FOIA Number: 2008-1524-F

FOIA MARKER

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

Collection/Record Group: Clinton Presidential Records

Subgroup/Office of Origin: Office of Science and Technology

Series/Staff Member:

Subseries:

OA/ID Number: 43311

FolderID:

Folder Title:
Director Actions [1]

Stack:	Row:	Section:	Shelf:	Position:
S	1	1	7	3

Withdrawal/Redaction Sheet
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. list	Conference attendees [National Security Act; 10 USC 424] (3 pages)	11/15/2000	P3/b(3), b(6)

COLLECTION:
Clinton Presidential Records
Office of Science and Technology Policy

OA/Box Number: 43311

FOLDER TITLE:
Director Actions [1]

2008-1524-F
kc1213

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Paul A.
Vic T.
Terry K.

Memo to NSTC regarding CNS International Technology Transfer effort

Attached is a copy of the memo that Neal Lane signed out to NSTC principals in an effort to sustain some momentum behind the effort to improve management of international technology transfer at the Federal laboratories.

Although CNS will probably not meet in the near future, Jon Paugh at the Department of Commerce has a parallel technology transfer group (many of the same experts) that can move forward. Jon's number is 202-501-8023 and e-mail is jpaugh@ta.doc.gov.

Gerald

THE WHITE HOUSE

WASHINGTON

January 18, 2001

MEMORANDUM FOR PRINCIPALS OF THE NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

FROM: NEAL LANE
ASSISTANT TO THE PRESIDENT
FOR SCIENCE AND TECHNOLOGY

SUBJECT: International Technology Transfer and the Federal Laboratories

The Committee on National Security (CNS) of the National Science and Technology Council has provided recommendations to improve the process by which the U.S. Government assesses and manages international participation in cooperative research and development agreements and exclusive licenses involving the Federal laboratories. Although there is not time in the Administration to make the recommended revisions to Executive Order 12591, "Facilitating Access to Science and Technology," I urge affected NSTC agencies to continue to move this process forward.

Over the past two and a half years, the CNS International Technology Transfer Working Group has been evaluating options to better assess and manage international participation in cooperative research and development agreements and exclusive licenses. This effort was launched as a result of concerns expressed in the Administration as well as by Congress that procedures of the U.S. Government were not consistent or adequate. Some of the Congressional concerns were reflected in H.R. 209, the Technology Transfer Commercialization Act of 2000, which the President signed into law on November 1, 2000. Section 8 of this Act directs the National Science and Technology Council through the Committee on National Security to assess policies and procedures for evaluating international participation in cooperative research and development agreements at the Federal laboratories. The law directs an initial assessment by agencies within 90 days and a report on the adequacy of existing procedures and issuance of appropriate guidance to the agencies within one year.

The work of the CNS International Technology Transfer Working Group, which was conducted in consultation with Congress, sets forth the key steps. Key recommendations include steps to clarify agency roles as well as the establishment of a process to gather more precise data on international participation and procedures for managing such participation. The recommendations are summarized in Attachment 1. Working with a long-standing interagency technology transfer working group led by the Department of Commerce, a process has been readied for implementation that would improve the management of international participation in cooperative research and development agreements and exclusive licenses involving the Federal laboratories, and that would meet the directives of the law. The data to be tracked are noted in Attachment 2. It is recommended that the NSTC agencies assign priority to this effort to ensure its success.

ATTACHMENT 1

Key Recommendations of the Committee on National Security regarding International Technology Transfer and the Federal Laboratories

Purpose: To review the assessment and management of international participation in cooperative research and development agreements and exclusive licenses involving Federal laboratories, so that these processes can be made more effective.

Scope: Cooperative Research and Development Agreements (CRADAs) and similar cooperative research agreements with Federal laboratories in which intellectual property may be created, and exclusive licenses from Federal laboratories.

Key points:

- Roles of the agencies should be clarified with respect to information that should be made available to conduct the reviews. Specifically, 1) the Departments of Commerce and State should cooperate to maintain a record of foreign practices regarding U.S. participation in similar arrangements in other countries; 2) USTR should provide clear guidance regarding foreign protection of intellectual property rights; and 3) the Departments of Commerce, State and Defense should cooperate with the Federal laboratories to ensure timely and accurate review of export control concerns.

- Agencies should be directed to consider the impact on the competitiveness of U.S. industry of international participation in cooperative research and development agreements with Federal laboratories, and of exclusive licensing to foreign entities of technologies developed at Federal laboratories.

- Agencies should be directed to provide data regarding international participation in CRADAs and other cooperative research agreements comparable to CRADAs, as well as exclusive licenses, and to meet quarterly to discuss their various approaches for dealing with this issue. At the end of one year, a report should be submitted to the National Science and Technology Council, in accordance with H.R. 209, with recommendations for further action, if any.

