Case Number: 2019-0203-F

FOIA MARKER

This is not a textual record. This is used as an administrative marker by the Clinton Presidential Library Staff.

Folder Title: NII Security Issues (National Information Infrastructure)
Staff Office-Individual: Intelligence Programs-Mislock, Raymond/Waguespack, Michael
Original OA/ID Number: 3179

Row:	Section:	Shelf:	Position:	Stack:
36	5	3	2	V

Draft Public Minutes

NII Security Issues Forum
of the IITF

Wednesday, May 11, 1994
3:00 - 5:00 PM
OEOB Room 180

Attendees:

Sally Katzen, OMB (Chair)
Chuck Chamberlain, USPS
Jim Flyzik, Treasury/GITS
Gayle Gordon, DOI
Dennis Bodson, NCS
Richard Carr, NASA
Donald McGinnis, EPA
Ronald Matzner, SBA
Bruce Lehman, PTO
Mike Keplinger, PTO
Brian Harris, NTIA
Richard Wilhelm, NSC
Barbara Valeri, DOD
Martin Ferris, Treasury
Stephen L. Squires, ARPA
Jim Burrows, NIST
Roger Callahan, NSA
Bob Marquette, NCS
Michael R. Nelson, OSTP
Robert Pepper, FCC
Scott Charney, DOJ
Louise Planet, OMB
Patricia Edfors, DOJ
Dennis D. Steinauer, NIST
Virginia Huth, OMB
Ed Springer, OMB
Rob Veeder, OMB
Bruce McConnell, OMB

I. Introductory Remarks - Sally Katzen, Chair, OMB

Mr. Bruce McConnell opened the meeting in the absence of Ms. Sally Katzen. Minutes of the previous meeting were distributed for correction.

Mr. McConnell stated that the previous week he had met with members of the U.S. Advisory Council on the NII. The Council is aware of the work of the NII Security Issues Forum and of the IITF and wants to help in the creation of a dialogue with the public. Joint efforts have begun to plan a public meeting on the issue of security in the NII.

Draft Public Minutes

II. Approve Revised Discussion Paper, "Roles and Responsibilities: NII Security Issues Forum"

The paper circulated represented previous thinking on the topic and comments from the last meeting. It suggests that this Forum act as a clearinghouse for other groups that are also working on privacy/security issues. Comments on the document included:

(1) Is there an interface between DII ("defense information infrastructure") and GII ("global information infrastructure")? It was suggested that groups which are international in scope could tell this group what they are doing.

(2) NCS will work with the Network Reliability and Vulnerability Working Group (NRVWG), but both report to the IITF. Independent groups will be encouraged to work together, thus pooling information and reducing duplication of effort.

(3) Relating to information and security management controls for information (page 2), it was suggested that expectations might be too high.

(4) NIST's work in assessing R&D was mentioned in the report, but what about other groups which are doing this? Perhaps the document should spell this out in more detail. Work with other agencies on assessing R&D should be done as deemed appropriate.

(5) Referring to NIST's work on identifying security products, is this too precise? Elsewhere in the document, it is suggested that other groups do this. It was also suggested that "practices" and "education" should be added to "tools" and "techniques" in the paper.

III. Collect Lists of Top Security Issues

Each agency in the Forum was responsible for making a list of top security issues to be submitted at this meeting. Mr. McConnell collected those lists submitted. NIST, NCS, NSA, and ARPA submitted lists; DOJ did not have a list but gave a sense of what it was doing. DOD raised two issues: (1) the omission of activity related to information security infrastructure, and (2) protection of information databases.

At this point, Ms. Katzen arrived and took over the discussion. With reference to DOD's first concern, one participant suggested that more information was needed on how input from the public and private sectors could be collected and combined. With reference

to the second concern, it was stated that while there has been much thought and action on network security/privacy, there has been little done relating to database information itself. DOD is not confident in the position of the Forum or the NII in these areas. It was stated that both the leadership role and the catalytic role of the Forum were paramount.

IV. Public Meeting

A. Progress Report -- Marty Ferris
B. Involvement of the Committee of the IITF - Sally Katzen
C. Involvement of the NII/AC - Bruce McConnell

Ms. Katzen stated that at the previous meeting, participants had agreed on the need for a public meeting to determine the public's view of information security.

Marty Ferris, who is organizing this effort, announced that a date for this meeting has been set for July 15. Position papers from users describing their unique security needs and perspectives are being sought. He also asked the representatives from the Committees to contribute the names of ten people who would be knowledgeable about this subject in the Committee's issue area. Names should represent a diverse range of users. Names should be submitted no later than two weeks from today. Position papers will be accepted by FAX and e-mail.

Two points were raised: (1) we need to solicit public dialogue for the Forum, even if it confirms some of what we as already know, because what emerges may be news to the public; (2) this needs to be a public Forum if public policies are to be made by this group.

The NII Advisory Council will act as "listeners" from the private sector alongside the IITF and will provide lists of people who would be knowledgeable speakers. To ensure a successful meeting, a large delegation of listeners is necessary.

The question was raised as to whether any meetings will be held outside of the DC Metro area. The response was that this will depend on the outcome of the first meeting. If it appears to be popular and productive, more programs will be scheduled.

It was suggested that the meeting be divided into sections of interest so that an attendee need not be present for a full day. This might ensure a better turn-out. This also allows for the presentation of more topics and a more diverse attendance.

It was suggested that the hours be 9:00 AM to 4:00 PM with flexibility for a lunch break. The agenda will be set once responses from potential speakers are received.

V. Status of Other Activities -- Brief Reports

A. Legislative Update -- Scott Charney, DOJ

An analysis of Federal and State laws on information security has demonstrated a shift in emphasis. Forty-nine states have comprehensive crime laws. Although early laws addressed hardware and software elements together, it is now acknowledged that computers and information are unique and must be handled differently under the law. For example, health information should be protected differently than proprietary business information. Also, as the South District Court of New York decided, not all information on a hard drive needs to be provided in response to a subpoena. An article on this subject has been written and will be made available at the next Working Group meeting.

The question was raised as to if and how the Forum can help in legislating information security. One individual stated that the Forum should assist in drafting legislation and that IITF should not only tie into the issue, but also get credit for it. The issue of information security is part of the Administration's reinventing government efforts. This is not just a DOJ issue.

B. Network Reliability and Vulnerability Working Group -- Bob Marquette, NCS

The National Security Information Oversight Working Group will meet in Dallas, May 24-25. The National Security Standard Oversight Group is looking at gaps in information security and a report will be made to this group. It was generally thought that it is good to hear from these smaller groups over time rather than waiting for one open meeting. A firewall workshop will be held June 28 on firewalls and other techniques to protect databases. Computer crime legislation vulnerabilities and weaknesses were discussed, especially where it comes to strengthening current laws. The Network Reliability and Vulnerability Working Group evaluated its charter and decided to work on a few specific tasks at a time. Separate working groups will address each responsibility, and all groups will be informed of what each is doing.

C. Working Group on Encryption and Telecommunications -- Mike Nelson, OSTP

A letter to the New York Times raised issues to which this

File
Security Issues
Forum

working group must respond. At the May 3 hearing on the Clipper Chip, Senator Leahy took a negative position. However, a hearing before Congressmen Valentine and Glickman proved to be more positive. Some individuals outside the Administration feel that legislation on this issue is necessary. Some work needs to be done relating to escrow agents, international agreements, sharing of knowledge, and security concerns with reference to the Clipper chip.

Nevertheless, better public relations are needed for these issues, as well as for digital telephony. A new public relations program is being put in place. DOJ was asked to be more active in this arena. It was agreed that more discussions are necessary.

A bill will probably be introduced next week on digital telephony, but it is strongly opposed by the telephone industry. Encryption issues will be moving to the front burner. Negotiations on patent rights are underway. Finally, export control legislation on encryption software has been introduced.

D. NIST, the Computer System Security and Privacy Advisory Board (CSSPAB), and the Forum of Incident Response & Security Teams (FIRST) -- Jim Burrows, NIST

National Performance Review (NPR) assignments have been given to these groups. There are four and one is on R&D. The Chair of the CSSPAB, Willis Ware, believes that its assignment is too expansive, given that it meets only once a quarter. The information security work and the response time of the private sector need to be looked at, and public comments need to be collected, distilled, and reported for the next three quarters. The FIRST steering committee met 3 weeks ago, and is pleased that NII is interested in its work and will provide input. NIST will expand FIRST in the Federal Government. Not all agencies are represented yet and must be brought on board. NPR recommendations on a crisis clearinghouse include a draft plan to beef up the bulletin board and incident response time activities as well. GITS security actions should be looked at for use by IITF, and this is in the planning stage. The INTERNET Security Plan has been picked up. As FIRST sees it, it is an organization of professional technicians who talk with each other, but the problem is that there is a lack of professional technicians at each agency to implement required changes. Each agency needs active technician experts to attack system problems. The question was raised on how the private sector manages this. The problem is that information is shared with customers on system vulnerabilities and solutions, but the Federal Government is unwilling to do this. This subject will be brought up at the Assistant Secretary level at the IRM Group meeting.

