

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

MEETING

Tuesday, July 22, 2003
11:30 a.m. – 1:30 p.m.

United States Chamber of Commerce
1615 H Street, N.W.
Washington D.C.

AGENDA

- I. Opening of Meeting:** Nancy J. Wong, *Director, Office of Planning and Partnerships, U.S. Department of Homeland Security (DHS)/Designated Federal Officer, NIAC*
- II. Roll Call of Members** NIAC Staff
- III. Opening Remarks:**
- Gen. John A. Gordon (USAF, ret.), *Assistant to the President and Homeland Security Advisor, Homeland Security Council*
- Lt. Gen. Frank Libutti (USMC, ret.), *Under Secretary for Information Analysis and Infrastructure Protection, DHS*
- Richard K. Davidson, *Chairman, President & CEO, Union Pacific Corporation; Chairman, NIAC*
- IV. Briefing on the National Security Telecommunications Advisory Committee (NSTAC):**
- a. Introductions:** Ms. Wong
- b. Briefing:** Dr. Vance D. Coffman, *Chairman & CEO, Lockheed Martin; NSTAC Chairman*, and Mr. F. Duane Ackerman, *Chairman, President & CEO, BellSouth; NSTAC Vice Chairman*
- c. Question and Answer Session:** Dr. Coffman, Mr. Ackerman, NIAC Members

V. Status Reports on Pending Initiatives

- a. Vulnerability Disclosure Guidelines:** Mr. John T. Chambers, *President & CEO, Cisco Systems, Inc.; NIAC Vice Chairman; and*
Mr. John W. Thompson, *Chairman & CEO, Symantec Corporation; NIAC member*
- b. Sector Interdependencies:** Mr. Martin G. McGuinn, *Chairman & CEO, Mellon Financial Corporation; NIAC member*
- c. Information Sharing:** Mr. Thomas E. Noonan, *Chairman, President & CEO, Internet Security Systems, Inc.; NIAC member*
- d. Role of Regulation** Ms. Karen L. Katen, *President, Pfizer Global Pharmaceuticals and Exec. V.P., Pfizer Inc.; NIAC member*

VI. New Business

Chairman Davidson, NIAC members

a. Composition of Remaining NIAC Vacancies

b. New Items

VII. Adjournment

MINUTES

NIAC Members present in Washington:

Ms Wong, *Designated Federal Official*; Chairman Davidson; Mr. Berkeley; Mr. Carty; Mr. Conrades; Mr. Edmonds; Ms. Grayson; Ms. Katen; Mr. Martinez; Mr. Noonan; Mr. Nye; Dr. Rose; and Mr. Webb.

Staff Designees Monitoring Proceedings on behalf of absent NIAC Members:

Ken Watson (for Vice Chairman Chambers), David Rose (for Mr. Barrett), Bobby Gillham (for Mr. Dunham), Michael O'Neill (for Commissioner Kelly), Chris Terzich (for Mr. Kovacevich), Teresa C. Lindsey (BITS, for Mr. McGuinn), Rob Clyde (for Mr. Thompson), and Bruce Larson (for Ms. Ware)

Other Dignitaries Present:

U.S. Government: General John A. Gordon (USAF, ret.), Assistant to the President and Homeland Security Advisor, Homeland Security Council; Lt. Gen. Frank Libutti (USMC, ret.), Under Secretary for Information Analysis and Infrastructure Protection, U.S. Department of

Homeland Security (DHS); Mr. Robert P. Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection, DHS; J. Paul Nicholas, Director, Critical Infrastructure Protection, Homeland Security Council; Cheryl D. Peace, Director, Cyberspace Security, Homeland Security Council

Others: Ms. Martha Marsh, President and CEO, Stanford University Hospital and Clinics (*new appointee to NIAC awaiting final processing*); Mr. Tom Lockwood and Mr. Chris Foster (on behalf of Robert L. Ehrlich, Jr., Governor of Maryland (*new NIAC appointee awaiting final processing*)); Dr. Vance Coffman, Chairman and CEO, Lockheed Martin Corporation, Chairman, National Security Telecommunications Advisory Committee; Mr. Duane Ackerman, Chairman, President and CEO, BellSouth Corporation, Vice Chairman, National Security Telecommunications Advisory Committee.

I. Opening of Meeting

The meeting was called to order and formally opened by Ms. Nancy Wong the Director of the Office of Planning and Partnerships for the Information Analysis and Infrastructure Protection (IAIP) Directorate and the Designated Federal Officer for the National Infrastructure Advisory Council (NIAC). After introducing herself and welcoming Chairman Davidson and the members and their staffs to the fifth meeting of the NIAC, Ms. Wong welcomed the representatives from the other cabinet departments and Federal Offices and the members of the press and the public on behalf of the Department of Homeland Security. Ms. Wong then asked Mr. Eric Werner of the NIAC staff to call the roll identifying the present NIAC members. After completion of the roll call Ms. Wong called to order the fifth meeting of the NIAC.

II. Opening Remarks

Ms. Wong opened the meeting by introducing General John Gordon, the Homeland Security Advisor and an Assistant to the President. She then explained that General Gordon's duties include developing interagency Homeland Security policy, advising the President during domestic incidents involving terrorism and natural disasters, and leading the Homeland Security Council staff. Ms. Wong then noted that prior to General Gordon joining the Homeland Security Council, he served as the Deputy National Security Advisor for combating terrorism at the White House and served as Under Secretary of Energy and Administrator of the National Nuclear Security Administration prior to joining the White House staff. She then turned the floor over to General Gordon.

General Gordon began by thanking Chairman Davidson, the members of the NIAC, and representatives of the National Security Telecommunications Advisory Committee (NSTAC) present. He expressed his gratitude that the NIAC was able to meet with the President prior to the day's Council meeting. General Gordon recognized the importance that the President places on cyber security, and on the NIAC. He encouraged the NIAC members to maintain their same high level of energy and commitment.

General Gordon then warned that cyber weapons are tested everyday in one form or another, and though this testing is done without cover, it is difficult to detect. He stressed the difficulty and

importance of defending against direct attacks from various sources, including terrorists, criminals, and amateur hackers, noting that cyber attacks, while dangerous in their own right, can also be launched as a prelude to a physical attack, thereby magnifying their potential for harm. He called the cyber threat both serious and real, and remarked that the NIAC is a visible sign of the importance placed on the partnership between the public and private sectors.

General Gordon recognized the NIAC's contribution to the development of the *National Strategy to Secure Cyberspace* and asked for the Council's further assistance in implementing the Strategy. He specifically noted the critical need to streamline the flow of information, and to ensure that the Information Sharing and Analysis Centers (ISACs) are effective, viable, and strong.

General Gordon then mapped the roles for the White House and DHS in coordinating these issues, observing that DHS is the operational lead on these matters, while the Homeland Security Council leads policy coordination to ensure that the process is "wired together" properly to enable all the pieces to work. Concluding his remarks, General Gordon thanked the Council and urged the NIAC members to continue to attack these threats aggressively. He then turned the floor over to General Libutti.

General Libutti opened by thanking General Gordon, Chairman Davidson, and the NIAC members for their attention and support of the Nation. He then stated that since his confirmation approximately a month ago, he has worked diligently with Secretary Ridge, Bob Liscouski (Assistant Secretary for Infrastructure Protection (IP)), Bill Parrish (Acting Assistant Secretary for Information/Intelligence Analysis (IA)) and others to bring together the disparate elements of IAIP into a smoothly functioning operational unit, capable of effectively responding to the new threat environment the Nation faces in the wake of September 11, 2001. General Libutti then applauded Commissioner Ray Kelly of the NYPD, his former boss and former marine, affirming that no one knows as well as he does the truth of Secretary Ridge's message that the nation's security depends on the security of its hometowns and cities.

