject to the same rules as meetings of the NIAC (*e.g.*, no advance public notice is required, and they need not be open to the public), the rules and regulations concerning document retention do apply. In addition, because such staff work is not subject to such notice, all reports prepared by subgroups or subcommittees must be delivered to and deliberated upon by the NIAC itself. In this regard, only the members of the Council may participate in the NIAC's deliberations and decide upon and approve reports and recommendations of the body. Ms. McKenna closed her briefing by reminding the members that all questions pertaining to the NIAC should be directed to the attention of the DFO.

VII. Briefing on the Draft *National Strategy to Secure Cyberspace*

Next, Mr. Davidson called upon Mr. Clarke to brief the NIAC on the *National Strategy to Secure Cyberspace*. Mr. Clarke omitted the portion concerning the history of cybersecurity efforts (Slides 1-13) in consideration of the members' familiarity with that background information. Mr. Clarke explained that in October 1997, a report was issued, which observed that all of America's critical infrastructure systems were becoming increasingly dependent on IT/computer systems, and that this growing reliance on computer controlled networks had left the U.S. less secure as a nation. Mr. Clarke took note of the increasing interconnection of such systems to the Internet, which Mr. Clarke observed was never designed with security in mind. In October 2001, the President created an interagency board (the President's Critical Infrastructure Protection Board) to investigate these issues, and charged the Board to draft a national strategy to secure cyberspace. Mr. Clarke reported that the strategy was released in draft form on September 18, 2002, with the unusual step of soliciting comments from the general public. Part of the public comment process has been a series of "town hall" meetings asking for input. Mr. Clarke underscored that Government does not believe that it can dictate a Strategy to private industry. Rather, he expressed the view that a national consensus is necessary so that all stakeholders feel a sense of ownership.

(Slide 14) On behalf of the Board, Mr. Clarke requested that the NIAC review the draft Strategy and provide comments. (The outline is provided on Slide 14 and reviews threats and vulnerabilities.) He noted that Section III of the draft Strategy outlines guiding principles, one of which is "avoiding Federal regulation to control the protection of cyberspace." He reiterated that the Administration believes that cooperation is better achieved without regulation; however, he noted that the draft Strategy had been criticized as not relying enough on mandates or regulation. The fear of the Administration is that regulation would create a homogeneous policy or protections that would be easier to attack; the preference is to use market forces instead of the

Government's power to create a set of rules for cyberspace security. Mr. Clarke identified the five levels within the National Strategy:

(1) Home Users and Small Businesses;
(2) Large Enterprises;
(3) Critical Sectors;
(4) National Priorities; and
(5) International/Global.

Since there are many recommendations and no prioritization, Mr. Clarke suggested that perhaps the NIAC might want to prioritize the recommendations or consider adopting five overall priorities as a way of organizing the recommendations. He proposed the following five draft priorities:

1) **A national response system for cybersecurity events**. This would be a way to share the information quickly with everyone who needs it. A continuity and restoration system is also necessary.

2) **A national program to examine threats and vulnerabilities**. The draft Strategy does not say that we do not know what the vulnerabilities are, because the systems in each of the sectors have not all been tested. Under this category, we would pursue cyber criminals, find vulnerabilities and fix them, in all of the sectors, and also in the Internet and in current software.

3) **A national awareness and education program**. "Awareness" is defined as informing everyone involved with computer/IT systems, from the individual user at home and at work, all the way up through the CEOs and Chairmen of American's businesses. "Education" is training and certifying individuals in cybersecurity.

4) **Securing government networks**. This includes state and local governments (e.g., the 911 system)

5) **Achieving greater international cooperation on cybersecurity**.

Mr. Clarke asked the NIAC to consider whether these priorities make sense, cover everything that they should, and whether there is any other issue that should be made a priority that falls outside of these five.

Mr. Clarke continued, stating that some of the public comments concerning the draft Strategy received to date critically questioned why the Strategy was concerned with the home users, and how such users could impact national security. Mr. Clarke explained that home users have been included because their systems can be networked and used as a platform to attack the critical infrastructures. Mr. Clarke observed that banks feel that home users are very vulnerable if they have Internet connections through a DSL or cable without the protection of a firewall. Hackers have strung together networks of home users ("zombie networks") to launch Denial-of-Service attacks. In fact, E-Bay had experienced this phenomenon in the past.