E. DOD Security Activities -- Barbara Valeri, DOD

The Joint Security Commission (JSC) looked at all security initiatives for streamlining at the end of the Cold War. Unclassified information security systems were found to be most vulnerable. DOD issued a directive on information warfare offensive and defensive tactics. The main concern is the vulnerability of the information infrastructure in war, i.e., the ability to disrupt or destroy it. JSC sees an increased reliance on commercial providers. DOD has recognized a need to educate senior leadership on policy and political issues and details. A meeting on May 6 touched on this, and the difficulty of the problem was recognized.

NSC is asking for input on the offensive and defensive information warfare idea. The main thrust must be for the government to convince the public that a real threat to information security exists and is important. It was thought that the reason for the lack of serious thought on this topic is that the media is over-reporting the ease of access to information and under-reporting the ease with which this information can be changed, and the effect this will have on the public. The Forum might take a leadership role in this area, e.g., support the issuing of an Executive Order. Today, we must change the culture and educate people in order to promote a secure NII.

E. New Item

An article in PC Week stated that there might be a Federal government issued ID card to be used for accessing public bank records. In April, a paper was presented on the concept of a US Card, i.e., a single card for government interface. Privacy is the paramount concern here, not for surveillance reasons, but, rather, to protect public health and financial information. The article in PC Week is a jumble of the information presented in the paper. A letter has been sent to PC Week on the misrepresentation and is to be published. INTERNET also had an article on this topic. It was thought that this issue needs to be addressed and misconceptions need to be rectified.

VI. Next Steps -- Sally Katzen

The group will meet again in June. Attendees are reminded of Marty Ferris' program on July 15 and were requested to send names of "listeners" to him within 2 weeks. Lists of top security issues submitted today and in the near future will be distilled and distributed. Thank you to all attendees.

AGENDA
NII Security Issues forum
of the Information Infrastructure Task Force

Security Issues Forum

OEOB Room 248
Tuesday, June 14, 1994
1:30 - 3:30 p.m.

I. Introductory Remarks -- Sally Katzen, Chair

Distribute minutes of the previous meeting for correction

II. Approve for public release revised draft discussion paper, "Roles and Responsibilities: NII Security Issues Forum"

III. Public Forum -- Marty Ferris

IV. Top security issues to be addressed

V. Status of Other Activities -- Brief Reports

A. Legislative Update
Scott Charney, DOJ

B. Network Reliability and Vulnerability Working Group
Dave Signori, DISA

C. Working Group on Encryption and Telecommunications
Richard Wilhelm, NSC

D. NIST, the Computer Security and Privacy Advisory Board (CSPAB), and the Forum of Incident Response & Security Teams (FIRST)
Jim Burrows, NIST

E. DoD Security Activities
Barbara Valeri, DoD

F. National Security Telecommunications and Information Systems Security Committee (NSTISSC)
Roger Callahan, NSA

G. Federal Networking Council
Steve Squires, ARPA

H. High Performance Computing and Communications Program
Don Lindberg, NLM

VI. Next Steps -- Sally Katzen

File NII Security Issues Forum

MEMORANDUM FOR PARTICIPANTS IN "SECURITY AND THE NII" MEETING

FROM: Bruce McConnell

SUBJECT: Next "NII Security" meeting

Attached is the revised draft document, "Roles and Responsibilities: The NII Security Issues Forum," and a draft agenda for the next meeting tomorrow (Tuesday, June 14, 1994), from 1:30 to 3:30 p.m. in OEOB 248.

I'd like to remind you that at our last meeting, Sally Katzen asked participants to submit the names of individuals who could represent a diversity of view in the NII user community at the July 15 public meeting. Please bring a list of names tomorrow.

If you have not already done so, please contact Mary Ann Robinson at (202) 395-3785 to confirm your attendance and arrange for access to the building. I'll see you there.

6/13/94

Roles and Responsibilities:
NII Security Issues Forum

The Role of Government in NII Security:

Government has an important public mission to support the secure use of the National Information Infrastructure (NII). The NII is an interconnecting network of networks, which includes the information content and the information system. Government must cooperate with the private sector and with the public-at-large in setting legal and policy ground rules for security in the NII. This responsibility is shared among the Federal government and State, local, and tribal governments. In addition, the Federal government should also assess the security implications for the NII presented by a global information infrastructure. It should also serve as a facilitator and a catalyst for private sector and other governmental activities.

The Role of the NII Security Issues Forum:

The NII Security Issues Forum will provide leadership for Federal NII security activities. It will ascertain the security needs of the various NII user communities and the Federal role in assuring such security. It will ensure coordination of the security activities across the various Committees of the Information Infrastructure Task Force (IITF) and serve as a clearinghouse for Federal security efforts related to the NII. The Forum will also consider the scope of legal and policy remedies necessary to achieve desired security in the NII.

Strategy:

The Committees of the IITF will work with the public to identify the security needs of various users of the NII. Committees should solicit input and initiate dialogue with their constituent users. This dialogue should help define the security requirements for the NII in order to determine needed polic technology, and managerial controls, and what the Federal r will be to assure that those needs are fulfilled.

To accomplish this, the Forum will solicit participation from individuals, organizations, and State, local, and tribal governments. An initial Public Meeting to stimulate this dialogue is being planned.

The Forum will also collect information concerning the impact of civil case law on security in electronic environments and will analyze the sufficiency of Federal criminal law. It will then foster the development of corrective legislation, if needed.

Finally, the Forum will collect and disseminate information about public and private sector security technology and management controls in order to ensure that needed security capabilities will be available.

Organizational Responsibilities:

The Forum will conduct outreach activities, assess current policies, and act as a clearinghouse for the security activities of the IITF and of other Federal government entities.

I. The Forum will:

- Initiate and maintain a public dialogue involving individuals, organizations, industry, and State, local, and tribal governments in discussions of the needs for, legal aspects of, and techniques for security in the NII.

- Assess the sufficiency of the current criminal statutory regime; notify the participants of movement on relevant legislation; report on developments in civil case law relevant to computer security; and consider the need for amendment to statutes or new laws.

II. The Forum will coordinate the following IITF activities:

- The **Telecommunications Policy Committee** (TPC), the **Information Policy Committee** (IPC), and the **Committee on Applications and Technology** (CAT) of the IITF will identify security requirements for their constituencies.

In addition, Working Groups of these Committees will also identify security requirements for their constituencies, as appropriate. For example:

- The **Intellectual Property Rights Working Group** (IPRWG) and the **Privacy Working Group** (PWG), through the Information Policy Committee, will advise the Forum on security issues pertaining to intellectual property rights and privacy.

- The **Government Information Technology Services Working Group (GITS)**, through the Committee on Applications and Technology, will advise the Forum on security issues pertaining to the application of information technology by Federal agencies to improve service delivery and accomplish agency missions.

- The **Network Reliability and Vulnerability Working Group** (NRVWG), with the assistance of the **National Communications System** and through the **Telecommunications Policy Committee**, will advise the Security Forum on (1) protection for all users from catastrophic failure of the network and the information services it provides, along with mechanisms for recovery from threats ranging from natural disasters to overt attacks, and (2) national security and emergency preparedness requirements.

- Other Working Groups in the **Committee on Applications and Technology** will identify sector-specific user requirements for security, such as those in the areas of health information and education.

III. The Forum will draw together technical and analytical support throughout the Federal government. In particular, the Forum will coordinate the efforts of the following Federal Government entities:

- **National Institute of Standards and Technology** (NIST) will encourage the **Computer System Security and Privacy Advisory Board** (CSSPAB) to assist NIST in the assessment of security tools and techniques in use outside of the Federal Government.

- **NIST**, and other agencies where appropriate, will assess where research and development on security technology would be useful for the NII.

- **NIST**, working with other agencies, will identify Federal security products, techniques, and practices that will be useful in the NII (e.g. recent EDI security guidance).

- **NIST** will work with the **Forum of Incident Response and Security Teams** (FIRST) to assess how private entities conduct emergency response and how the efforts of Government can be coordinated with them to ensure a "911" capability for the NII.