Next, General Libutti outlined his duties over the past sixteen months, serving as the Deputy Commissioner for Counter-Terrorism of the New York City Police Department, where he was responsible for the prevention of, response to, and investigation of terrorist acts in New York City. He then reported that prior to his work as Deputy Commissioner, he helped stand up the Office of Homeland Security for the Department of Defense while serving as the Special Assistant to the Executive Agent for Homeland Security. General Libutti continued describing his work history, pointing out his 35 years of service in the U.S. Marine Corps, during the last nine years of which he routinely dealt with operational and strategic issues at the national level, including the Nation's major war plans and humanitarian operations.

After discussing his career highlights, General Libutti focused attention on his current position as Under Secretary, where he asserted that his job is to muster and motivate the resources of the IAIP Directorate to accomplish the mission of IAIP: delivering an integrated, end-to-end capability to identify and assess current and future threats to the homeland; map those threats against the nation's vulnerabilities; coherently and efficiently communicate 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 in the wake of a crisis event. He then declared that significant progress has been, and continues to be made in the IAIP Directorate and acknowledged the quality of the people comprising IAIP. General Libutti recognized that there is work to be done to refine IAIP's organizational skill-set, but avowed his confidence that IAIP can handle today's challenges, and that IAIP will handle them with increasing skill and aplomb.

General Libutti concluded his remarks stating that Ms. Wong had briefed him regarding the important work undertaken in the areas of sector interdependencies, information sharing, vulnerability disclosure, and regulation; and acknowledged how difficult an undertaking it is to take on these four challenges on the national agenda for IAIP. He then expressed his anticipation for the remainder of the day's working groups and turned the meeting over to Chairman Davidson.

Chairman Davidson thanked General Libutti and applauded the President's appointment of a hard working group of dedicated people who serve their industries and the country and comprise the NIAC. Acknowledging General Gordon's remarks, he then introduced a few of the day's issues, commenting that one of the subcommittees is working on the ISAC issue regarding the barriers to effectively sharing information between the government and private sector. He then asserted another key issue is vulnerability recognition, and the appropriate timing for sharing vulnerabilities. Chairman Davison reiterated the fact that the Council has indeed taken on four difficult issues, and that the subcommittees are working diligently to resolve the issues in the near future.

The Chairman also introduced two new appointees to the NIAC: Martha Marsh, the CEO of Stanford Hospital and Clinics and the Governor of Maryland, Robert L. Ehrlich, Jr. Chairman Davidson then welcomed the Chairman and the Vice Chairman of the President's NSTAC, commenting that their presence afforded a valuable opportunity for the NIAC to learn about the NSTAC and for the two panels to open a dialogue about their respective initiatives and to begin to share. He encouraged the NIAC members to participate actively in the NSTAC discussion and to ask questions. He then asked Nancy Wong to introduce the NSTAC representatives.

III. Briefing on the National Security Telecommunications Advisory Committee [For additional information see Attachment A.]

Ms. Wong introduced the NSTAC discussion by asserting that the telecommunications systems make up the backbone of information highway on which many of the Critical Infrastructures have built their business operations, their business efficiency and productivity, and new service capabilities. She explained that NSTAC advises the President on all telecommunications aspects affecting National Security and Emergency Preparedness (NS/EP). Ms. Wong then introduced Dr. Vance D. Coffman Chairman of the President's NSTAC and chairman and CEO of Lockheed Martin Corporation and Mr. F. Dwayne Ackerman Vice Chairman of the NSTAC and Chairman and CEO of the Bell South Corporation. She then welcomed Dr. Coffman and Mr. Ackerman and turned the floor over to Dr. Coffman.

Dr. Coffman thanked the Council for the opportunity to talk about NSTAC. He then provided some of NSTAC's background, explaining it was formed in 1982 under a directive from President Ronald Reagan and it has been renewed every two years since. Dr. Coffman asserted that NSTAC's focus then and now is national security/emergency preparedness (NS/EP) telecommunications. He commented that he is the chairman for the 27th cycle, and Dwayne Ackerman will take over as chairman during the 28th cycle. He noted that NSTAC brings major telecommunication industry people to the table and works issues that no single Point of Contact (POC) in the industry could work. He further explained that some of the key government concerns which fostered the need for NSTAC included the potential impact of new technologies for the NS/EP issues, the increased government reliance on commercial industries, the growing importance of command and control systems, and the increased dependence on communication activities to drive disaster relief. Dr. Coffman attributed NSTAC's success to the environment of trust regarding information sharing, thus allowing cross-sector information sharing without proprietary issues. Dr. Coffman then highlighted the three NSTAC informational areas he believed worthy for discussion.

1. NSTAC recommended founding the National Coordinating Center for Telecommunications in 1984. There, industry representatives work with government on a continuing basis regarding the responsibilities surrounding crisis management.
2. NSTAC recommended the Telecommunications Service Priority Program in 1986. Its mission is to resolve regulatory and administrative framework related issues in terms of priority provisioning for networks and restoration of NS/EP telecommunications service when a crisis exists.
3. NSTAC recommended the Wireless Priority Service in 1994. It provides an end-to-end nationwide wireless priority communications capability to NS/EP personnel during disasters. Use of a special access code has been developed, and is required to ensure that those with the incorrect type of information to be transmitted do not use the system.

Dr. Coffman then turned attention to the NSTAC's priority list of tasks including:

1. Legislative and Regulatory Task Force (LRTF) – focuses primarily on information sharing issues as well as penalties associated with cyber-crime and wireless priority service issues;
2. Research and Development Task Force (RDTF) – focuses on the continuation of conducting Research and Development associated primarily with NS/EP issues, and builds a community of both industry and government representatives in the process of executing research and development;
3. Financial Services Task Force (FSTF) – focuses on the banking communities and insurance communities, which rely heavily on access to telecommunications based activities;
4. NSTAC Outreach Task Force (NOTF) – focuses on communicating NSTAC's mission, its responsibilities, and issues to governments, academia, and other industry participants,

so that those participants know there is a voice available to them in the system, and when a concern arises, how they can use that voice;

5. Satellite Task Force (STF) – focuses on determining the potential mitigation efforts, determining whether foreign ownership of satellites is an impediment to the security of commercial satellite infrastructure, and whether the practice should be continued; and
6. Trusted Access Task Force (TATF) – focuses on developing guidance for national standards and capabilities for National Security background checks, including screening and national crime information center reviews, so that those people controlling telecommunications assets are trustworthy individuals that will function in the nation's best interest if and when an emergency occurs.

Dr. Coffman then requested questions and comments from the NIAC members. Chairman Davidson inquired about the research paper from the George Mason Student who wrote about the access provided by the fiber optic cables to all the businesses and critical facilities in the U.S. He asked if this provokes some questions about how public information should be.

Dr. Coffman responded that the vulnerabilities issue involves telecommunications hotels where common infrastructure is massed mostly for efficiency purposes and it also involves the ability of individuals to penetrate networks both on a hardware basis and a logic basis, which could give pause in terms of future threats to both the country and involved businesses.

Mr. Edmonds then raised the issue of sector interdependencies, referring to the last NSTAC slide concerning vulnerabilities. He noted that many of the infrastructure sectors represented by the members of the NIAC depend on the telecommunication infrastructures that Dr. Coffman and Mr. Ackerman represent. Given this fact, Mr. Edmonds asked what the NSTAC and DHS are doing to prevent the vulnerabilities like those in the slide from impacting other sectors like banking and transportation.