NIAC members interposed the following questions and/or comments:

- *The draft Strategy does not manifest priorities. For example, in the list of the five possible priorities, nowhere does it state: "Secure private industry networks". Since the Strategy's goal is to have a private-public partnership, and the NIAC mostly consists of members from the private sector, looking ten years down the road, wouldn't the Administration want to open it up beyond the Federal, State and Local Governments and the 911 systems?* Mr. Clarke responded that he believed that concern is covered under Level II; the suggestion was made that the discussion be made more explicit as it is under Level IV.

- *In both the draft Strategy and in the possible priorities, the recommendations suggested would require quite a bit of time to implement. What should the NIAC look at for cybersecurity actions/protection that could be implemented immediately/short-term? Shouldn't there be a greater sense of urgency?* Mr. Clarke said that both types of actions were contained among the five priorities, but he would highlight them to make them more prominent.

- *Does the Strategy recommend that manufacturers make their systems more secure, especially for the home user? In addition, is the Administration considering whether to use the Federal government's buying power as leverage with manufacturers and suppliers?* Mr. Clarke pointed out that the draft Strategy, under Level IV, calls for the use of Federal procurement power as leverage with manufacturers and vendors. He observed that $52 billion is being spent by the Federal government on computers/IT this year alone, although this is just a small percentage of the overall IT procurement market. The Department of Defense has a program that will require Federal certification of IT products before procuring them. Mr. Clarke noted that Software and Internet protocols should be a subheading under Level II Vulnerabilities.

- *In reference to both Mr. Clarke's comments and those of other members, if the NIAC focuses on the "low-hanging fruit," could the Administration give the NIAC a sense of what/where is the "really tough nut to crack"? What is the highest risk? The private sector may not be as aware as they should be*. Mr. Clarke agreed.

- *In the draft Strategy, under Level III Awareness, the complexity of software and program performance needs to be understood; small businesses and users must be taught how to install firewalls and must be communicated to in an effective manner. They need to be educated on why cybersecurity makes a difference to them, and to the nation.*

- *How does research activity fit into the five priorities?* Mr. Clarke replied that it falls under Level II in vulnerability reduction for both the private sector and federally funded areas, with the hope that the two would feed off of each other. The Administration is developing a national plan for cyberspace-security research and development with Dartmouth to determine where and how to allocate the R&D. The Dartmouth team plans on talking to each sector to see how they all fit together.

- *There is a concern about outsourcing hardware and software code overseas – it does not seem to be addressed in the draft Strategy.* Mr. Clarke thought it was a good point and would be included in the next version of the Strategy. He agreed that there is a risk, but that such risk always exists regardless of where the code is written. Methods of quality assurance are necessary to ensure that no one person can damage software and operations.

As there were no other questions or comments, Mr. Clarke turned to Slide 25. He emphasized that although it is up to the NIAC to decide, he would propose that the members think about these issues, develop individual comments, circulate them, and compile them into a commentary for the President. He proffered the following six questions as a possible framework for the members' consideration of the draft Strategy, again stating that it is completely up to the NIAC members themselves to decide what to discuss:

1) Is the proposed National Strategy overall an appropriate response to the problem of vulnerabilities in computer networks supporting critical infrastructures? Have we placed appropriate emphasis on the problem? Is the overall thrust of our policy appropriate?

2) The proposed National Strategy does not call for new Federal mandates or regulations to address the issue; is that the right path?

3) The proposed National Strategy includes discussion of the home user and general citizen awareness; should it include such issues?

4) Are there key elements that are missing or given insufficient treatment?

5) Are there parts of the proposed National Strategy that your committee wants to especially call out as being important and with which the committee is in agreement?

6) We do not have a national assessment of our cyber infrastructure vulnerabilities. Such an assessment would require participation of the private sector. What recommendations does NIAC have for proceeding with such an assessment in cooperation with the private sector?