- **National Communications System** (NCS), in coordination with the industry's **National Security Telecommunications Advisory Committee** (NSTAC), will work with the **Network Reliability and Vulnerability Working Group** to ensure that National Security and Emergency Preparedness (NS/EP) needs are accommodated in the NII.

- **National Security Telecommunications and Information Systems Security Committee** (NSTISSC) will identify useful security tools and techniques in the national security community that may be applicable to the NII.

- **Working Group on Encryption and Telecommunications** (WGET) will develop policy recommendations regarding the Government's response to the spread of digital telecommunications equipment and inexpensive encryption devices which could prevent effective wiretaps. This will require development and evaluation of technologies and policies that balance law enforcement's need for access with the need for strong security.

- **The High Performance Computing and Communications Program** (HPCC) will assure development and testing of new technologies for computer security suitable to a high performance environment.

- **The Federal Network Council** (FNC), a multi-agency committee that oversees Federal research networks, shall explore specific issues relating to security of the Internet.

DRAFT AGENDA
NII Security Issues Forum
OEOB Room 248
Tuesday, June 14, 1994
1:30 - 3:30 p.m.

I. Introductory Remarks -- Sally Katzen, Chair

Distribute minutes of the previous meeting for correction

II. Approve for public release revised draft discussion paper, "Roles and Responsibilities: NII Security Issues Forum"

III. Public Forum -- Marty Ferris

IV. Top security issues to be addressed

V. Status of Other Activities -- Brief Reports

A. Legislative Update
Scott Charney, DOJ

B. Network Reliability and Vulnerability Working Group Bob Marquette, NCS

C. Working Group on Encryption and Telecommunications
Mike Nelson, OSTP

D. NIST, the Computer Security and Privacy Advisory Board (CSPAB), and the Forum of Incident Response & Security Teams (FIRST)
Jim Burrows, NIST

E. DoD Security Activities
Barbara Valeri, DoD

F. National Security Telecommunications and Information Systems Security Committee (NSTISSC)
Roger Callahan, NSA

G. Federal Networking Council
Steve Squires, ARPA

H. High Performance Computing and Communications Program
Don Lindberg, NLM

VI. Next Steps -- Sally Katzen

File / NII Security Issues Forum

IITF Security Issues (Stephen L. Squires, ARPA, 1994 May 11)

This needs to be viewed as an opportunity to listen, learn, rethink, and lead.
These are written in a constructive way to get them discussed.

What is the Administration position and rationale?

What can be said about the Equity issue in public?

NII Infosec is not necessarily the same as Defense Infosec although they are related.

Export policy and technology.

Interoperable Infosec among different consenting communities.

Global Information Infrastructure Infosec policy and technology.

Key Escrow in general rather than a particular point solution.

Education in Safe Computing, Risk Management, and Ethics.

The Internet should be treated as an experimental environment for learning about the technologies, their early experimental applications, and social and legal implications.

Alternative approaches need to be explored to find an appropriate balance among privacy, equity, international issues.

NIST

From POP2-Server@csmes Wed May 11 10:35:28 1994
Received: from mot.ncsl.nist.gov (MOT.NCSL.NIST.GOV [129.6.54.38]) by csmes.ncsl.nist.gov (
Received: from localhost (uucp@localhost) by mot.ncsl.nist.gov (8.6.4/8.6.4) id UAA05768 fo
Received: from sparrow.nist.gov(129.6.16.8) by mot via smap (V1.3mjr)
id sma005766; Tue May 10 20:31:43 1994
Received: from DIRECTORY-DAEMON by SPARROW.NIST.GOV (PMDF V4.2-13 #4653) id
<01HC6RP5ZRF40006GY@SPARROW.NIST.GOV>; Tue, 10 May 1994 20:52:01 EDT
Received: from st1.ncsl.nist.gov by SPARROW.NIST.GOV (PMDF V4.2-13 #4653) id
<01HC6RP2FP340006D9@SPARROW.NIST.GOV>; Tue, 10 May 1994 20:51:55 EDT
Received: from st21.ncsl.nist.gov by st1.ncsl.nist.gov (4.1/NBS-rbj.11) id
AA11396; Tue, 10 May 94 20:55:16 EDT
Date: Tue, 10 May 1994 20:55:16 -0400 (EDT)
From: katzke@st1.ncsl.nist.gov (Stuart W. Katzke)
Subject: Re: RE: NII Security Issues Forum
In-reply-to: <9405102333.1F410C@csme1.ncsl.nist.gov>
To: dds@NIST.GOV, mcnulty@ecf.ncsl.nist.gov
Message-id: <QDD017F0@st21>
Organization: National Institute of Standards and Technology formerly National
Bureau of Standards
Content-transfer-encoding: 7BIT
Disclaimer: Opinions expressed are those of the sender and do not reflect NIST
policy or agreement.
Content-Length: 1678
Status:

Lynn and Dennis,

I noticed that the material for the NII Security Issues Forum meeting includes a reminder for each individual to bring a list of top security issues they are working on and a list of issues they believe should be addressed by others. Would one of you please discuss the major initiatives we are planning, including:

PK Infrastructure

Development of specifications for a public key infrastructure that is developed to meet gov't and industry needs--developed in consultation with all stake holders. Long term goal is to get infrastructure operational for conducting business.

Advanced Authentication Technology

Development of interface standards and standard services for I&A mechanisms that allow all forms of I&A techniques to be used and transmitted securely throughout networks.

Incident Prevention, Detection, Response, and Clearinghouse

Development of guidance, tools, and techniques for assisting gov't and industry users connect to the Internet (short term goal). Longer term goal is to assist in secure connections to other networks or networks that evolve to be the NII. This area includes incident response capabilities required for the NII and Nat'l Clearing House activities.

Security Criteria and Evalaution.

Includes international efforts to develop Common Criteria and an evaluation methods that forms the basis for mutual recognition of evaluations. The efforts include establishment of an evaluation capability in the US that will significantly speed-up evaluations and reduce their costs. This activity in needed to improve the

trust in products and systems that form the fabric of NII services, systems and applications.

~~NSA~~

draft NSTISSC

ISSUES:

- Achieving a comprehensive set of security ~~of~~ solutions for national security community within a framework of common and open network environment.

Being addressed by establishing a security architecture and security services to meet the needs of this community in partnership with industry. Significant R&D in software assurance required.

- Identifying the common security service requirements and interoperabilty needs with the non-national security community to avoid duplication of systems, while assuring inappropriate risks are not accepted.

Integrating Technical Reference Models and looking for siginificant commonality and differences.

- Updating and introducing required information safeguarding policies and practices to reflect the changing information technology environment.

Joint Security Commission report.

- Education and Awareness, derived from updated threat analysis.

Lack of awareness percipatating increased risks.

- Security Management Infrastructure and common security practices and procedures for various security services.

Completing Certificate and Key Management, Registration, etc. standards/common services required across many applications within national security community

Roger Callahan

INFORMATION PAPER

May 11, 1994

MEMORANDUM FOR NII SECURITY ISSUES FORUM MEMBERS

FROM: Deputy Manager, NCS

SUBJECT: **Security Issues in the NCS, NSTAC, and the NII Network Reliability and Vulnerability Working Group**

1. PURPOSE. This information paper provides a brief summary of **what we are doing in security** and **what issues need to be worked** in the National Communications System (NCS), The President's National Security Telecommunications Advisory Committee (NSTAC), and the NII Network Reliability and Vulnerability Group.

2. DISCUSSION.

A. **NCS/NSTAC Current Issues.** The NCS and NSTAC current security issues are:

(1) **Network Security Information Groups (NSIEs).** The industry and Government NSIEs will meet jointly on 24 - 25 May in Dallas. The NSIEs exchange information on current threats, vulnerabilities and countermeasures. They will also tour the GTE and MCI network facilities.

(2) **Network Security Standards Oversight Group (NSSOG).** This NSTAC standards group is currently working on a report that will identify gaps and "holes" in existing standards where security is inadequately addressed, and will also identify key technologies where security is not addressed at all. The draft version will be reviewed by the NSIE and NSSOG members this month; the final version is scheduled for presentation to the NSTAC in January 1995.

(3) **Firewalls Workshop.** The NCS and NSTAC are sponsoring a Firewalls Workshop on June 28, 1994. The purpose is to provide up-to-date information on current firewall technologies and network connection security strategies applicable to National Security and Emergency Preparedness (NS/EP) communications systems. The agencies represented in the NII Security Issues forum have been extended an invitation through the NCS Committee of Principals (COP). Forum members interested in receiving an invitation can contact Mark Centra, OMNCS-NT, at 703-746-8536.