Dr. Coffman responded that the telecommunications industry has tended to focus on its own issues. However, he stressed that he is fully aware of other sectors' dependence on telecommunications, noting that major gas-lines and railroads for example, depend on the telecommunications industry for their interconnected systems, whether over the internet or through their own networks. He pointed out that the NSTAC is looking at telecommunications vulnerabilities and threat issues and that he expects to have answers at the NSTAC's Spring meeting.

Mr. Ackerman commented that the telecommunications infrastructure has a physical layer, and while all vulnerabilities are not completely understood, the infrastructure has a reasonably good understanding of what vulnerabilities exist in the physical layer. He explained that once the broadband environment is reached, the logical layer begins to overlay, and that's where the Internet, voice over IP, and the actual integration of the logical layer with that physical network come into play. Dr. Coffman clarified that once the logical layer is reached, the security issue becomes broad and multiple players are involved. He then expressed that narrowing the threats at the logical layer while improving and nailing down the physical layer will be a continuing challenge.

Chairman Davidson thanked Dr. Coffman and Mr. Ackerman for their insights and reemphasized the importance of telecommunications to the other infrastructure sectors. He noted that the NIAC would, later in the meeting, consider a proposal to recommend to the President that a representative of the telecommunications sector be appointed to the NIAC.

IV. Status Reports on Pending Initiatives

a. Vulnerability Disclosure Guidelines [For additional information see Attachment B.]

After concluding the briefing on the NSTAC, Chairman Davidson began the Status Report on Pending Initiatives by introducing Rob Clyde of Symantec and Ken Watson of Cisco and turned the floor over for discussion of vulnerability disclosure guidelines.

Mr. Watson began by describing the Inter-network Operating System (IOS) software vulnerability Cisco disclosed the previous week. He stated that Cisco created a software fix and work-around solution and followed an established process to notify the customers to address the issue. Mr. Watson explained that there had been no confirmed reports of an outage or a successful exploitation of this vulnerability, and based on customer feedback Cisco believes that the likelihood of any successful attack will continue to diminish over time. He then expressed his opinion that both the full-disclosure and limited-disclosure arguments have merit and that the Vulnerability Disclosure Working Group is trying to accommodate both points of view while developing general guidelines. Mr. Watson recognized that it would take time for the Internet community to fully appreciate the benefits of vulnerability disclosure guidelines even after researchers, security companies, vendors, and governments accept them. He then turned the floor over to Mr. Clyde.

Mr. Clyde thanked Mr. Watson, and explained that the working group had been developing a reasonable vulnerability disclosure framework to serve as a reference tool for security professionals and other involved parties when a new vulnerability is discovered. He indicated that new vulnerabilities continue to be discovered, and that there are differing opinions among industry leaders as to how best to inform the public about potential vulnerabilities. He asserted that the conflicting views have hindered robust sharing of threats and vulnerabilities between industry and government, which is the key to proactively protecting the National Critical Infrastructure.

Mr. Clyde described the Vulnerabilities Disclosure Working Group stating that its purpose is to provide guidance through the development of a beginning-to-end framework for the notification, investigation, disclosure, and resolution of discovered and reported network security vulnerabilities. He explained that the framework would include recommendations to the President as to how to improve the information sharing process, including steps that can better secure the nations critical assets. Mr. Clyde reported that research has included sifting through best practices regarding process related issues including, but not limited to, defining a vulnerability, determining its severity, and notifying the public. He noted that the working group has outlined the scope and mission of the proposed framework at several industry conferences to gauge its receptivity and that feedback has generally been positive and encouraging.

Mr. Clyde then outlined the working group's key actions to date on their deliverables:

1. Established the scope for the document including the identification of the many roles of key individuals and organizations in the vulnerability disclosure process;
2. Created a vulnerability scoring group to find consensus regarding the differing views on defining the severity of a vulnerability;
3. Developed presentations to solicit feedback and comments from targeted industry organizations as to the direction of the working group's activities; and
4. Incorporated significant input from the working group members.

Mr. Clyde then turned the floor back over to Ken Watson to explain the working group's methodology, the next steps, and highlight the areas where the working group is seeking guidance from the NIAC.

Mr. Watson discussed the working group's initial data gathering efforts reporting that they drew from a number of sources including the working group members, a Computer Emergency Response Team (CERT) Coordination Center vulnerability questionnaire, other submitted industry best practices, and various contributing research papers, articles, and case studies. He stated that the working group created presentations and organized birds-of-a-feather sessions at that year's North American Network Operators' Group (NANOG) and the Forum of Incident Response and Security Teams (FIRST) conferences in Advanced Computing Systems Association (USENIX). Mr. Watson commented that after looking at several threat and vulnerability scoring methods they decided that a common scoring methodology is needed to support the framework because the existing scoring methods yield different results for the same vulnerabilities that run through the process and most often do not correlate well. He reported the working group was in its final stages of reviewing the draft framework, prior to soliciting additional feedback and peer review from a select audience. This, Mr. Watson noted, is expected to be completed in August, and a final version will be delivered to the NIAC members for review shortly afterward.

Mr. Watson requested feedback from the NIAC members regarding the following three statements:

1. The working group believes that general guidelines will be more useful than a U.S. Federally centered policy.
2. The scope of the process may need to be expanded to consider the specific requirements and implications in the case of a vulnerability directly impacting National Security.
3. Given that the internet is global and that the vulnerabilities affecting the U.S. Information Technology (IT) infrastructure also impact other connected nations, a strategy should be developed to promote the resulting framework to the larger U.S. audience and internationally.

Mr. Watson then asked the NIAC members if there was any specific guidance that the working group should consider regarding the three issues he raised. Mr. Noonan responded that writing

descriptive guidelines not prescriptive policy is still appropriate and that it is certainly the best step before regulative or legislative policy. He advised that the challenge is going to be finding the middle ground where guidelines are descriptive yet sustain the input, both negative and positive.

Mr. Watson thanked Mr. Noonan and explained that the working group's original thought was to develop a national vulnerability disclosure policy, but the group came to the conclusion that it couldn't be applied nationally because vulnerability disclosure is an international issue. He stated that guidelines are needed that can be generally useful for those that discover vulnerabilities in the research community, vendors that have to create the solutions, government agencies that are part of the notification and National Security process, and the user community that ends up having to implement the solutions to vulnerabilities that are already out there. Mr. Watson restated that what the working group would like to know is whether it is still appropriate to be descriptive rather than prescriptive in the overall paper.

Ms. Katen responded that she represents the subcommittee looking at regulation versus non-regulation. She confirmed that the majority of the subcommittee agrees with the argument for a descriptive rather than prescriptive approach and that guidelines are better than strict regulation. Ms. Katen warned however, that no one-size-fits-all type of approach would be the answer for the diverse sectors, particularly in the area of vulnerability disclosure.

Mr. Webb also agreed with guidelines rather than prescriptive policy and asked that the working group look into guidelines for responding to companies or industry that don't comply. Mr. Noonan commented that getting to the point where companies and industries know what compliance is or isn't would be a great first step. Ms. Katen asked the Vulnerability Disclosure Working Group to speak more about the scorecard on vulnerabilities proposal.

Mr. Watson responded that the Vulnerability Disclosure Working Group has a scoring subcommittee that has started looking at the available scoring methods. He reported that ISS, Symantec, the CERT Coordination Center at Carnegie Mellon, Microsoft, and Cisco all have scoring methods. He explained that the working group has created a matrix and ran several vulnerabilities through that matrix to see if the scores correlated at all. Mr. Watson asserted that the scores didn't correlate and that each of the scoring methods had a different customer-set. He reaffirmed the need for a common scoring methodology to serve as a framework for all guidelines. Mr. Watson commented that when the working group finishes its report, it would most likely recommend a 6-month research project be conducted by the NIAC to develop a common scoring methodology.