Data Collection:

- To ensure that appropriate data are collected to best guide policy and procedures, a data collection form was developed in close consultation with the Department of Commerce-led technology transfer working group. This is provided in Attachment 2.

ATTACHMENT 2

Draft Procedures for Quarterly Meeting Participation

1) Participating Agencies

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Interior
Department of Transportation
Department of Veterans Affairs
Environmental Protection Agency
National Aeronautics and Space Administration
Other agencies using technology transfer agreements as defined in E.O. 12591

2) Data to be collected for quarterly meetings

Two categories of information to be collected for meetings:

a. Data reflecting relevant characteristics of covered agreements entered into in the quarter

b. Presentation concerning one or more of these agreements in a way that illuminates the question of the adequacy of existing procedures to deal with the questions of foreign[1] participation/competitive impacts.

a) **Data** reflecting relevant characteristics of covered agreements:
   i) Total # of agreements of each type entered into
   ii) Total # of agreements involving foreign parties
   iii) Total and average value of private sector party contributions (cash and in-kind during first three years of agreement)
   iv) Total and average value of foreign party contributions (cash and in-kind)
   v) # of agreements in which domestic manufacture requirement waived (including both domestic party and foreign party waivers)
   vi) For agreements involving foreign parties (or domestic parties where domestic manufacture requirement waived):
      (1) Technology subject matter of agreement
      (2) Lab point of contact
      (3) Name and location of foreign party
   vii) # of agreements requiring compliance with export control laws (application for license)

[1] Consistent with E.O 12591, "foreign entities" are defined as entities that are directly or indirectly controlled by a foreign company or government.

b) **Presentations**: Each agency would be required to offer one written presentation at each quarterly meeting. The purpose would be to add to the collective understanding of the extent and nature of foreign participation in technology transfer agreements. Possible topics include:
   i) Experience during quarter in application of domestic manufacture requirement (cases where agreement could not be reached, cases where it was applied, cases where it was waived)
   ii) Experience with public notice requirement in exclusive licenses involving foreign parties (comments concerning competitive or national security issues)
   iii) Trends in the technology subject matters of interest to foreign parties
   iv) Agency-specific procedures designed to deal with foreign participation and competitive issues that may be of interest to the group (best practices) in areas such as negotiation of royalty rates, resolution of domestic manufacturing issues, etc.

3) Format for submission of data/issues for quarterly meetings

a) **Data:** The format for the data to be submitted (Item 1, above) can be worked out by the agencies.

b) **Presentations:** The format for the submission of issues would be as follows:

Submitting Agency:

Issue and Relevance to E.O. Procedures:

Background:

Discussion:

4) Potential threshold tests

These would be developed on basis of data submitted at meetings. At this point, possible tests might relate to:

a) Fact of foreign involvement
b) Waiver of SMR (even if no foreign party)
c) Extent of foreign contribution to work
d) Anticipated size of contract, value of IP (reflected in royalty rates)
e) Concerns expressed by domestic industry in response to notice, etc.
f) Area of technology involved

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

November 28, 2000

Dr. Neal Lane
Assistant to the President
for Science and Technology
Executive Office of the President
Washington, DC 20502

Dear Dr. Lane:

Thank you for the kind remarks in your 24 October letter. I am looking forward to working with you and your staff on the critical National Security and Emergency Preparedness (NS/EP) communications issues facing our Nation.

In regards to your request for the National Security Telecommunications Advisory Committee (NSTAC) to undertake a fresh look at the possibility of a widespread outage in the converged and Next Generation Network environment, I have asked NSTAC's Industry Executive Subcommittee (IES) to determine the best approach for addressing your tasking. The review will take into consideration previous NSTAC analysis of widespread outages, recent network convergence studies, and the results of the NSTAC/OSTP sponsored R&D Exchange Forum. We will work closely with Dr. Terry Kelly of your staff and the staff of the National Communications System (NCS) on this study effort. An interim report will be provided at the NSTAC XXIV meeting in June 2001.

The NSTAC recognizes the criticality of this study for national security and emergency preparedness operations and our national economic security. We will endeavor to provide you and the new Administration timely recommendations on this important NS/EP task.

Sincerely,

Daniel P. Burnham
NSTAC Chair

cc: NSTAC Principals
Industry Executive Subcommittee
National Security Council (Mr. Clarke)
Executive Agent, NCS (SECDEF)
Manager, NCS

THE WHITE HOUSE

WASHINGTON

October 24, 2000

Mr. Daniel P. Burnham
President and CEO
Raytheon Company
Executive Offices
141 Spring Street
Lexington, Massachusetts 02421

Dear Mr. Burnham:

I was pleased to meet with and welcome you to the Chair of the National Security Telecommunications Advisory Committee in September. As I mentioned at the time, I look forward to working with you on the critical issues we face. It is on one of these, the potential for a widespread outage in the information infrastructure, that I write today.