(4) **Proposal for Computer Crime Legislation.** The jointly sponsored NCS and NSTAC recommendations to the President on computer crime laws - corrections dealing with legislative deficiencies affecting the capability to gather evidence about

computer crimes and to prosecute computer criminals who target computers that support the national telecommunications infrastructure - are being forwarded through the National Security Council to the Department of Justice for action.

(5) **NCS and the Government Information Technology Services Working Group (GITS).** The NCS is working with the GITS Working Group to foster the industry-government partnership for improving services and security in public telecommunications. The objective is a unified concept of operational security for new technological developments such as universal personal telecommunications.

B. **NCS/NSTAC Issues that need to be worked.**

(1) **NS/EP Security Issues.**

(a) At the wireless interface of the NII we are working with both cellular industry and the newly emerging Personal Communications Services (PCS) standards bodies to introduce the federal security requirements being developed by the Federal Wireless Policy Committee, which is chaired by the NTIA and OMNCS. Such requirements include: confidentiality, identification, geolocation, integrity, and recovery.

(b) We also need to look at the security concerns that all levels of government and respective emergency services must rely on when using the Public Switched Network (PSN) and the evolving NII. An example is use of secure communications between state and local emergency operations centers when discussing evacuation and recovery efforts for natural disasters.

(2) **International and Industry Standards.** We need to closely coordinate with on-going high-speed NII standards development projects, especially for synchronous optical networks (SONETs) with asynchronous transfer mode (ATM), to ensure that security is considered as the systems evolve. Examples of areas of immediate concern are:

(a) exchange of cryptographic keys and resynchronization of cryptographic engines when bits are lost in transmission, and

(b) authentication methods and privacy of data residing in the emerging telecommunication management networks (TMNs).

These security methods are needed both for electronic commerce and for Government communications.

(3) **Cable Companies and the NII.** What security considerations are being given to the cable companies? Should they be regulated as are the common carriers? We are already looking at the PSN and Internet; are we missing this industry?

C. **The NII Network Reliability and Vulnerability Working Group.** (Current and Future Issues)

(1) Dr. Dave Signori, DISA, chaired an all day meeting of the Network Reliability and Vulnerability Working Group on April 22. The OMNCS has representatives on this working group and provides the Secretariat function. The attendees at the meeting discussed the roles of the Working Group, candidate issues to be worked, and a structure for working them. The charter for the Reliability and Vulnerability (R&V) Working Group contained guidance including the addressal of a number of specific issue areas. The issues fell into four broad groups:

(a) the reliability of information services to meet critical needs of NS/EP users,

(b) the reliability of information services to meet the needs of general business, private, and government users, both in normal and emergency situations,

(c) protection of the networks, and

(d) protection of the confidentiality and integrity of the information being transported.

Since privacy and information security issues are being addressed in other committees and working groups, the R&V group will focus its efforts on the first three areas and formed three subgroups to do so: National Security and Emergency Preparedness (NS/EP); reliable service to general users; and security protection of the networks. The R&V Working Group will be the focal point for addressing issues in these three areas and will provide a framework for considering related issues that cut across the interests of other IITF elements (e.g. reliability implications of extending the NII to international infrastructures).

(2) The objective of each subgroup, in subsequent meetings, is to develop a gameplan to include: issues to undertake; a methodology and timeline to follow; and outcomes or products envisioned. The next meeting of the Working Group is scheduled for Monday, June 6, 1994 from 1300 - 1600 at the DISA HQ in Arlington, VA.

3. CONCLUSION. This information paper outlines the current and future security issues that the NCS, NSTAC, and the NII Network Reliability and Vulnerability Working Group are working on.

WILHELM

MEMORANDUM FOR PARTICIPANTS IN "SECURITY AND THE NII" MEETING

FROM: Bruce McConnell Bruce

SUBJECT: Next "NII Security" meeting

File

The next meeting of the NII Security Issue Forum will be Tuesday, June 14, 1994, from 1:30 to 3:30 p.m. in OEOB 248. The agenda will include discussion of the revised "Roles and Responsibilities" document, a progress report on the public meeting, discussion of the work plan of the Forum, and brief reports from participants on security-related activities.

A draft agenda and draft public minutes from the last meeting will be circulated in advance.

Please contact Mary Ann Robinson at (202) 395-3785 to confirm your attendance and arrange for access to the building.

Ray - have you nothing on this Day - are you going.

YES

NO

6/13

Rich - pls discuss with Mike Nelson and determine what the input of IWG on this should be and who should make presentation.

R

MAY 10 1994

MEMORANDUM FOR PARTICIPANTS OF NII SECURITY ISSUE FORUM

FROM: Bruce McConnell BMcC

SUBJECT: Next meeting of the NII Security Issues Forum

Attached is a draft agenda and a revised version of the paper, "Role and Strategic Plan: NII Security Issues Forum," for approval at the meeting on Wednesday, May 11, 1994, from 3:00 to 5:00 p.m. **Please note that the location has been changed to room 180 in the OEOB.**

Representatives of each group should remember to bring a list of top security issues they are addressing and a list of issues they believe should be addressed by others.

If you haven't already, please contact Mary Ann Robinson at (202) 395-3785 to confirm your attendance and arrange for access to the building.

Enclosures (2)

folder

Ray - FYI - I gave a copy to Wilhelm -

LISA to file in NII Sec. Forum

LISA - this is in my book case drawer.

Draft Agenda
NII Security Issues Forum
of the Information Infrastructure Task Force

OEOB Room 180
Wednesday, May 11, 1994
3:00 - 5:00 p.m.

I. Introductory Remarks -- Sally Katzen, chair

Distribute minutes of the previous meeting for correction.

II. Approve revised discussion paper, "Roles and Responsibilities: NII Security Issues Forum."

III. Collect lists of top security issues

IV. Public Forum

A. Progress Report -- Marty Ferris

B. Involvement of the Committees of the IITF -- Sally Katzen

C. Involvement of the NII/AC -- Bruce McConnell

D. Involvement of the Computer Security and Privacy Advisory Board -- Jim Burrows

IV. Status of Other Activities -- Brief Progress Reports

A. Legislative Update -- Scott Charney, DOJ

B. Network Reliability and Vulnerability Working Group -- D. T. Signori, DISA

C. Working Group on Encryption and Telecommunications -- Mike Nelson, OSTP

D. NIST, the Computer Security and Privacy Advisory Board (CSPAB), and the Forum of Incident Response & Security Teams (FIRST) -- Jim Burrows, NIST

E. DoD Security Activities -- Barbara Valeri, DoD

F. National Security Telecommunications and Information Systems Security Committee (NSTISSC) -- John Nagengast, NSA

V. Next Steps -- Sally Katzen

Roles and Responsibilities:
NII Security Issues Forum

The Role of Government in NII Security:

Government has an important public mission to support the secure use of the National Information Infrastructure (NII). Government must cooperate with the private sector and with the public-at-large in setting legal and policy ground rules for security in the NII. This responsibility is shared between the Federal government and State, local, and tribal governments.

The Role of the NII Security Issues Forum:

The NII Security Issues Forum will ascertain the security needs of the various NII user communities and the Federal role in assuring such security. It will ensure coordination of the security activities across the various Committees of the IITF and serve as a clearinghouse for Federal security efforts related to the NII. The Forum will also consider the scope of legal and policy remedies necessary to achieve desired security in the NII.

Strategy:

The Committees of the IITF will identify the security needs of various user sectors affiliated with the NII. Committees should solicit input and initiate dialogue with their constituent users. This dialogue should help define the security requirements for the NII in order to determine needed policy, technology, and managerial controls, and what the Federal role will be to assure that those needs are fulfilled.

To accomplish this, the Forum will solicit participation from individuals, organizations, and State, local, and tribal governments. An initial Public Meeting to stimulate this dialogue is being planned.

The Forum will also gather information concerning the impact of civil case law on security in electronic environments and will analyze the sufficiency of Federal criminal law.

Finally, the Forum will gather information about public and private sector security technology and management controls in order to ensure that needed security capabilities will be available.

Organizational Responsibilities:

As initial steps, the Forum will conduct outreach activities and assess current policies, as well as act as a clearinghouse for the security activities of the IITF and of other Federal government entities.

I. The Forum will:

- Maintain a public dialogue involving individuals, organizations, industry, and State, local, and tribal governments in discussions of the needs for, legal aspects of, and techniques for security in the NII.

- Assess the sufficiency of the current criminal statutory regime; notify the participants of movement on relevant legislation; report on developments in civil case law relevant to computer security; and consider the need for amendment to statutes or new laws to address emerging crimes.