Mr. Conrades then expressed confusion as to whom the guidelines or the policy would apply, and whether they would be aimed at the vendor once a vulnerability is known and if the discoverer, who is often not the vendor has some obligation under these guidelines. Mr. Watson replied that no one has a legal obligation to comply with guidelines. He further explained that the working group is trying to produce a reference book that can be used as a general guideline by discoverers, vendors, users, and the government. However, he added that the working group does plan to include specific policy recommendations for the Council to consider sending to the

President. Mr. Clyde added that the document contains specific guidelines for each role (e.g., discoverer, vendor, user, etc.).

Mr. Conrades further stated that he understands the vendor process, and why that would be more self-regulated but he was less certain about what, if any, responsibility a discoverer actually has. Mr. Clyde responded that most discoverers are looking for guidelines and are anxious to receive credit for their work, which they can get by following the process. He observed that it would not be possible to get everyone to comply every time, but the vast majority will. Mr. Watson added that it was the working group's experience that most discoverers have been easy to work with, want to support the public, are interested in security, and want to work with vendors and government agencies to ensure that the timing of these advisories benefits everybody.

Assistant Secretary Liscouski then interjected that the four issues on the table could not be "de-coupled", that looking at any one in-depth requires looking at all the issues, because in writing guidelines and discussing the disclosure requirements there's a national security implication that drives what is, and is not disclosed. He further urged scrutinizing what should be disclosed to international partners while maintaining a national security perspective.

Mr. Liscouski then expressed that he is deeply interested in, and more importantly, actively engaged in working these issues and affirmed his desire to use where it is appropriate, resources from the National Cyber Security Division to improve the process. He added that there is a great deal of work to be done, which if staged correctly will add value to the vendor community, the consumer community, and the National Security Community. Mr. Liscouski then turned the floor back over to Mr. Watson.

Mr. Watson concluded his remarks stating that the working group determined that their initial timeline was too aggressive given the number of issues to resolve and that their revised timeline places delivery of their final draft to NIAC members in one month. He further explained that the working group expected the final version to be ready for presentation to the President for the October NIAC meeting. Mr. Carty then asked whether the working group's revised timeline included development of a final scoring system. To this Mr. Watson responded that the working group was unsure whether the scoring system could be developed in time, and most likely additional time would prove necessary to finish that part of the project.

Chairman Davidson then thanked Mr. Clyde and Watson and introduced Chris Terzich of Wells Fargo to update the Council about Sector Interdependencies.

b. Sector Interdependencies [For additional information see Attachment C.]

Chris Terzich introduced Teresa Lindsey as a fellow member of the Sector Interdependencies Working Group and stated their objectives are to 1) develop guidance on cross-sector interdependencies with the ultimate result being policy advice, 2) develop common definitions around critical infrastructure not only within a sector, but within an organization and specific processes, 3) develop a model for crisis management that functions not only within each sector, but across the sectors, 4) develop a method to effectively share best practices, 5) develop the national strategy for DHS and other national documents, and 6) develop critical infrastructure

definitions. Mr. Terzich explained that his working group consists of NIAC member institutions as well as participants and Sector Coordinators from Energy, Information, Telecommunications, Financial Institutions, and Water.

Mr. Terzich noted that the working group's research included an inventory and review of all the available studies and assessments about cross-sector vulnerabilities and vulnerabilities within certain sectors; briefings from electrical power, financial services, and railroads regarding their sector crisis management processes; and briefings from the National Infrastructure Simulation and Analysis Center (NISAC) concerning modeling of sector and cross sector vulnerabilities. He noted that based on the working group's research they would recommend:

- Telecommunications should be recognized as an infrastructure separate from Information and that a telecommunications CEO be appointed to the NIAC;
- Each critical infrastructure should have a consistently appointed and consistently funded Sector Coordinator;
- Development of sector crisis plans with a clear accountability for testing and include common terminology, response organizations, resource management, and communication protocols; and
- Development of crisis management plans, which can be used throughout the critical infrastructure sectors.

Mr. Terzich then expounded on the issue of Sector Coordinator role, stating that their roles are not broadly understood and with that lack of understanding follows a lack of effectiveness. He commented that one of the responsibilities of the Sector Coordinator would be to ensure that there is a crisis management plan and that it works with all the other sectors based on their vulnerabilities. Mr. Terzich posed the following questions to the Council:

- How does the appointment process for Sector Coordinators work?
- Should the nomination come from within the sector to be ratified by the lead agency?
- At what level is the authority of the Sector Coordinator?
- Does each sector need to have a coordinating Council?
- How do we connect the Sector Coordinators to the CEOs of the companies within that sector?
- Should the Sector Coordinator be affiliated with specific private entities or some other entity?
- Should the role of Sector Coordinator be full time?

Mr. Noonan asked, if each industry needs a Sector Coordinator, who will appoint the Sector Coordinators, and do they have similar obligations in terms of response. To this question Mr. Terzich responded that Presidential Decision Directive (PDD)-63 states that each of the critical infrastructures would be represented by a Sector Coordinator and the lead agency for that

infrastructure would appoint the Sector Coordinator. He also indicated that all the critical infrastructures will have Sector Coordinators.

Ms. Lindsey offered additional information explaining that the working group mapped the critical infrastructures, and found that not all critical infrastructures have Sector Coordinators; some have not yet been appointed. She further commented that the working group also mapped the sectors with designated Sector Coordinators against the list of Sector Representatives by the NIAC's membership to determine which NIAC members have Sector Coordinators for their sectors. Ms. Lindsey confirmed that even though the Sector Coordinator role is not broadly understood they are the lynchpins for coordinating and working out the cross-sector interdependencies. She then turned the floor over to Nancy Wong.

Ms. Wong explained that the role of the Sector Coordinator was written into PDD-63 decision directive before DHS was created. She pointed out that a set of best practices has emerged for Sector Coordinators resulting in IAIP gathering, documenting, and sharing those best practices with the working group. Ms Wong warned, however, that there has been no consistency in execution, but stressed that IAIP we will be disseminating some consistency in the execution and compliance of the roles and responsibilities of the Sector Coordinators.

Mr. Edmonds then commented that there is a real the lack of a command center and a command function and recommended that the NIAC create a focal point, either virtual or physical where the Sector Coordinators can come together. He further noted that Sector Coordinators need to sit in the same physical or virtual space to be connected. He affirmed that once exercising begins the concept becomes real at which point a clearinghouse for the lessons learned will be needed. Mr. Edmonds further recommended that timelines be created so that the concept can be supported, both on Capital Hill and in the administration.

Chairman Davidson then seized upon the working group's observation that the lack of a Sector Coordinator in some sectors, or a clearly defined role for the Sector Coordinator, presents a serious challenge. He suggested that the working group could add real value by trying to bring some clarity and focus to these "areas of opportunity". Chairman Davidson further stated that by "teeing up" such critical weak spots the working group could enable the members working through the Council and within their respective sectors to take action to ensure these deficiencies are addressed.

Assistant Secretary Liscouski reported that many of the issues previously pointed out are works in progress for DHS, supported by its sister agencies. First, he noted that while looking at interdependency issues, it is often valuable to have a clear picture of the threat that confronts a particular infrastructure or facility and how it transcends to other infrastructures as well. He extended those NIAC members with appropriate clearances an invitation to attend DHS briefings regarding threats to critical infrastructure so that they can better understand that important contextual element which impacts interdependency and crisis planning. Second, he noted that DHS has initiated action on development of national coordination centers. He observed that a lesson of the TOPOFF 2 exercise is that communication at all levels, government as well as into the private sector is absolutely critical to manage events. He then deferred to Under Secretary Libutti to discuss these points further.