In the past, established telecommunications carriers operating under government regulation and industry agreements made up the public telephone network that provided the critical communications services the nation depended upon in National Security/Emergency Preparedness (NS/EP) situations. The NSTAC *Information Technology Progress Impact Task Force Report on Convergence,* released this past May, made clear that the convergence of the voice and the largely unregulated data networks will change not only the physical nature of the communications network, but may introduce many new technical, operational and security concerns as well. I applaud the NSTAC for producing this timely and important report.

The challenges that this report so clearly highlight may require government to develop new policies, plans, programs, and perhaps protections under law or other mandates to help ensure the availability of NS/EP communications. Most importantly, in the twenty-first Century NS/EP communication requirements extend beyond traditional voice communications, and include the full range of broadband capabilities the President and other senior government officials need to guide the nation in times of crisis. These new concerns and technologies require us to consider the possibility and impact of a widespread outage, not just in the legacy public switching network, but in the Internet and the emerging converged network as well.

In view of these facts, we need to take a fresh look at the possibility of a widespread outage, and for this the President needs the expertise of the NSTAC. I therefore ask that you undertake this task. In particular, I believe the NSTAC's view on the following questions would be particularly helpful:

- Given the expanded functionality mentioned above, is a widespread outage of the converged and next generation networks a realistic possibility, and what are the risk factors that both the government and industry need to consider?

- How are the NSTAC and the industry in general preparing to deal with those aspects of network convergence, and the Next Generation Network(s) in particular, that adversely affect NS/EP communications security and reliability? In particular,

  - What does the industry and government need to do to help mitigate the increased vulnerabilities of the converged network?
  - What reasonable steps could the government take to help the NSTAC and the industry in general better prepare to detect and contain threats likely to act upon those vulnerabilities and cause a widespread outage or other significant degradation of NS/EP readiness?

- How do we deal with widespread outages of this broader category of communications services? In particular,

  - How should existing NSTAC, NCS/NCC, and other private and government organizations evolve with the networks to ensure a quick, organized and technically competent response in the case of a widespread outage?
  - What reasonable steps could the government take to help the NSTAC and the industry in general better prepare to react to a widespread outage in these networks?

You should not limit yourself to these specific concerns, but address whatever additional related issues you feel should be brought to the President's attention. You should also give consideration to the potentially sensitive nature of your findings and recommendations, as it is entirely possible that this report may need to be classified in order for it to give sufficiently detailed descriptions of and recommendations for addressing vulnerabilities to this critical piece of our national infrastructure.

In conclusion, I ask that you apply the unique resources of the NSTAC to undertake this effort aimed at understanding the dimensions of this problem and identifying cost-effective measures that industry and government can take to prevent, or in the worst case to restore services after, a widespread outage. I know that this effort will not be completed on my watch, but this will be a key component in building the understanding of this issue for my successor and the next President, and for crafting wise and effective policy. My point of contact for this effort will be Dr. Terry Kelly (202-456-6057).

Sincerely,

Neal Lane

Neal Lane
Assistant to the President
for Science and Technology

THE WHITE HOUSE

WASHINGTON

October 24, 2000

Mr. Daniel P. Burnham
President and CEO
Raytheon Company
Executive Offices
141 Spring Street
Lexington, Massachusetts 02421

Dear Mr. Burnham:

I was pleased to meet with and welcome you to the Chair of the National Security Telecommunications Advisory Committee in September. As I mentioned at the time, I look forward to working with you on the critical issues we face. It is on one of these, the potential for a widespread outage in the information infrastructure, that I write today.

In the past, established telecommunications carriers operating under government regulation and industry agreements made up the public telephone network that provided the critical communications services the nation depended upon in National Security/Emergency Preparedness (NS/EP) situations. The NSTAC *Information Technology Progress Impact Task Force Report on Convergence*, released this past May, made clear that the convergence of the voice and the largely unregulated data networks will change not only the physical nature of the communications network, but may introduce many new technical, operational and security concerns as well. I applaud the NSTAC for producing this timely and important report.

The challenges that this report so clearly highlight may require government to develop new policies, plans, programs, and perhaps protections under law or other mandates to help ensure the availability of NS/EP communications. Most importantly, in the twenty-first Century NS/EP communication requirements extend beyond traditional voice communications, and include the full range of broadband capabilities the President and other senior government officials need to guide the nation in times of crisis. These new concerns and technologies require us to consider the possibility and impact of a widespread outage, not just in the legacy public switching network, but in the Internet and the emerging converged network as well.

In view of these facts, we need to take a fresh look at the possibility of a widespread outage, and for this the President needs the expertise of the NSTAC. I therefore ask that you undertake this task. In particular, I believe the NSTAC's view on the following questions would be particularly helpful:

- Given the expanded functionality mentioned above, is a widespread outage of the converged and next generation networks a realistic possibility, and what are the risk factors that both the government and industry need to consider?