II. The Forum will coordinate the following IITF activities:

- The **Telecommunications Policy Committee**, the **Information Policy Committee**, and the **Committee on Applications and Technology** of the IITF will identify security requirements for their constituencies.

In addition, Working Groups of these Committees will also identify security requirements for their constituencies, as appropriate. For example:

- The **Intellectual Property Rights Working Group (IPRWG)** and the **Privacy Working Group (PWG)**, through the Information Policy Committee, will advise the Forum on security issues pertaining to Intellectual Property Rights and Privacy.

- The **Government Information Technology Services Working Group (GITS)**, through the Committee on Applications and Technology, will advise the Forum on security issues pertaining to the application of information technology by Federal agencies to improve service delivery and accomplish agency missions.

- The **Network Reliability and Vulnerability Working Group**, with the assistance of the NCS and through the Telecommunications Policy Committee, will advise the Security Forum on (1) protection for all users from

catastrophic failure of the network and the information services it provides, along with mechanisms for recovery from threats ranging from natural disasters to overt attacks, and (2) national security and emergency preparedness requirements.

- Other Working Groups in the **Committee on Applications and Technology** will identify sector-specific user requirements for security, such as in the areas of health information and education.

III. The Forum will draw together technical and analytical support throughout Government by coordinating the efforts of the following federal Government entities:

- **NIST** will encourage the Computer Security and Privacy Advisory Board (CSPAB) to assist NIST in the assessment of security tools and techniques in use outside of the Federal Government and assess where research and development on security technology would be useful for the NII.

- **NIST** will identify Federal security products and techniques that will be useful in the NII (e.g. recent EDI security guidance).

- **NIST** will encourage the CSPAB to work with FIRST to assess how private entities conduct emergency response and how the efforts of Government can be coordinated with them to ensure "911" capability for the NII.

- **NCS**, in coordination with the industry's National Security Telecommunications Advisory Committee (NSTAC), will work through the Network Reliability and Vulnerability Working Group to ensure that National Security and Emergency Preparedness (NS/EP) needs, if any, are accommodated in the NII.

- **NSTISSC** will identify useful security tools and techniques in the national security community that may be applicable to the NII.

- **Working Group on Encryption and Telecommunications** will develop policy recommendations regarding the Government's response to the spread of digital telecommunications equipment and inexpensive encryption devices which could prevent effective wiretaps. This will require development and evaluation of technologies and policies that balance law enforcement's need for access with the need for strong security.

- **The High Performance Computing and Communications Program** (HPCC) will assure development and testing of new technologies for computer security suitable to a high performance environment.

- **The Federal Network Council**, a multi-agency committee that oversees Federal research networks, shall explore specific issues relating to security of the Internet.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

ADMINISTRATOR
OFFICE OF
INFORMATION AND
REGULATORY AFFAIRS

RAY
I PUT ON YOUR
CALENDAR -
Lisa

APR 29 1994

5/11/94
3-5PM

MEMORANDUM FOR PARTICIPANTS IN THE NII SECURITY ISSUES FORUM

FROM: Sally Katzen

SUBJECT Next Meeting of the NII Security Issues Forum

The next meeting of the NII Security Issues Forum will be Wednesday, May 11, 1994 from 3:00 - 5:00 p.m. in OEOB 248. A revised version of the working paper, "NII Security Issues Forum: Role and Strategic Plan," will be available shortly.

Please contact Mary Ann Robinson at (202) 395-3785 to confirm your attendance and arrange access to the building.

NATIONAL SECURITY COUNCIL 5/12

Lisa -

Start a file, if we don't already have one, called

NII Security Issues

former -

and put this stuff in it.

Thanks,

Rich

NII Security Issues Forum 5/11/94

OS Advisory Board - interested in security, will co-sponsor

NII SIF - Roles & Missions
NIST - What about GII connections

Public Forum -
Public's perception of the NII.
15 July 94, Dept of Commerce Auditorium ACC 9-4-DAY.
10 speakers, who would be good
Action: Each of the subcommittees must come up with a good list of speakers

Need a strong contingent of listeners

Report of Other Activities

* Legislation Update - Drafts of legislation proposals - Proposal for adequate improvement provisions.
* Network Reliability & Vulnerability Working Groups:
Bob Marquette
* - Exchange info mtg in Dallas to take a look at what an knowledge of vulnerabilities in networks.
- Firewalls workshop: technology to protect OS.

* NCS

On next page.

* Network Reliability & Vulnerability Working Group
  - Met to organize
  - 3 sub-groups

&

x Encryption IWG

Summary of Hearings - Senator Leahy
Valentine

Outside of Administration, witnesses said we need legislation

S.K. - What's our news PR program?
M.N. - Yes, perhaps Jamie Gorelick, D/AG.

DOD Securities Activities
- JSC report
-

What is the scoop on access to back issues in the C/I PDD.

Lisa -
File under NII
Security Issues forum.

DRAFT PUBLIC MINUTES

NII Security Issue Forum
Cross-cutting Meeting of the IITF

April 19, 1994, 2:00 pm
Room 248, OEOB

Attendees:

Sally Katzen, OMB (Chair)
Bruce McConnell, OMB
Donald McGinnis, EPA
Richard W. Carr, NASA
Jeff Sutton, NASA
Gayle Gordon, DOI
Neil J. Stillman, HHS
Ross Stapleton, DCI/CMS
Brian Harris, NTIA
Vic Bowser, NCS
Stephen L. Squires, ARPA
David Lytel, OSTP
Barbara Valeri, DOD
Michael Keplinger, PTO
Judy Stork, LOC
Stephen Wolff, NSF
Arnold Donahue, OMB
Ronald Matzner, SBA
Eric Dodds, EPA
Ed Springer, OMB
Virginia Huth, OMB
Scott Charney, DOJ
Michael R. Nelson, OSTP
Robert Marquette, NCS
Michele Farquhar, NTIA
Martin Ferris, Treasury
Stu Katzke, NIST
Roger Callahan, NSA
Robert Pepper, FCC
Robert Veeder, OMB

I. Opening Remarks - Sally Katzen, OMB

Following introductions, Ms. Katzen, Chair of the Information Policy Committee of the Information Infrastructure Task Force (IITF), noted that this gathering is a forum for discussion, not a task force or working group. It will solicit input from the public and other agencies and will gather information about public and private sector techniques regarding security.

The IITF is supportive of our efforts. They agree that security is everyone's business. The Government's role is to develop a framework for discussion, while turning to the public sector for direction. The IITF also recognizes that we need to do the job right and do it soon.

II. Federal Role in NII Security

Sally Katzen began by noting that it is important to put down in words just what this Forum is doing and what we see as its role. These issues are important to many people, but can also be misunderstood. A draft discussion paper has been prepared, which I hope we can release soon to clearly set forth our role.

Participants commented that the paper was a good start and helped to clarify issues of concern. Many people are confused by the multifaceted nature of security.

Other comments included:

The paper should emphasize what the Government can learn from the public. The sooner we initiate a dialogue between the public and the Government, the better. This is the way to eliminate misunderstandings.

The ways in which the various Government groups work together also needs to be addressed. Since responsibilities are not sharply delineated, we need to address gaps and areas of overlap.

The Forum should identify needs rather than solutions. The Forum is not ready to give answers, but will raise issues which should be studied.

The Forum should serve as a bridge to the private sector for the exchange of information. The NII is for the people, and in this regard it is different than other systems the government has been involved with. The language needs to recognize this feeling of partnership.

The paper should establish a broad view. The public meetings should help identify diverse user security needs as well as a range of ways to meet these needs, whether legal, policy, technical, or managerial controls.

The Forum should identify needs and recommend changes that should be made. A set of principles should be developed which can serve the entire NII.

State governments are concerned about the Federal role in the NII.

A revised draft incorporating the comments of the groups will be circulated to the Forum participants for review. After the review, the product will be publicly released.

Ms. Katzen stated that we need more information from each Government group in attendance. Each group needs to identify what should be accomplished generally, what they think their group should be working on, and what they think other groups should be working on.

III. Public Meeting -- Discussion of Proposed Strategy

Ms. Katzen noted that it is generally agreed that there is a need for a public meeting. Through a public meeting, we can begin to ascertain the public's view of the NII in order to develop consensus on what security problems should and should not be addressed. The public meeting will focus on the security needs generated by different applications of the NII.

It is important to include those who provide services, not just end users. For example, the health care sector is very interested in security issues as handlers of important personal information.