General Libutti emphasized DHS's willingness to reach out, both in terms of sharing information so that the NIAC members can understand and appreciate the threat landscape. He stated that DHS has put an initiative on the table to stand up a world-class command center for Homeland Security. He further noted that there are other command centers, both in FEMA and TSA and the rest of the twenty-two organizations that comprise DHS, and that IAIP, on behalf of Secretary Ridge is looking at how to consolidate these efforts more effectively. Chairman Davidson introduced Tom Noonan to discuss the issue of Information Sharing.

c. Information Sharing [For additional information see Attachment D.]

Tom Noonan introduced himself as the Chairman and CEO of Internet Security Systems (ISS) and Pete Allor, the lead officer for the Information Sharing Working Group effort. Mr. Noonan commented that information sharing and analysis is erratic, that there are pockets of excellence where ISACs are performing well and ISACs that have no money. He stated that the Information Sharing Working Group's goal is to determine best practices and to leverage those best practices in coordination with the IAIP's work at DHS. Mr. Noonan then turned the floor over to Mr. Allor's Group's to discuss the progress to date.

Mr. Allor affirmed that the working group is anticipating a closing date around the middle of October and explained the Information Sharing Working Group's task is to review the current state of information sharing and analysis. He commented that the working group would make specific recommendations to the NIAC for their review and later on pass on the recommendations to the President. Mr. Allor noted that part of the working group's continuing mission is fostering communication among the ISACs and between the ISACs and DHS and other elements of the Federal government. He reported that the working group has monitored the ISACs as each reviews their business models, financial models, their ability to continue operations, and operational matters, including Telecommunications, Information Technology, Financial Services, Surface Transportation, Trucking, Energy, Electric Power, Water, Chemical, and Health Care.

Mr. Allor remarked that the working group is also planning to solicit additional feedback from the major ISACs and the ISAC Council. He commented that the working group broke their work down to four objective groups.

- Business models – how they operate and what are the considerations related to information sharing?
- Financial models – how should information sharing be funded?
- Level of information analysis and aggregation – how should analysis at the industry level be aggregated?
- Communication – how to communicate with government, and do so in a secure and protective manner?

Mr. Allor stated that the working group is looking at the ISACs in their formative time as being the future. He then asked how vulnerability information, remediation, and best practices should

be disseminated to the entire sector regardless of membership and how that information should be vetted, categorized, and protected. Mr. Allor emphasized that the value of proposition is in consolidation of information, the analysis of that consolidated information, and development of actual information for enactment. He further stressed the need for propagating relevant information, that announcing that a vulnerability exists in a particular product is not sufficient. Mr. Allor asserted that the important question is how to transmit relevant information in a timely, and most importantly secure manner. He then asked for questions and comments?

Tom Noonan affirmed his belief that the financial models are paramount to creating a solid foundation for cross-industry information sharing. He acknowledged that the working group had initially raced forward with ISACs as the basis for sharing information when they didn't fully understand the cost and the financial model compared to the scope of cross-industry information sharing, but research and the support of the NIAC has been a boon to their project. Chairman Davidson thanked the Information Sharing Working Group and introduced Karen Katen to discuss the final of the four issues, the role of regulation.

d. Role of Regulation [For additional information see Attachment E.]

Ms. Katen explained that she would be updating the Council regarding the progress the Role of Regulation sub-group had made in developing policy. She began by outlining the sub-group's three objectives, which were to: 1) assess the impact of regulation on each sector; 2) identify where regulation might improve security or reduce risk; and 3) determine the most effective drivers of security improvement in each sector. Ms. Katen noted that after speaking with the NIAC members and their delegates, it became clear that their study was different than those of the other groups and sub-groups. She explained that where the other groups were recommending changes to regulations, their group uncovered a great difference of opinion about the role of government itself, and in light of these differing opinions they interviewed the NIAC members to glean the areas of accord and discord, and focused on identifying the few core questions that had to be addressed in the final recommendations.

Ms. Katen then illustrated the wide-ranging views concerning the role of government with a pie chart dividing the three positions. She noted the largest group favored market oriented approaches as the primary way to address the nation's security problems, the second - marginally smaller - group believed that the market would work to drive change if government points the way, and a small minority feel that special circumstances prevent market forces from working effectively in their industry or sector.

Ms. Katen clarified that the first group, "market faithful," comprised a disproportionate number of technology-oriented companies and has a strong belief that markets respond faster and innovate around challenges better than government. She explained that this group believes that in a world where the enemy is constantly probing and challenging the nations defenses, a more rapid response is needed across a broader front than the machinery of government can manage. Ms. Katen pointed out that in their competitive world companies that don't provide secure products are eliminated, and that this Darwinian process enables them to maintain robust defenses. She explained that they feel allowing firms to tailor their security requirements to their

individual needs is the most effective way to optimally deploy resources to meet each industry and every company's needs.

Ms. Katen continued with the second group, which believes there is an important role for government in setting direction for companies. She explained that some pointed to the difficulty getting companies to invest in protection against rare but catastrophic events while the obvious threats are well funded. Ms. Katen stressed how difficult it is to determine the level of protection that is needed for rare catastrophic events in the absence of good tools for describing and quantifying risks. She explained that some feared that in the absence of regulations, well-managed companies would invest in security protection whereas poor performers might cut corners, in effect penalizing the good companies for taking proper action. Ms. Katen noted that they prefer that security regulations be spelled out so that everyone completed on a level playing field.

Ms. Katen moved on to the third group, those who were skeptical of the ability of market forces to work for them at all. She remarked that this group was concerned that the economic viability of their own company might be threatened. Ms. Katen noted that others found it challenging to get investments at the state and local level in new security measures when budget discussions were already difficult to resolve. Finally, she asserted that both groups felt that in the absence of new funding or incentives at the Federal level they were doubtful that the security of the nation would be secured.

After discussing the differing points of view regarding government regulation, Ms. Katen outlined the Role of Regulation Working Group's agenda. First, Ms. Katen noted is determining how to introduce performance standards without loss of innovation. She stated her group recognizes that there are some sectors where innovation is essential to enhanced security, but her group also hears the strong opinion voiced by others requiring guidance on what is an acceptable level of risk. The answer, Ms. Katen asserted would probably lie in a sector-by-sector assessment of what drives better security, and a more flexible, tailored recommendation on government's role.

The second item, Ms. Katen stated is determining how to sustain top management attention when events are infrequent. She explained that many people felt government guidance had an important role to play through documentation of what good practice is, and suggested government could perhaps be laying out the "what" in security and physical protection without mandating the "how". Ms. Katen reported a great difference of opinion on whether there should be "light touch government" with publication of best practices and recommended guidelines, or there should be a role for government in enforcement of these practices with defined standards, official oversight, and punitive damages for non-compliance.

The third item, Ms. Katen remarked is determining how to motivate the consistent application of best practices across all players within an industry. She explained that in the banking sector one weak player failing to comply with required standards might lead to damage rippling through the entire industry. Ms. Katen reported strong support among these NIAC members for the new banking regulations, for official oversight bodies, and for guidelines underpinned by strong enforcement mechanisms. She asserted that almost all participants spoke of the existence of

good oversight bodies today for their industry, with extensive knowledge of the local issues, and felt that they could work with pre-existing agencies and regulatory bodies to shape future legislation or guidelines.

The fourth item, Ms. Katen stated is aligning the private and public sectors more effectively across interdependent systems. She reported a great deal of praise for Federal and local government disaster planning, and for exercises such as the TOPOFF event in Chicago to prepare for future threats, but these are still largely government-only exercises. Ms. Katen explained that in real emergency events the interaction of public sector agencies with private transportation, private communications, and private service companies is generally responsible for successfully restoring order. She asserted that better joint information exchange and planning would be essential in securing a swift future response to emergency situations.