- How are the NSTAC and the industry in general preparing to deal with those aspects of network convergence, and the Next Generation Network(s) in particular, that adversely affect NS/EP communications security and reliability? In particular,

  - What does the industry and government need to do to help mitigate the increased vulnerabilities of the converged network?
  - What reasonable steps could the government take to help the NSTAC and the industry in general better prepare to detect and contain threats likely to act upon those vulnerabilities and cause a widespread outage or other significant degradation of NS/EP readiness?

- How do we deal with widespread outages of this broader category of communications services? In particular,

  - How should existing NSTAC, NCS/NCC, and other private and government organizations evolve with the networks to ensure a quick, organized and technically competent response in the case of a widespread outage?
  - What reasonable steps could the government take to help the NSTAC and the industry in general better prepare to react to a widespread outage in these networks?

You should not limit yourself to these specific concerns, but address whatever additional related issues you feel should be brought to the President's attention. You should also give consideration to the potentially sensitive nature of your findings and recommendations, as it is entirely possible that this report may need to be classified in order for it to give sufficiently detailed descriptions of and recommendations for addressing vulnerabilities to this critical piece of our national infrastructure.

In conclusion, I ask that you apply the unique resources of the NSTAC to undertake this effort aimed at understanding the dimensions of this problem and identifying cost-effective measures that industry and government can take to prevent, or in the worst case to restore services after, a widespread outage. I know that this effort will not be completed on my watch, but this will be a key component in building the understanding of this issue for my successor and the next President, and for crafting wise and effective policy. My point of contact for this effort will be Dr. Terry Kelly (202-456-6057).

Sincerely,

Neal Lane

Neal Lane
Assistant to the President
for Science and Technology

Kelly -
mailed 11/28/00
(dist. list
attached)

THE WHITE HOUSE

WASHINGTON
November 27, 2000

MEMORANDUM FOR ARTHUR MONEY, ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS & INTELLIGENCE

GREGORY RHODE, ASSISTANT SECRETARY, COMMUNICATIONS AND INFORMATION

FERNANDO BURBANO, CHIEF INFORMATION OFFICER, DEPARTMENT OF STATE

MICHAEL POWELL, DEFENSE COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION

CLAY HOLLISTER, ASSOCIATE DIRECTOR, INFORMATION TECHNOLOGY, FEMA

DENNIS FISCHER, COMMISSIONER, FEDERAL TECHNOLOGY SERVICE

LIEUTENANT GENERAL HARRY D. RADEUGE, JR., MANAGER, NATIONAL COMMUNICATIONS SYSTEM

SUBJECT: JTRB Viability through the Administration Transition Period

As the Clinton Administration draws to an end, I want to thank you for your service to the nation and to the President as members of the Joint Telecommunications Resources Board (JTRB). Your willingness to serve and, in particular, the expertise you provided through the Y2K preparation period were important.

There is, however, one more task I must ask you to perform before this Administration ends. We must ensure that the JTRB can come together should a crisis occur during the transition to a new Administration. Therefore, if your tenure in office will be ending, please ensure that a knowledgeable representative from your agency who will remain through the transition period is identified and available to fulfill your JTRB duties until a new Principal is selected and, if applicable, confirmed by the Senate.

Please forward a copy of the document naming your agency's representative, and his or her contact information, to Dr. Terry Kelly on my staff. He can be reached at 202-456-6057.

Neal Lane

Neal Lane
Assistant to the President
for Science and Technology

ADDRESSES OF JTRB MEMBERS
(Updated 11/29/00)

ART MONEY
ASD/C3I
Pentagon, Room 3E172
Washington, DC 20301-6000
POC: Petty Officer Craig Donovan, USN
E-mail: craig.donovan@osd.pentagon.mil
Phone: (703) 695-0348
Fax: (703) 614-8060

DENNIS FISCHER
Commissioner, Federal Technology Service
General Services Administration
10304 Eaton Place, Suite 3-1005
Fairfax, VA 22030
POC: Mary Ann (e-mail: maryanne.green@gsa.gov)
Phone: (703) 306-6020
Fax: (703) 306-6029

GREGORY L. ROHDE
Assistant Secretary, Communications and Information
Department of Commerce
14th & Constitution Avenue, NW
Room 4898
Washington, DC 20230
POC: Sheila Williams (e-mail: swilliams@ntia.doc.gov)
Phone: (202) 482-1840
Fax: (202) 482-1635

MICHAEL POWELL
Defense Commissioner
Federal Communications Commission
1919 M Street, NW
Room 844
Washington, DC 20554
POC: Toni (e-mail: tmcgowan@fcc.gov)
Phone: (202) 418-2200
Fax: (202) 418-2820