Mr. Clarke explained that a group of cyberspace professionals does not think the draft Strategy is strong enough, but no one really knows how vulnerable the nation's critical infrastructures are. Perhaps, he suggested, we should use the best "white hat hackers" to see if there are any problems. He stated that some testing is already occurring but there is not a real national net assessment program. He further asked how such test intrusions could be conducted on real, live systems such as the NASDAQ, for example, without undue risk? How would the owners of these systems feel about testing them? He also noted that liability issues would need to be addressed.

It was suggested that many problems are the result of poor practices, not poor code or design. This point, it was observed, is often difficult for people to "get our arms around" but, nevertheless, is an important point to consider.

Returning to the schedule, Mr. Clarke asked the NIAC members to compile their individual answers and comments into a document, and proposed that the NIAC meet again on November 26th to review the comments for final approval. At Mr. Davidson's request, Mr. Clarke said that both he and John Tritak would be available to assist the NIAC.

Mr. Davidson asked the members if they believed that the proposed timeline was doable. Mr. Clarke recommended that the comments be submitted to David Howe and Paul Nicholas of the PCIPB; John Tritak recommended that Eric Werner of the CIAO also be copied for the record.

Mr. Davidson suggested November 20th or 21st as the due date for submissions to the PCIPB and CIAO to allow enough time for all of the comments to be provided to the members by November 23rd. Mr. Clarke promised to send out copies of the six questions and the five priorities.

The members asked if they could receive feedback on the questions from other interested parties in the private sector, and also asked about the timetable for the release of the revised Strategy. On the latter point, Mr. Clarke stated that, if the changes recommended by the NIAC were generally in keeping with the five priorities discussed earlier (or were similar), a revised version of the Strategy could be completed in as little as a week because it would require only reordering points already contained in the document to emphasize the new focus.

Mr. Clarke also requested that each NIAC member identify and designate a staff member who could assist the member with NIAC-related tasks, so those persons could complete the financial disclosures and receive waivers, if required. In response to another question as to whether that person should be someone with experience in IT Security, Mr. Clarke left it up to the discretion of each member to designate a "substantive" other than an administrative assistant. The names should be e-mailed to Eric Werner by the beginning of the week of November 17th.

It was also noted that the NIAC might wish to consider creating lower-level subordinate groups, led by a member of the NIAC and including the "substantives" or staff. Mr. Davidson agreed that this made sense in order to help ensure the work is completed. Pursuant to a previous question, he was asked whether the NIAC could go to outside groups for input; Mr. Clarke referred the NIAC to the Executive Order, and stated that it was allowed.

At this point, the question was advanced that *although the NIAC is currently focused on the draft Strategy, how does the Administration see the NIAC moving forward?* Mr. Clarke mentioned importance of the five draft priorities and the need to build the private-public partnership; once the comments are submitted to the President, there will still be other work for the NIAC. Once the final Strategy is released, it would likely stimulate further ideas in the members, and the members should also think about possible ideas for the future as well.

Mr. Davidson emphasized again the need for the members to submit their comments in time for the next meeting on November 26th; John Tritak announced that guidelines for using subcommittees and outside groups would be provided. A final question was raised on how to control the number of subcommittees; Mr. Clarke said it was the responsibility of the NIAC. Mr. Tritak 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: 2/13/03
Richard K. Davidson, Chairman

Filename: NIAC Inaugural Meeting Minutes11-15-02
Directory: H:\Outreach\NIAC\MINUTES
Template: C:\WINNT\Profiles\werneret\Application Data\Microsoft\Templates\Normal.dot
Title: National Infrastructure Advisory Council (NIAC) Meeting
Subject:
Author: Wanda Rose
Keywords:
Comments:
Creation Date: 12/16/2002 2:55 PM
Change Number: 8
Last Saved On: 4/9/2003 10:59 AM
Last Saved By: werneret
Total Editing Time: 197 Minutes
Last Printed On: 6/4/2003 4:36 PM
As of Last Complete Printing
Number of Pages: 9
Number of Words: 3,805 (approx.)
Number of Characters: 21,691 (approx.)