The final item, Ms Katen reported is determining how to make the nation more resilient to systemic effects when security breaches do occur. She reported all participants felt that complete prevention of any attack was impossible regardless of whether the threats are physical or cyber-security related. Ms. Katen advised that plans for disaster scenarios should address not only the prevention of events but also mechanisms for recovery, to ensure that restoration of order is achieved as swiftly as possible. She further asserted the need to be better prepared for recovery from tragic events.

Upon completing the review of the Role of Regulation Group's agenda, Ms. Katen moved on to timetables. She noted that her group would, for the most part follow the same calendar as other groups, with the team taking until late September to resolve their issues and present findings in early October. Ms. Katen reported that the group has already assembled a preliminary team of NIAC members and delegates who have offered their help. She requested involvement from those who have not been able to participate yet, and expressed the group's desire for the broadest possible engagement from the NIAC members.

Mr. White expressed his belief that regulation is the most difficult and most important step in gaining public acceptance. He recommended cataloging the entire range of regulatory interfaces and stated that there is a large number of models in the United States. Mr. White further explained that there is direct regulation in the FCC model of telecommunications companies and indirect regulation of lawyers through the American Bar Association. He concluded by affirming that engaging millions of Americans in protecting the nation will succeed or fail based on how these regulatory interfaces work.

V. New Business

a. Composition of Remaining NIAC Vacancies [For additional information see Attachment F]

Mr. Davidson mentioned that the Telecommunications industry plays a critical role in infrastructure protection; however they are not represented on our committee. He then mentioned the proposed letter to the President requesting that someone be appointed to the NIAC from this sector. He then called for a vote recommending that the letter be sent. All were in favor and the motion passed.

b. New Items

No new business was introduced.

VI. Adjournment

Chairman Davidson 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
Richard K. Davidson, Chairman

Dated: 10/20/03

ATTACHMENT A

*(National Security Telecommunications Advisory Committee
Briefing Materials)*



NSTAC Success Stories

- National Coordinating Center for Telecommunications (NCC)
- NCC Telecommunications Information Sharing and Analysis Center (NCC Telecom-ISAC)
- Government Emergency Telecommunications Service (GETS)
- Information Sharing
- Wireless Priority Service (WPS)
- Telecommunications Service Priority (TSP) program
- Telecom vulnerability and survivability assessments
- Telecom industry engagement in Critical Infrastructure Protection (CIP) issues
- Network Security Information Exchange (NSIE)
- Network convergence studies
- Enhanced call completion studies
- Critical telecom facility protection
- Telecommunications interdependencies
- Commercial satellite survivability
- Last mile bandwidth vulnerabilities
- Wireless security studies (802.11, etc)
- Various issues related to classified matters
- And much more




Making a Difference

National Coordinating Center for Telecommunications:
(NSTAC recommended in 1984)

- Industry representatives work with Government during day-to-day operations and coordinate NS/EP responses during crises
- Facilitates industry-Government interaction, exemplified on 9/11

Telecommunications Service Priority Program:
(NSTAC recommended in 1986)

- Regulatory, administrative and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications service

Wireless Priority Service: (NSTAC recommended in 1994)

- Will provide an end-to-end nationwide wireless priority communications capability to NS/EP personnel during disasters




NSTAC Task Forces


For the NSTAC Cycle XXVII (May 2003 - Present), the NSTAC has six task forces

- 1** Legislative and Regulatory Task Force (LRTF)
- 2** Research and Development Task Force (RDTF)
- 3** Financial Services Task Force (FSTF)
- 4** NSTAC Outreach Task Force (NOTF)
- 5** Satellite Task Force (STF)
- 6** Trusted Access Task Force (TATF)

As of July 15, 2003

 **Other NSTAC Issues**

- Critical facility vulnerability analysis
- National policies, laws, and regulations affecting NS/EP telecommunications
- National Response Plan



 **Questions and Answers**

ATTACHMENT B

*(Vulnerability Disclosure Guidelines Working Group
Status Report Briefing Materials)*

NIAC Vulnerability Disclosure Working Group (VDWG)

2nd Status Report & Update
National Infrastructure Advisory Council
2003 July 22

Rob Clyde Ken Watson
rclyde@symantec.com kwatson@cisco.com

Background

- NIAC charged by Executive Order 13231, amended by EO 13286, to foster improved cooperation among ISACs, the Department of Homeland Security, and other Federal Government entities
- Vulnerability Disclosure Working Group established by NIAC on January 8, 2003
 - Task: Develop global framework for handling a security vulnerability from initial report to final resolution
 - Deliverable: Derive specific recommendations for the President

2003 July 22 NIAC Working Paper: 2nd VDWG Status Report for NIAC 2

Background (2)

- Internet is global, with multiple, diverse stakeholders
- No common understanding of vulnerabilities or disclosure steps—need “best practice” common approach to improve information sharing and responses
- Great diversity of existing best practices; wide range of experience in working group and supporting organizations
- No “One size fits all” solution—framework will provide decision support process to increase awareness enable better decision-making

2003 July 22 NIAC Working Paper: 2nd VDWG Status Report for NIAC 3

Activities to Date: Participants

- Working Group 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
- Additional feedback and input from members of FIRST, NANOG, USENIX

Activities to Date: Deliverables

- Scope established. Guidelines will support a wide audience including discoverers, vendors, users, and government entities
- Established vulnerability scoring group—evaluating multiple methodologies
- Developed presentations to solicit feedback from stakeholders
- Developing final document

Activities to Date: Methodology

- Literature search
- Stakeholder contributions
- Distributed writing assignments
- Presented to key industry conferences; solicited feedback
- Develop common vulnerability scoring methodology
- Working group reviewing initial draft
- External input from selected organizations to follow in August

Key Issues

- Writing descriptive guidelines, not prescriptive policy—still appropriate?
- Should we investigate specific national security implications of vulnerability disclosure?
- How can framework be promoted nationally and internationally?

Next Steps

- Revised schedule:
 - 07/14: First draft reviewed by working group
 - 07/22 – 08/15: External inputs received
 - 08/22: Final draft presented for NIAC review
 - 09/22: NIAC members review completed
 - 09/29: Final version presented for NIAC approval
 - 10/07: NIAC members approve by e-mail
 - 10/10: NIAC-approved version delivered to DHS for final printing and preparation
- Formal presentation to the President in mid-October

Comments and Suggestions

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

ATTACHMENT C

*(Critical Sector Interdependencies Working Group
Status Report Briefing Materials)*

NIAC Working Group on Cross Sector Interdependencies & Risk Assessment Guidance

Interim Progress Report
Martin G. McGuinn, Chairman & CEO,
Susan Vismor, Senior Vice President,
Mellon Financial Corporation

Presented by
Chris Terzich, Manager – Wells Fargo & Company
Tuesday – July 22, 2003
Washington D.C.

1

Presentation Outline

- Background
- Report on Actions to Date
- Key Issues and Preliminary Considerations
- Next Steps

2

Background

- April 22 – NIAC Members recommend establishment of working group to study cross sector interdependencies and risk assessment guidance.

3

Mission/Objectives

- Provide risk assessment guidance based on cross-sector interdependencies and gaps identified in the process.
- Provide advice and guidance to the President on what needs to be addressed.