CLAY HOLLISTER
Associate Director, Information Technology
FEMA
500 C Street, SW
Room 238
Washington, DC 20472
POC: Angie
Phone: (202) 646-3006
Fax: (202) 646-4655

LTG HARRY D. RADEUGE, JR.,USA
Manager
National Communications System
701 S. Court House Road
Room 4345
Arlington, VA 22204-2199
POC: Priscilla McMahon
Phone: (703) 607-6001
Fax: (703) 607-4082

FERNANDO BURBANO
Chief Information Officer
Department of State
2201 C Street, NW
Room 6313
Washington, DC 20520
POC: Eloise
Phone: (202) 647-2226
Fax: (202) 647-2294

EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

WASHINGTON, D.C. 20502

CONFERENCE ON "FUTURE DIRECTIONS IN NATIONAL SECURITY SCIENCE AND TECHNOLOGY"

DATE: WEDNESDAY, NOVEMBER 15, 2000
TIME: 8:30 AM-5:30 PM
LOCATION: RAND, 1200 SOUTH HAYES STREET, ARLINGTON

From: Gerald Epstein

I. Objectives

You are hosting a first-of-its kind conference in which 11 national security agencies will give an overview of their major science and technology issues over the next decade. The objectives of the conference are to provide an opportunity for the attendees to view and to discuss these plans with the benefit of the experience of the past 8 years and to create a document that may be of assistance to the agencies involved and to the new Administration. You are slated to make 5 minutes of introductory remarks, and to participate in the discussions as you wish. Assuming you agree, I will announce the speakers and facilitate the discussions following their presentations.

II. Background

Attached at Tab A is the conference agenda. Five military/defense agencies, three intelligence agencies, and three other national security agencies (State, DOE, NASA) will be making presentations, each lasting 20 minutes with 10 minutes following for discussion. The presentations will be followed by three, 30-minute, moderated discussions on R&D issues for weapons, for sensors, and for supporting technologies (such as space launch and information technology). We have received read ahead material from most of the speakers should you care to see it. You also invited a number of additional agencies to send participants to join in the discussion and to contribute written material for the conference proceedings. There has been good reception by the agencies, and at last count some 90 individuals were planning to come. Attached at Tab B is a list of attendees as of a few days ago. At the conclusion of the conference, there will be a reception (with a cash bar). People will be asked to contribute toward the lunch and coffee breaks. The RAND Science and Technology Policy Institute is providing logistical support for the conference, and RAND's Bruce Don will open the conference by welcoming people to the facility, giving logistical information, and calling on you for introductory remarks. I suggest that you then call on me to introduce the first speaker. Suggested talking points for your introductory remarks are at Tab C. For reference, your initial letter is at Tab D, and a map to the RAND facility is at Tab E.

Tab A	Conference Agenda
Tab B	List of Attendees
Tab C	Suggested Talking Points
Tab D	Initial Letter to Participants
Tab E	Map to RAND

Future Directions in National Security Science & Technology
November 15, 2000

UPDATED AGENDA

8:30 a.m.	Introduction by Dr. Neal Lane
8:45 a.m.	OUSD Presentation: Dr. Delores Etter
9:15 a.m.	Army Presentation: Dr. A. Michael Andrews
9:45 a.m.	Navy Presentation: RADM Jay Cohen
10:15 a.m.	Break
10:30 a.m.	Air Force Presentation: Dr. Donald C. Daniel
11:00 a.m.	DARPA Presentation: Dr. Frank Fernandez
11:30 a.m.	NRO Presentation: Carol Staubach
12:00 p.m.	CIA Presentation: Dr. John Phillips
12:30 p.m.	NSA Presentation: Dr. Nancy Welker
1:00 p.m.	Lunch
1:30 p.m.	State Department Presentation: Dr. O.J. Sheaks & Ambassador Stapleton Roy
2:00 p.m.	NASA Presentation: Samuel Venneri
2:30 p.m.	DOE Presentation: Dr. David Crandall
3:00 p.m.	Break
3:15 p.m.	Discussion 1: Weapons Technologies, moderator TBD
3:45 p.m.	Discussion 2: Sensor Technologies, moderator TBD
4:15 p.m.	Discussion 3: Supporting and Enabling Technologies, Dr. Vic Utgoff, IDA, moderator
4:45 p.m.	Reception

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. list	Conference attendees [National Security Act; 10 USC 424] (3 pages)	11/15/2000	P3/b(3), b(6)

COLLECTION:
Clinton Presidential Records
Office of Science and Technology Policy

OA/Box Number: 43311

FOLDER TITLE:
Director Actions [1]

2008-1524-F
kc1213

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Suggested Talking Points

- It is a pleasure to welcome everyone to this conference on "Future Directions in National Security Science and Technology."

- A conference with such an ambitious title could--and maybe will--cover just about anything, given how our national security depends on our scientific and technological strength across the board.