Marty Ferris, who is organizing the public meeting, reported that the public meeting is planned for this summer in Washington, D.C. It would be desirable to take the public meeting outside the beltway, but it appears to be too costly to do so at this time. Notice of the public meeting will be made in the Federal Register, on bulletin boards, on Internet, and through the press.

Mr. Ferris proposed that each committee chair set up a discussion panel. One participant noted that we want to focus on long term, big picture issues, although one component could be set aside to allow the public to address on "hot" issues.

A discussion of the public meeting ensued, during which a number of particular organization suggestions were made.

The public meeting may require two days. A first session in July is most likely, with a possible follow-up session later in the summer.

It was noted that the Committee on Applications and Technologies is organizing a September public event, which will cover a related issue, barriers to applications.

The Forum needs to be aggressive about publicizing this meeting. Turnout at other, similar, meetings has been small, because the topics were esoteric.

It was suggested that individuals who wish to speak might be asked to submit a 1-2 page position statement as a means of ensuring that a diversity of views are presented for consideration.

The meeting should focus on the needs of users and stay away from specific techniques and hardware. The approach to the public must be utterly candid in order to avoid misunderstandings.

It should be remembered that the Government is the audience for this meeting. IITF members and other high level officials should attend.

Several Forum participants volunteered to assist Mr. Ferris to set up the Public Meeting. [NOTE: The Public Meeting is being scheduled for July 15 in Washington, D.C.]

IV. Legal Issues Update

Scott Charney provided updates on three items:

1. HR 1900, the Privacy for Workers and Consumers Act, is going to full Committee mark-up. If passed in its current form, it could constrain the ability of businesses to back-up files.

2. The U.S. District Attorney in Boston has indicted an MIT student who set up a bulletin board which allegedly allowed copyrighted software to be downloaded for free. Both "Nightline" and "McNeal/Lehrer" have been covering this story.

3. Steve Jackson has appealed the one decision he lost in District Court. It stated that wiretap statutes were <u>not</u> violated. If the appellate court reverses, employers would not be able to legally look at e-mail on their own servers. A decision is expected in 4-5 months.

On the question of the adequacy of current laws to protect security on the NII, a recommendation will soon go to the Attorney General for a "High Tech Crime Package". The National Communications System has made similar suggestions to the National Security Advisor. We will soon involve other agencies, and we hope to have it ready in time for the next Congress. To assist the Forum, the Department of Justice is starting a project

to track civil lawsuits.

IV. Status of Other Activities - Progress Reports

1. Network Reliability and Vulnerability Working Group
Robert Marquette, NCS

The Working Group has held meetings and briefings concerning new technologies and network security. It is looking at issues and identifying those which require more study.

NCS has started a pilot program for secure e-mail. DOD is being wired, and if it works, the number of agencies participating will increase. The largest need at this time is to develop interfacing software. NCS is also holding a symposium on firewalls.

Recently, a meeting was held concerning emergency preparedness with the Department of Energy and telephone utility companies.

2. NIST and the Computer Security and Privacy Advisory Board (CSPAB)
Stuart Katzke, NIST

At the request of the Forum, NIST and the Advisory Board will prepare a study of the uses of security technology by private organizations. The study will focus on the perspective of private industry. Topics to be discussed include varying views of security issues, justification of management, different products used, ease of integration of products, operational procedures, oversight, and needed technologies not available.

3. Forum of Incident Response & Security Teams (FIRST)
Stuart Katzke, NIST

At its September meeting, FIRST will discuss how the private sector conducts its emergency procedures. FIRST has recently published guidance on subjects such as anti-virus operations and electronic commerce. These are all available on-line. Several more handbooks are near publication.

In describing NIST's security program, Dr. Katzke noted that public input is a necessary factor for all aspects of NIST's work. NIST is working on standards for authentication interfaces. NIST will also play a role in determining and evaluating security criteria, especially on the international front.

Dr. Katzke also noted that it is generally agreed among the

civilian agencies that the DOD level of protection for e-mail is probably overkill for non-military uses. We need to develop a business quality product which won't interfere with the system's functionality.

4. Working Group on Encryption and Telecommunications
Mike Nelson, OSTP

The Group is discussing the following:

1. Capstone technology for encryption and authentication
2. Lag in working with industry to develop new security technologies
3. Software systems
4. NIST's role in security
5. International encryption

5. National Security Telecommunications and Information Systems Security Committee (NSTISSC)
Roger Callahan, NSA

The initial NSTISSC report has been completed and copies were distributed. It takes a comprehensive approach and includes descriptions of some programs now at NIST and who is responsible for them.

V. Next Steps

Ms. Katzen concluded the meeting by noting that the Working Groups and Committees should prepare lists of key security issues, while the Forum will keep an eye on pending legislation. The Forum will meet again in 2-3 weeks.

DRAFT PUBLIC MINUTES

NII Security Issue Forum
Cross-cutting Meeting of the IITF

April 19, 1994, 2:00 pm
Room 248, OEOB

Attendees:

Sally Katzen, OMB (Chair)
Bruce McConnell, OMB
Donald McGinnis, EPA
Richard W. Carr, NASA
Jeff Sutton, NASA
Gayle Gordon, DOI
Neil J. Stillman, HHS
Ross Stapleton, DCI/CMS
Brian Harris, NTIA
Vic Bowser, NCS
Stephen L. Squires, ARPA
David Lytel, OSTP
Barbara Valeri, DOD
Michael Keplinger, PTO
Judy Stork, LOC
Stephen Wolff, NSF
Arnold Donahue, OMB
Ronald Matzner, SBA
Eric Dodds, EPA
Ed Springer, OMB
Virginia Huth, OMB
Scott Charney, DOJ
Michael R. Nelson, OSTP
Robert Marquette, NCS
Michele Farquhar, NTIA
Martin Ferris, Treasury
Stu Katzke, NIST
Roger Callahan, NSA
Robert Pepper, FCC
Robert Veeder, OMB

I. Opening Remarks - Sally Katzen, OMB

Following introductions, Ms. Katzen, Chair of the Information Policy Committee of the Information Infrastructure Task Force (IITF), noted that this gathering is a forum for discussion, not a task force or working group. It will solicit input from the public and other agencies and will gather information about public and private sector techniques regarding security.

The IITF is supportive of our efforts. They agree that security is everyone's business. The Government's role is to develop a framework for discussion, while turning to the public sector for direction. The IITF also recognizes that we need to do the job right and do it soon.

II. Federal Role in NII Security

Sally Katzen began by noting that it is important to put down in words just what this Forum is doing and what we see as its role. These issues are important to many people, but can also be misunderstood. A draft discussion paper has been prepared, which I hope we can release soon to clearly set forth our role.

Participants commented that the paper was a good start and helped to clarify issues of concern. Many people are confused by the multifaceted nature of security.

Other comments included:

The paper should emphasize what the Government can learn from the public. The sooner we initiate a dialogue between the public and the Government, the better. This is the way to eliminate misunderstandings.

The ways in which the various Government groups work together also needs to be addressed. Since responsibilities are not sharply delineated, we need to address gaps and areas of overlap.

The Forum should identify needs rather than solutions. The Forum is not ready to give answers, but will raise issues which should be studied.

The Forum should serve as a bridge to the private sector for the exchange of information. The NII is for the people, and in this regard it is different than other systems the government has been involved with. The language needs to recognize this feeling of partnership.

The paper should establish a broad view. The public meetings should help identify diverse user security needs as well as a range of ways to meet these needs, whether legal, policy, technical, or managerial controls.

The Forum should identify needs and recommend changes that should be made. A set of principles should be developed which can serve the entire NII.

State governments are concerned about the Federal role in the NII.

A revised draft incorporating the comments of the groups will be circulated to the Forum participants for review. After the review, the product will be publicly released.

Ms. Katzen stated that we need more information from each Government group in attendance. Each group needs to identify what should be accomplished generally, what they think their group should be working on, and what they think other groups should be working on.

III. Public Meeting -- Discussion of Proposed Strategy

Ms. Katzen noted that it is generally agreed that there is a need for a public meeting. Through a public meeting, we can begin to ascertain the public's view of the NII in order to develop consensus on what security problems should and should not be addressed. The public meeting will focus on the security needs generated by different applications of the NII.

It is important to include those who provide services, not just end users. For example, the health care sector is very interested in security issues as handlers of important personal information.

Marty Ferris, who is organizing the public meeting, reported that the public meeting is planned for this summer in Washington, D.C. It would be desirable to take the public meeting outside the beltway, but it appears to be too costly to do so at this time. Notice of the public meeting will be made in the Federal Register, on bulletin boards, on Internet, and through the press.