4

Report on Actions Taken to Date

- Project Initiation – May 8, 2003
 - Invitation sent to NIAC members
 - Invitation sent to Sector Coordinators
- Kick-off Meeting – May 14, 2003
- Progress Report – Next NIAC Meeting – July 22, 2003
- Deliver Final Recommendations – September 2003

5

Working Group Participants

- NIAC Member Institutions and DHS Support
 - Susan Vismor, SVP, Mellon Financial Corp., Working Group Chair
 - Teresa C. Lindsey, Chief of Staff, BITS (*supporting Susan Vismor*)
 - Peter Ailor – Internet Security Systems, Inc.
 - Bob Bergman, United Parcel Service
 - Andy Ellis – Akamai Technologies
 - Bobby Gilham – ConocoPhillips (Also listed as sector coordinator)
 - Rick Holmes – Union Pacific Corp.
 - Douglas Hurt – V-One Corporation
 - Aaron Meckler – Wells Fargo
 - Chris Terzich – Wells Fargo
 - Ken Watson – Cisco Systems, Inc.
 - Nancy Wong, DHS
 - Eric Werner, DHS
 - Clay Woody, DHS

6

Working Group Participants

- Sector Coordinators
 - Michehl Gent, North American Electric Reliability Council, Energy *
 - Lou Leffler, NERC
 - Dave Nevius, NERC
 - Bobby Gilham, ConocoPhillips, Inc., Energy *
 - Kathryn Condello, CTIA, Information and Telecommunications *
 - Matthew Flanigan, TIA, Information and Telecommunications*
 - David Thompson, TIA Online
 - Harris Miller, ITAA, Information and Telecommunications*
 - Greg Garcia, ITAA
 - Daniel Phythyon, USTA, Information and Telecommunications*
 - David Kanupke, USTA
 - Ed Hamberger, Association of American Railroads, Transportation*
 - Nancy Wilson, Association of American Railroads
 - Rhonda MacLean, Bank of America, Financial Services *
 - Peggy Lipps, Bank of America
 - Roger Callahan, Bank of America
 - Diane Van DeHei, Association of Metropolitan Water Agencies, Water *

* Accepted to participate (or send substitute).

7

Methodology

- Formed Working Group comprised of representatives from NIAC member institutions and sector coordinators.
- Working Group meets by conference call every week.
- Working Group reviewed existing interdependency studies.
- Working Group has requested a briefing on modeling capabilities by National Labs.
- Critical infrastructures are providing briefings to the working group on their incident response plan.

8

Expected Deliverables

- Recommend common definitions:
 - Dependency and Interdependency
 - Critical Infrastructures
 - Roles of Sector Coordinators
- Create an inventory of completed and pending studies and assessments.
- Recommend an approach to model cross-sector crisis management.
- Identify issues related to cross-sector crisis management.
- Compile sector best practices.
- Create a report of conclusions and recommendations.

9

Key Issues

1. Inconsistencies exist in the definition of the critical infrastructures.
2. The sector coordinator role is not broadly understood by private industry, and therefore is not leveraged as the focal point for establishing crisis management within and across the sectors.
3. Crisis management plans do not exist for each sector and are not tested end-to-end, across the sectors.
4. A National Command Center (either virtual or physical) does not exist as a confluence point for the sectors during times of crisis.
5. Government sponsored exercises (e.g., TOPOFF 2) do not actively solicit private industry representation.

10

Key Issues

6. There is an underestimation of the dependency of the Nation's critical infrastructures on the Internet.
7. Coordination in planning and response between public emergency management (federal, state and local) and private critical infrastructure is inadequate and/or inconsistent.
8. There is a lack of incentives that would help defray the additional expense burden resulting from strengthening the resiliency of the critical infrastructures.
9. While sophisticated modeling capabilities exist at the National Laboratories, to date the Working Group has been unable to get a briefing or understanding of those capabilities.

11

Preliminary Considerations

12

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

- Promote organizational consistency:
 - The National Strategy should set the agreed upon definition for “Critical Infrastructures”.
 - The Telecommunication’s industry should be represented as a critical infrastructure, separate from the Information Technology sector.
 - The NIAC should include a representative from each critical infrastructure.
 - A CEO from the Telecommunications sector should be appointed to the NIAC.
-

13

2. The sector coordinator role is not broadly understood by private industry, and therefore is not leveraged as the focal point for establishing crisis management within and across the sectors.

- Define the Role of Sector Coordinators:
 - Each “Critical Infrastructure” should have a *consistently appointed and consistently funded* sector coordinator.
 - The Sector Coordinator should be responsible to insure that a Crisis Management Plan exists for the sector.
 - The Sector Coordinator should also provide the “cross-sector” liaison role for their respective critical infrastructure.
-

14

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

- Crisis Management Plans should exist for each sector and be tested including validation of cross sector coordination.
 - Each crisis management plan should include clearly defined responsibility for testing.
 - Consideration should be given to establishing common terminology and response organization, resource management, and communications protocols.
-

15

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

- Establish a National Command Center.
 - A physical and/or virtual command center should exist that provides for a call tree, alerting mechanism, and command center that can be utilized by the critical sectors during an emergency situation.
 - Sector Coordinators should have a seat at the National Infrastructure Coordination Center.

16

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

- The government, through DHS, should sponsor exercises that include the participation of the critical infrastructures as soon as possible, and annually thereafter.

17

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

- Recommend that the physical versus cyber argument is moot.
- Promote an understanding of the potential vulnerabilities we face as the Nation continues to evolve towards an Internet Protocol based communications infrastructure.

18

7. Coordination in planning and response between public emergency management (federal, state and local) and private members of the critical infrastructure is inadequate and/or inconsistent.

- Incorporate a Critical Infrastructure Role into the National Incident Management System (NIMS).
- Establish planning partnership and response communication procedures, considering need for liaison or direct representation of private entities within Emergency Operations Centers.
- Develop access procedures (such as credentialing of staff to enter secure disaster areas) and resource priorities for critical infrastructure companies.

19

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

- Provide incentives to private sector companies to encourage investment to harden critical infrastructure.

20

9. While sophisticated modeling capabilities exist at the National Laboratories, to date the Working Group has not been able to get a briefing or understanding of those capabilities.

- It is time to move from theoretical to practical. The National Laboratories should be tasked with modeling critical infrastructure interdependencies and proposing solutions. This working group believes that the Telecommunications Sector be given priority, based on its standing as one of the most critical infrastructures.

21

Critical Decision Point

- ❑ Roles of the Sector Coordinators

22

Next Steps

- ❑ Continue meeting on a weekly basis.
- ❑ Receive a briefing from the National Laboratories.
- ❑ Refine these issues and considerations into a framework for crisis management within and across the critical infrastructure sectors.
- ❑ Complete the inventory review.
- ❑ Submit final recommendations.

23

ATTACHMENT D

*(Working Group on Evaluation and Enhancement of
Information Sharing and Analysis
Status Report Briefing Materials)*

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

Status Report
National Infrastructure Advisory Council
July 22, 2003

Thomas Noonan
tnoonan@iss.net

Background

- EEIS Working Group established at NIAC meeting April 22, 2003
- Task:
 - Review current state of Information Sharing and Analysis
 - Make specific recommendations for improving and enhancing information sharing and analysis capabilities within the public and private sector
- Derive specific recommendations for the President

Background (2) Mission

- NIAC charged by Executive Order 13231, amended by Executive Order 13286, to:
 - Foster improved cooperation among ISACs, DHS, and other Federal Government entities
 - Monitor the development of private sector ISACs
 - Provide recommendations to the President, on how these organizations can best foster improved cooperation

Background (3) Approach

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

2003 July 22

NIAC Working Group: Eval and Enhancement of Info
Sharing & Analysis

4

Activities to Date: Participants

- ❑ Working Group Chair: Tom Noonan
- ❑ Participants include: ISS, Wells Fargo, NYPD, EDS, Union Pacific, UPS, Inter-Con Security Systems, V-ONE, NERC, SIAC, ConocoPhillips, Cisco, Symantec, DuPont, and DHS/IAIP
- ❑ Additional feedback and input to come from members of IT-ISAC, FS-ISAC, ISAC Council