- Moreover, to fully do this topic justice, the program would have to be quite long, considering the diversity of agencies and constituencies that we now recognize to be part of the broader national security community.

- All of us, I think, recognize that our national security requires that we take maximum advantage of science and technology developed in the commercial sector, in academia, and overseas--outside what has traditionally been thought of as the U.S. national security community.

- On the other hand, I also believe that our national security will continue to depend on a core set of technical competencies that we cannot assume will be developed by others. In these areas, our military, intelligence, and other security agencies will need to maintain robust, dedicated science and technology efforts of their own.

- It is these that I would like to concentrate on today. I have asked some of the "core" national security agencies to discuss with us the key S&T issues they face.

- Even so, this is not a discussion that these agencies can or should have solely among themselves, so I have invited those of you from the broader community to participate as well.

- We believe that the conference should prove useful to all of you, to your agencies, and to the new Administration.

November 14, 2000

- We hope that it will serve to uncover areas in which one agency might make use of R&D done by another and areas in which agencies might cooperate in some way.

- We will be making a (Secret-level) volume with the presentations and a summary of the discussion as well as of any comments or other material people would like to submit following the event.

- {**FYI**: *Should Bruce Don not make the following remark, you might do so.* We think a lot of the conference value will be in having frank discussions. If you wish to say something that you believe should not be included in the Proceedings volume, just make that clear when you make your remark.}

- Finally, I should remark on the timing of this conference. When we first started discussing it, some of us at OSTP thought we should wait to hold it until after the election, to avoid any perception that there might be some sort of a political agenda. Others, however, suggested it might be better to hold it before we knew who won, to eliminate any perception that the conference were somehow tailored to suit the views of the winning candidate. We never dreamed we could have it both ways.

- I look forward to what I will find a fascinating day, and thank you all for participating.

- At this time I'd like to ask Jerry Epstein, my Assistant Director for National Security, to introduce our first speaker.

D

LETTER THAT WENT TO ALL AGENCIES INVITED TO MAKE PRESENTATIONS

THE WHITE HOUSE
WASHINGTON

The Honorable Frank Fernandez
Director, Defense Advanced Research Projects Agency
3701 North Fairfax Drive, Room 983
Arlington, Virginia 22203-1714

Dear Mr. Fernandez:

I am writing to invite you to participate in a one-day governmental conference on "Future Directions in National Security Science and Technology." The conference will be held on November 15, 2000, in the RAND Main Conference Room, 1200 South Hayes Street, Arlington, Virginia. Its purpose is to provide an opportunity for national security community agency directors and their most senior technical people to exchange and to compare views on R&D challenges and opportunities.

We seek a 20-minute (Secret) presentation from each agency on its most important likely science and technology directions, looking perhaps a decade into the future. We are most interested in science and technology that cannot be drawn from the commercial technology base. We would like a written (up to Secret-level) document, which can go beyond the presentation, to distribute in advance. The product of the conference will be a report summarizing and elaborating on the topics discussed.

Our intent is *not* to supplant any interagency or budgetary process. Our goal is to assemble, to discuss, and to record a collective, educated guess as to the major directions for national security R&D over the next decade–for the benefit of conference participants, their agencies, and the new Administration. Enclosed is a preliminary agenda and list of presenting agencies.

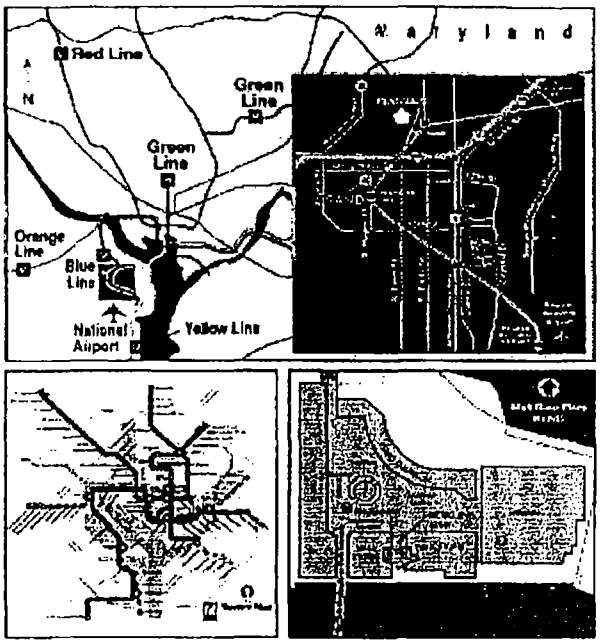
To permit a manageable colloquy, we would like two participants from each agency–the agency head and the chief scientific or technical officer, if at all possible–plus up to six interested listeners from each agency. We are also inviting officials from a few other agencies, NSC, and OMB to observe. We would like to hear, at your earliest convenience, who will attend for your agency. Our point of contact is Vic Teplitz at (202) 456-6058. We would welcome suggestions on maximizing the utility of the conference and product.