Mr. Ferris proposed that each committee chair set up a discussion panel. One participant noted that we want to focus on long term, big picture issues, although one component could be set aside to allow the public to address on "hot" issues.

A discussion of the public meeting ensued, during which a number of particular organization suggestions were made.

The public meeting may require two days. A first session in July is most likely, with a possible follow-up session later in the summer.

It was noted that the Committee on Applications and Technologies is organizing a September public event, which will cover a related issue, barriers to applications.

The Forum needs to be aggressive about publicizing this meeting. Turnout at other, similar, meetings has been small, because the topics were esoteric.

It was suggested that individuals who wish to speak might be asked to submit a 1-2 page position statement as a means of ensuring that a diversity of views are presented for consideration.

The meeting should focus on the needs of users and stay away from specific techniques and hardware. The approach to the public must be utterly candid in order to avoid misunderstandings.

It should be remembered that the Government is the audience for this meeting. IITF members and other high level officials should attend.

Several Forum participants volunteered to assist Mr. Ferris to set up the Public Meeting. [NOTE: The Public Meeting is being scheduled for July 15 in Washington, D.C.]

IV. Legal Issues Update

Scott Charney provided updates on three items:

1. HR 1900, the Privacy for Workers and Consumers Act, is going to full Committee mark-up. If passed in its current form, it could constrain the ability of businesses to back-up files.

2. The U.S. District Attorney in Boston has indicted an MIT student who set up a bulletin board which allegedly allowed copyrighted software to be downloaded for free. Both "Nightline" and "McNeal/Lehrer" have been covering this story.

3. Steve Jackson has appealed the one decision he lost in District Court. It stated that wiretap statutes were not violated. If the appellate court reverses, employers would not be able to legally look at e-mail on their own servers. A decision is expected in 4-5 months.

On the question of the adequacy of current laws to protect security on the NII, a recommendation will soon go to the Attorney General for a "High Tech Crime Package". The National Communications System has made similar suggestions to the National Security Advisor. We will soon involve other agencies, and we hope to have it ready in time for the next Congress. To assist the Forum, the Department of Justice is starting a project

to track civil lawsuits.

IV. Status of Other Activities - Progress Reports

1. Network Reliability and Vulnerability Working Group
Robert Marquette, NCS

The Working Group has held meetings and briefings concerning new technologies and network security. It is looking at issues and identifying those which require more study.

NCS has started a pilot program for secure e-mail. DOD is being wired, and if it works, the number of agencies participating will increase. The largest need at this time is to develop interfacing software. NCS is also holding a symposium on firewalls.

Recently, a meeting was held concerning emergency preparedness with the Department of Energy and telephone utility companies.

2. NIST and the Computer Security and Privacy Advisory Board (CSPAB)
Stuart Katzke, NIST

At the request of the Forum, NIST and the Advisory Board will prepare a study of the uses of security technology by private organizations. The study will focus on the perspective of private industry. Topics to be discussed include varying views of security issues, justification of management, different products used, ease of integration of products, operational procedures, oversight, and needed technologies not available.

3. Forum of Incident Response & Security Teams (FIRST)
Stuart Katzke, NIST

At its September meeting, FIRST will discuss how the private sector conducts its emergency procedures. FIRST has recently published guidance on subjects such as anti-virus operations and electronic commerce. These are all available on-line. Several more handbooks are near publication.

In describing NIST's security program, Dr. Katzke noted that public input is a necessary factor for all aspects of NIST's work. NIST is working on standards for authentication interfaces. NIST will also play a role in determining and evaluating security criteria, especially on the international front.

Dr. Katzke also noted that it is generally agreed among the

civilian agencies that the DOD level of protection for e-mail is probably overkill for non-military uses. We need to develop a business quality product which won't interfere with the system's functionality.

4. Working Group on Encryption and Telecommunications
Mike Nelson, OSTP

The Group is discussing the following:

1. Capstone technology for encryption and authentication
2. Lag in working with industry to develop new security technologies
3. Software systems
4. NIST's role in security
5. International encryption

5. National Security Telecommunications and Information Systems Security Committee (NSTISSC)
Roger Callahan, NSA

The initial NSTISSC report has been completed and copies were distributed. It takes a comprehensive approach and includes descriptions of some programs now at NIST and who is responsible for them.

V. Next Steps

Ms. Katzen concluded the meeting by noting that the Working Groups and Committees should prepare lists of key security issues, while the Forum will keep an eye on pending legislation. The Forum will meet again in 2-3 weeks.

Agenda
NII Security Issues forum
of the Information Infrastructure Task Force

OEOB Room 180
Wednesday, May 11, 1994
3:00 - 5:00 p.m.

I. Introductory Remarks -- Sally Katzen, Chair

Distribute minutes of the previous meeting for correction

II. Approve revised discussion paper, "Roles and Responsibilities: NII Security Issues Forum"

III. Collect lists of top security issues

IV. Public Forum

A. Progress Report
Marty Ferris

B. Involvement of the Committees of the IITF
Sally Katzen

C. Involvement of the NII/AC
Bruce McConnell

V. Status of Other Activities -- Brief Reports

A. Legislative Update
Scott Charney, DOJ

B. Network Reliability and Vulnerability Working Group
Bob Marquette, NCS

C. Working Group on Encryption and Telecommunications
Mike Nelson, OSTP

D. NIST, the Computer Security and Privacy Advisory Board (CSPAB), and the Forum of Incident Response & Security Teams (FIRST)
Jim Burrows, NIST

E. DoD Security Activities
Barbara Valeri, DoD

F. National Security Telecommunications and Information Systems Security Committee (NSTISSC)
Roger Callahan, NSA

VI. Next Steps -- Sally Katzen

MAY 10 1994

MEMORANDUM FOR PARTICIPANTS OF NII SECURITY ISSUE FORUM

FROM: Bruce McConnell

SUBJECT: Next meeting of the NII Security Issues Forum

Attached is a draft agenda and a revised version of the paper, "Role and Strategic Plan: NII Security Issues Forum," for approval at the meeting on Wednesday, May 11, 1994, from 3:00 to 5:00 p.m. **Please note that the location has been changed to room 180 in the OEOB.**

Representatives of each group should remember to bring a list of top security issues they are addressing and a list of issues they believe should be addressed by others.

If you haven't already, please contact Mary Ann Robinson at (202) 395-3785 to confirm your attendance and arrange for access to the building.

Enclosures (2)

NCR Wilhelm,
can you Please
attend this today
for Ray Thank you-
Lisa

Draft Agenda
NII Security Issues Forum
of the Information Infrastructure Task Force

OEOB Room 180
Wednesday, May 11, 1994
3:00 - 5:00 p.m.

I. Introductory Remarks -- Sally Katzen, chair

Distribute minutes of the previous meeting for correction.

II. Approve revised discussion paper, "Roles and Responsibilities: NII Security Issues Forum."

III. Collect lists of top security issues

IV. Public Forum

A. Progress Report -- Marty Ferris

B. Involvement of the Committees of the IITF -- Sally Katzen

C. Involvement of the NII/AC -- Bruce McConnell

D. Involvement of the Computer Security and Privacy Advisory Board -- Jim Burrows

IV. Status of Other Activities -- Brief Progress Reports

A. Legislative Update -- Scott Charney, DOJ

B. Network Reliability and Vulnerability Working Group -- D. T. Signori, DISA

C. Working Group on Encryption and Telecommunications -- Mike Nelson, OSTP

D. NIST, the Computer Security and Privacy Advisory Board (CSPAB), and the Forum of Incident Response & Security Teams (FIRST) -- Jim Burrows, NIST

E. DoD Security Activities -- Barbara Valeri, DoD

F. National Security Telecommunications and Information Systems Security Committee (NSTISSC) -- John Nagengast, NSA

V. Next Steps -- Sally Katzen

Roles and Responsibilities:
NII Security Issues Forum

The Role of Government in NII Security:

Government has an important public mission to support the secure use of the National Information Infrastructure (NII). Government must cooperate with the private sector and with the public-at-large in setting legal and policy ground rules for security in the NII. This responsibility is shared between the Federal government and State, local, and tribal governments.

The Role of the NII Security Issues Forum:

The NII Security Issues Forum will ascertain the security needs of the various NII user communities and the Federal role in assuring such security. It will ensure coordination of the security activities across the various Committees of the IITF and serve as a clearinghouse for Federal security efforts related to the NII. The Forum will also consider the scope of legal and policy remedies necessary to achieve desired security in the NII.

Strategy:

The Committees of the IITF will identify the security needs of various user sectors affiliated with the NII. Committees should solicit input and initiate dialogue with their constituent users. This dialogue should help define the security requirements for the NII in order to determine needed policy, technology, and managerial controls, and what the Federal role will be to assure that those needs are fulfilled.