2003 July 22

NIAC Working Group: Eval and Enhancement of Info
Sharing & Analysis

5

Activities to Date: Deliverables

- ❑ Establish objective-focused groups:
 - Business models for sharing and analyzing information
 - Financial models for supporting information processes
 - Level of information analysis and aggregation
 - Dissemination breadth and coverage
- ❑ Establish milestones for task completion
- ❑ Develop white papers to present issues to the group for soliciting information and feedback
- ❑ Develop draft document for comment from stakeholders
- ❑ Develop a final document for the NIAC
- ❑ Make recommendations to deliver to President

2003 July 22

NIAC Working Group: Eval and Enhancement of Info
Sharing & Analysis

6

Key Issues

- Come up with a broad definition of the ISAC for today and the future.
- Determine liability and its effect on business models.
- Ensure broad participation for successful information sharing
- Define the level of information protection
 - DHS rules may protect sharing with government
 - NDAs may work within sectors

Key Issues

- Value proposition lies in the consolidation and analysis of actionable information
- Distribution needs to be relevant and secure (broad-based and/or targeted) in a timely fashion

Next Steps

- Schedule:
 - July 24 – WG Meeting in Atlanta – full discussion on white papers and working group goals, review timeline
 - August 14 – submit reworked white papers
 - August 26 – discuss white papers, outline draft report
 - September 15 – review white papers and initial report draft
 - September 21 – list serve review and comments on initial draft due
 - September 30 – discuss/review report for posting on DHS Web site - public comment – Atlanta face-to-face
 - October 1 – post to DHS Web site
 - October 15 – close public comment period
- Formal presentation to the President in October

Comments and Suggestions

- Principal authors:
 - Peter Allor, Internet Security Systems

- Working Group's e-mail address:
 - niac_eeis_wg@iss.net

ATTACHMENT E

*(Working Group on the Role of Regulation
Status Report Briefing Materials)*

Regulatory Guidance Best Practices for Enhancing Security of Critical Infrastructure Industries

NIAC Working Group
Interim Progress Report

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

July 22, 2003
Washington D.C.

1

Presentation Outline

- Objectives
- Methodology
- Expected Deliverables
- NIAC member perspectives
- Consistent themes & Planned Resolution
- High Level Timeline and Next Steps
-
- *Appendix*
 - *Contributors to this document*
 - *Identified Future Working Group Participants*

2

Objectives

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

3

Methodology

- Engaged representative members of NIAC working group
- Conducted structured interviews with 14 NIAC member institutions to identify differing perspectives
- Identified key areas of agreement and difference across sectors
- Constructed working team to define and synthesize recommendations by October.

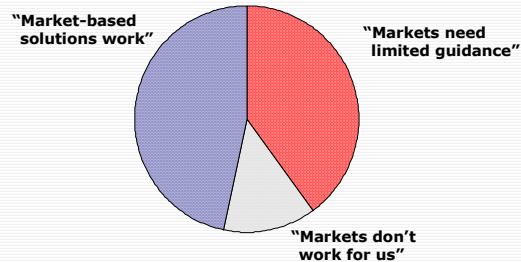
4

Expected Deliverables

- Policy recommendation to NIAC
 - Make sector-specific recommendations
 - Specify the role of market forces
 - Offer advice on role of regulation
 - Identify special circumstances needing focus

5

NIAC perspectives



6

“Market solutions work”

1. Markets give a rapid response to a changing environment
2. Risk can be quantified and responses tailored locally to meet different needs
3. Innovation operates faster than legislation
4. Markets do not lock companies into ineffective or outmoded standards

7

“Markets need limited guidance”

1. Rare but catastrophic events may not be given sufficient consideration
2. Can be hard to keep focus when competing priorities exist (Sarbanes-Oxley)
3. Weaker players do not always strive for the same levels of excellence
4. Disaster planning is invariably local – cross-industry interdependencies may be missed

8

“Markets don’t work for us”

1. Public sector institutions have difficulty getting mandate for risk-mitigating investment
2. State and local government currently have difficulty getting budgets to cover existing needs
3. Long-term contracts in utility arena prevent full costs from being covered by customers

9

Consistent concerns

- ❑ Ensuring industry performance standards are attained without loss of innovation
- ❑ Sustaining top management attention when events are infrequent or low likelihood
- ❑ Motivating consistent application of best practices across all players within an industry
- ❑ Aligning private and public sector more effectively across interdependent systems
- ❑ Making the nation more resilient to systemic effects when security breaches do occur

10

Resolution

1. Gain sector-specific understanding of requirements and efficacy of current oversight mechanisms
2. Specify special circumstances when markets may not reach working solution
3. Defining the role of regulatory guidelines especially in addressing cross-sector issues

11

High Level Timeline

- ❑ Project Initiation
– May 8, 2003
- ❑ Initial scoping
– June, 2003
- ❑ Progress Report
–NIAC Meeting – July 22, 2003
- ❑ Deliver Final Recommendations
– Early October, 2003

12

Appendix

- Institutions contributing to date.
- Working members for phase 2.

13

Institutions contributing to date

- Bill Sayles, Intel Corp.
- Bob Bergman, UPS
- Bobby Gillham, Conoco Phillips
- Bruce Larson, American Water
- Chris Terzich, Wells Fargo & Company
- Daryl Eckard, EDS
- Douglas Hurt, V-One
- Ed Ternan, Intercon
- Glenn Rust, Sterling Bank
- Rick Holmes, Union Pacific Corp.
- Susan Vismor, Mellon Financial Corp

14

Working members for phase 2

- Agreed NIAC Member Institutions
 - Susan Vismor, Mellon Financial Corp
 - Daryl Eckard, EDS
 - Chris Terzich, Wells Fargo & Company
 - Bobby Gillham, Conoco Phillips
 - Bill Sayles, Intel Corp.
 - Others (*TBD*)
- DHS Support
 - Nancy Wong, DHS
 - Eric Werner, DHS

15

ATTACHMENT F

(Draft Recommendation Letter)

DRAFT – FOR DISCUSSION PURPOSES – DRAFT

July 17, 2003

The Honorable Tom Ridge
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Ridge:

On behalf of the members of the National Infrastructure Advisory Council (NIAC), we are writing to you to recommend respectfully that the President appoint representation from the telecommunications sector for membership on the NIAC.

While the NIAC currently enjoys broad representation from most critical infrastructure sectors, the telecommunications sector is not represented on the Council. NIAC working groups have noted this deficiency as they work through their initiatives. Critical infrastructure sectors currently represented on the Council such as energy, banking and finance depend on reliable, robust telecommunications networks. Indeed, telecommunications systems are a fundamental infrastructure of modern society, and a successful attack on the networks could jeopardize national security and severely disrupt the economy and everyday lives of the citizenry.

The National Security Telecommunications Advisory Committee (“NSTAC”) has been advising the President on national security and emergency preparedness issues since 1982. The NSTAC is composed of key American telecommunications and information technology companies. Therefore, we respectfully suggest that the President solicit recommendations from the Chairman and Vice Chairman of the NSTAC regarding telecommunications industry representation on the NIAC.

DRAFT – FOR DISCUSSION PURPOSES – DRAFT

In sum, we believe that dedicated, full participatory telecommunications representation is essential to ensuring that the NIAC deliberations and recommendations cover all critical infrastructures it is commissioned to protect. Thank you for considering this request.

Sincerely,

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

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

CC: General Frank Libutti, Under Secretary for Information Analysis and Infrastructure Protection, U.S. Department of Homeland Security

The Honorable Robert P. Liscouski, Assistant Secretary, Intrastate Protection, U.S. Department of Homeland Security