Sincerely,

Neal Lane
Assistant to the President
for Science and Technology

Enclosure

RAND
Washington Office
1200 South Hayes Street
Arlington, Virginia 22202-5050
Phone: 703-413-1100 Fax: 703-413-8111



Click on images for larger versions

Location in the Region

RAND's Washington Office is located just off Interstate 395, near both the Pentagon and National Airport.

Driving Access

The building fronts on South Hayes Street in Arlington and is colocated with the Fashion Centre at Pentagon City. To get there,

- **Driving south on I-395**--Cross the 14th Street bridge to Virginia. Get in the left lane and take Exit 9B-15th Street South/Pentagon City.
- **Driving north on I-395**--Take Exit 8C-Route 1 South/Pentagon City.
- **Driving south on the George Washington Parkway**----Follow the National Airport signs. Stay left until the Route 1 South sign, and exit right onto I-395 South to Exit 9B-15th Street South/Pentagon City.
- **Driving north on the George Washington Parkway**--Take the Richmond/I-395 South exit. Get in the left lane and take Exit 9B-15th Street South/Pentagon City.
- **Driving south on Route 1**--Exit at 15th Street South/Pentagon City. Turn right.
- **Driving north on Route 1**--Exit at 15th Street South/Pentagon City. Turn left.
- **Driving east on I-66, toward D.C.**--Take Exit 75-Route 110 Pentagon City. Follow the Route 1 South signs and pass the Pentagon Building to the Pentagon City exit.
- **From the Woodrow Wilson Bridge**--Take Route 1 North, through Alexandria, until you reach Crystal City. Exit at 15th Street and turn left.

Parking is available in the parking structure of the Fashion Centre at Pentagon City and can be entered from either Army-Navy Drive or 15th Street.

As of May 1, 2000, the fees are as follows:
Monday-Friday

White House Office of Science & Technology Policy's Conference On Future Directions in National Security Science & Technology

November 15, 2000

FINAL AGENDA

8:30 a.m.	Welcoming Remarks Dr. Bruce Don, Director Science and Technology Policy Institute at RAND
8:35 a.m.	Introduction Dr. Neal Lane, Assistant to the President for Science and and Technology, Director, Office of Science and Technology Policy
8:45 a.m.	OUSD Presentation: Dr. Delores Etter, Deputy Under Secretary of Defense for Science and Technology (DDR&E)
9:15 a.m.	Army Presentation: Dr. A. Michael Andrews, Deputy Assistant Secretary/Chief Scientist (SAAL-ZT)
9:45 a.m.	Air Force Presentation: Dr. Donald C. Daniel, Deputy Assistant Secretary, Science & Technology (SAF/AQR)
10:15 a.m.	Break
10:30 a.m.	Navy Presentation: Rear Admiral Jay Cohen, Chief of Naval Research
11:00 a.m.	DARPA Presentation (Classified): Dr. Frank Fernandez, Director
11:30 a.m.	NRO Presentation (Classified): Ms. Carol Staubach, Director, Advanced Systems and Technology Directorate
12:00 p.m.	CIA Presentation (Classified): Dr. John Phillips, Chief Scientist

12:30 p.m. NSA Presentation:
Dr. Nancy Welker, Associate Deputy Director for Technology for Advanced Programs

1:00 p.m. Lunch

1:30 p.m. State Department Presentation:
Dr. O. James Sheaks, Assistant Secretary Verification & Compliance
Ambassador J. Stapleton Roy, Assistant Secretary Intelligence & Research Bureau

2:00 p.m. NASA Presentation:
Mr. Samuel Venneri, Associate Administrator Aerospace Technology

2:30 p.m. DOE Presentation:
Dr. Maureen McCarthy, Chief Scientist, National Nuclear Security Administration and Senior Advisor to the Secretary of Energy for National Security and Nuclear Energy

3:00 p.m. Break

3:15 p.m. Discussion 1: Weapons Technologies
Dr. Mark Lewellyn, Vice President for Advanced Technology and Systems Analysis Division, Center for Navy Analyses

3:45 p.m. Discussion 2: Sensor Technologies
Dr. Peter Bythrow, Chief Scientist, Central MASINT Office

4:15 p.m. Discussion 3: Supporting and Enabling Technologies
Dr. Vic Utgoff, Deputy Director, Strategy Forces and Resources Division, Institute for Defense Analyses

4:45 p.m. Reception

Kelly

6660

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

October 24, 2000

ACTION

MEMORANDUM FOR SAMUEL R. BERGER

FROM: JEFFREY HUNKER

SUBJECT: Convergence of Internet and Telecommunications Systems

Currently, the Internet operates over a 'packet data' network, while voice calls are carried over a largely separate 'public switched network (PSN).' However, industry and government experts predict that these two largely distinct networks will merge sometimes in the 2003-2005 period, and evolve into a next generation network (NGN) combining voice and data. This convergence may have significant implications for ensuring National Security/Emergency Preparedness (NS/EP) communications.