To accomplish this, the Forum will solicit participation from individuals, organizations, and State, local, and tribal governments. An initial Public Meeting to stimulate this dialogue is being planned.

The Forum will also gather information concerning the impact of civil case law on security in electronic environments and will analyze the sufficiency of Federal criminal law.

Finally, the Forum will gather information about public and private sector security technology and management controls in order to ensure that needed security capabilities will be available.

Organizational Responsibilities:

As initial steps, the Forum will conduct outreach activities and assess current policies, as well as act as a clearinghouse for the security activities of the IITF and of other Federal government entities.

I. The Forum will:

- Maintain a public dialogue involving individuals, organizations, industry, and State, local, and tribal governments in discussions of the needs for, legal aspects of, and techniques for security in the NII.

- Assess the sufficiency of the current criminal statutory regime; notify the participants of movement on relevant legislation; report on developments in civil case law relevant to computer security; and consider the need for amendment to statutes or new laws to address emerging crimes.

II. The Forum will coordinate the following IITF activities:

- The **Telecommunications Policy Committee**, the **Information Policy Committee**, and the **Committee on Applications and Technology** of the IITF will identify security requirements for their constituencies.

In addition, Working Groups of these Committees will also identify security requirements for their constituencies, as appropriate. For example:

- The **Intellectual Property Rights Working Group (IPRWG)** and the **Privacy Working Group (PWG)**, through the Information Policy Committee, will advise the Forum on security issues pertaining to Intellectual Property Rights and Privacy.

- The **Government Information Technology Services Working Group (GITS)**, through the Committee on Applications and Technology, will advise the Forum on security issues pertaining to the application of information technology by Federal agencies to improve service delivery and accomplish agency missions.

- The **Network Reliability and Vulnerability Working Group**, with the assistance of the NCS and through the Telecommunications Policy Committee, will advise the Security Forum on (1) protection for all users from

catastrophic failure of the network and the information services it provides, along with mechanisms for recovery from threats ranging from natural disasters to overt attacks, and (2) national security and emergency preparedness requirements.

- Other Working Groups in the **Committee on Applications and Technology** will identify sector-specific user requirements for security, such as in the areas of health information and education.

III. The Forum will draw together technical and analytical support throughout Government by coordinating the efforts of the following federal Government entities:

- **NIST** will encourage the Computer Security and Privacy Advisory Board (CSPAB) to assist NIST in the assessment of security tools and techniques in use outside of the Federal Government and assess where research and development on security technology would be useful for the NII.

- **NIST** will identify Federal security products and techniques that will be useful in the NII (e.g. recent EDI security guidance).

- **NIST** will encourage the CSPAB to work with FIRST to assess how private entities conduct emergency response and how the efforts of Government can be coordinated with them to ensure "911" capability for the NII.

- **NCS**, in coordination with the industry's National Security Telecommunications Advisory Committee (NSTAC), will work through the Network Reliability and Vulnerability Working Group to ensure that National Security and Emergency Preparedness (NS/EP) needs, if any, are accommodated in the NII.

- **NSTISSC** will identify useful security tools and techniques in the national security community that may be applicable to the NII.

- **Working Group on Encryption and Telecommunications** will develop policy recommendations regarding the Government's response to the spread of digital telecommunications equipment and inexpensive encryption devices which could prevent effective wiretaps. This will require development and evaluation of technologies and policies that balance law enforcement's need for access with the need for strong security.

- **The High Performance Computing and Communications Program** (HPCC) will assure development and testing of new technologies for computer security suitable to a high performance environment.

- **The Federal Network Council**, a multi-agency committee that oversees Federal research networks, shall explore specific issues relating to security of the Internet.

Agenda
Security and the National Information Infrastructure
OEOB 180
Friday, February 18, 2:00 - 5:00

I. Opening Remarks: Sally Katzen

II. Legal and Policy Issues

A. Federal Criminal Statutes
Scott Charney, Department of Justice

B. Civil perspective -- Sally Katzen

III. Emerging User Requirements

A. Tom Wasilewski, NTIA
Telecommunications Policy Committee

B. Kaz Kazenske, Patent & Trademark Office
Information Policy Committee, Intellectual Property Rights Working Group

C. Rob Veeder, Office of Management and Budget
Information Policy Committee, Privacy Working Group

D. Cita Furlani, NIST
Committee on Applications and Technology

IV. Technical Issues

A. Lynn McNulty, NIST, and Computer Security Privacy Advisory Board (CSPAB)

B. John Nagengast, National Security Telecommunications and Information Systems Security Committee (NSTISSC)

NSD created

C. Major General Robert Marquette (Retired), National Communications System (NCS)

D. Dennis Steinauer, Forum of Incident Response & Security Teams (FIRST)

E. Mike Nelson, OSTP, Working Group on Encryption and Telecommunications

V. Next Steps: Sally Katzen

Session of NII

2/18/94

Sally Katzen - OMB

Govt Role in Area of Security in Embracing the NII > Govt est. Legal & Policy Framework
> Private Sector will develop.

Security
- Confidentiality
- Integrity
- Reliability

Legal/Policy Issues

DOJ - Scott Charney

ECPA comms privacy act — Protects both Govt & Public

Problems
> Provides some security for electronic mail
> But missing is provisions re Private Providers may provide.

Computer Security Act — (18 USC T 1030)

T 18 USC § 1030 A2 | A3 | A4 | A5

Key vehicle for protecting citizens from attacking networks — but does not protect against insiders from attacking — "acting in excess of your authority" with lawful access.

Senator Crime Bill — addresses this gap.

But decriminalizes some current criminal acts

Security & the NII

(2)

2/18/94

Trying over past year to shift away from idea that "Hackers" who do not intend harm would be OK.

Focus on Non-Economic Harms.

Increasing # cases of people stealing source codes.
ITSP does not cover intangible property well.
IBM/Digital concerns — expressed interest in trade secrets legislation
Corporate security wants "
Corporate management does not "

D working w/ABI on trade secrets legislation.

Problem — where does intangible property reside?

International component (III)

① There is not agreement between countries on what constitutes a crime
② Trying to promote International Convention re Computer Crime.
③ Procedural problems — rapid swift actions.

Council of Europe is taking lead on this problem but we do not have status.

o Minutes will be available to the public

Communications Privacy is jeopardized by advances in telecommunications.
> In immediate future illegal wiretapping will be on the rise.

Cellular & Cordless phones also not protected.

CIVIL PERSPECTIVE > AN ABSENCE OF INFORMATION / CASE LAW FROM CIVIL PERSPECTIVE?

(*) THERE IS CIVIL REMEDY UNDER FED WIRETAP STATUTE AND ELECTRONIC MAIL STATUTE > COST OF BRINGING SUIT IS PROHIBITIVE TO REALLY BE EFFECTIVE

WHAT IS PRIVATE SECTOR DOING? BRINGING SUIT?

LEAD ON STATUS ON CIVIL REMEDIES — ELECTRONIC MAIL ASSOCIATION COULD BE

o JUSTICE FOLLOWUP ON THESE ISSUES CRIMINAL LAW & [redacted]

o [redacted] - TAKE LEAD ON CIVIL SIDE -

III. EMERGING USER REQUIREMENTS

A. TEL COMMS POLICY — MUST NEED TO DEFINE WHO ARE THE USERS.

> WHAT IS COST OF SECURITY? WHO PAYS?

B. SEE AS MUCH BIGGER MULTI-MEDIA PROBLEM VIA COM-US PARAMOUNT.

(9)

2/18/94

★ Privacy is lynchpin to ~~confidence~~ Public confidence in using NII

users will want a form of security that will keep pace with the geometric growth of use of NII.

Some evidence that peoples behavior indicates that there that concerned all that much about privacy — at this point — as it relates to NII.

D, NIST

★ > go back to your groups — get clear statement of privacy / security — concerns manifested how?

★ have to marry good policy with what the future will hold in this new electronic world.

IV. TECHNICAL ISSUES

STANDARDS

★ NII > CI THREAT — COB SHOULD TAKE ON AS ISSUE - Study and prepare paper.

FIS use of NII or III

Should look at from Defensive & Offensive point of view — how could use to what end →

(5)

2/18/94

▶ NII is here now - and already growing
- not something that will be switched on in the future.

⊛ Convene 2nd Meeting in about 30 days

Sally wants to engage the public

Forums ① Briefing - to hear from industry - what they want, need - etc.

② Open discussion - to hear public - and talk with them.

public outreach