Executive Order 12472 gives oversight of NS/EP communications primarily to NSC and OSTP, with a smaller role for OMB. All three offices have met and agreed that the impending convergence of voice and data networks makes it important to examine the implications of this convergence for NS/EP communications.

The attached memo will create a Convergence Task Force to identify the policy, legal, technical, and security issues of convergence on the ability of the government to assure NS/EP communications for the President, and a process for resolving these issues. It directs that a report be made to you and the Assistant to the President for Science and Technology by January 1 of next year.

RECOMMENDATION

That you sign the attached memorandum.

Attachment
Tab I Berger/Lane Memorandum on NS/EP

THE WHITE HOUSE

WASHINGTON

MEMORANDUM FOR THE SECRETARY OF DEFENSE
THE SECRETARY OF COMMERCE
DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
ADMINISTRATOR, GENERAL SERVICES ADMINISTRATION

SUBJECT: National Security and Emergency Preparedness (NS/EP) Communications under Convergence of the Voice and Data Networks

Executive Order 12472 gives oversight of National Security/Emergency Preparedness (NS/EP) communications to the NSC, OSTP and OMB. The impending convergence of the voice and data networks makes it important to examine the implications of this convergence for NS/EP communications.

Industry and government experts predict that the Internet and Public Switching Network (PSN) networks - now largely distinct - will merge sometime in the 2003-2005 period, and evolve into a next generation network (NGN) combining voice and data. This convergence may have significant implications for ensuring NS/EP communications under all circumstances.

The President's National Security Telecommunications Advisory Committee (NSTAC) highlighted the impact of the convergence of the voice and data networks on National Security and Emergency Preparedness (NS/EP) Communications in their May 2000 report, *Information Technology Progress Impact Task Force Report on Convergence*. The report notes that under the existing systems, the Public Switching Network (PSN) gives priority to NS/EP Communications, and prioritizes service restoration should the network fail. The report further notes that these capabilities are technology dependent and will not transition from the PSN to the NGN without modification. The NSTAC explicitly recommends that the President "promptly determine precise functional NS/EP requirements for Convergence and the NGN."

The NSC and OSTP, in consultation with OMB, will convene a Convergence Task Force (CTF) to identify the policy, legal, technical, and security issues of convergence on ability of the government to assure NS/EP communications for the President, and a process for resolving them. The CTF will consider the

following in their efforts, and will issue a report to the Assistant to the President for National Security Affairs and the Assistant to the President for Science and Technology by January 1, 2001 that lays out the critical issues in these four areas, and recommends a process for resolving them.

- Determine the "precise functional NS/EP requirements for Convergence and the NGN," and any other pertinent concerns in these four areas necessary to ensure that the President and the National Leadership have uninterrupted access to NS/EP communications in times of crisis.
- Examine what types of communication should fall under the rubric of NS/EP communications.
- Consult, to the extent necessary and allowable by law, with the NSTAC and other private sector bodies as the CTF deems necessary or desirable.

The NSC and OSTP will contact your office to arrange for appropriate representation from your agency on the CTF. The initial meeting will be chaired by the NSC (Dr. Jeffrey Hunker) and OSTP (Dr. Gerald Epstein).

Please contact Dr. Terry Kelly, OSTP Senior National Security Officer (202-456-6057), or Dr. Jeffrey Hunker, NSC Senior Director for Critical Infrastructure (202-456-9351), if you wish to discuss this prior to the meeting.

Samuel Berger
Assistant to the President
for National Security Affairs

Neal Lane
Assistant to the President
and Director, Office of
Science and Technology

cc:
Assistant Secretary of Defense, C3I
Commissioner, Federal Technology Services
Assistant Secretary of Commerce, Communications and Information
Defense Commissioner, FCC
Associate Director (FEMA), Information Technology
Manager, NCS

OSTP CONCURRENCE SHEET

Date Routed: 10-24-00

Comments: Tony Kelly has reviewed & recommends you sign the attached memo.

CLEARED BY OMB? N/A ☐ YES ☐ NO ☐ PENDING ☐

CLEARED BY OTHER EOP OFFICE(S)? N/A ☐ YES ☐ NO ☐ PENDING ☐
(specify) _____

DRAFT PACKAGE				FINAL PACKAGE			
Route to (√)		Initial	Date		Initial	Date	Route to (√)
X	Author's Name			Author's Name NSC - Jeff Hunker			
	Administrative Assistant			Administrative Assistant Pat Thiel	fw	10/24	✓
	Assistant Director			Assistant Director Gerald Epstein →	T. Kelly has reviewed on Travel		
	Arthur Bienenstock Associate Director for SCI			Arthur Bienenstock Associate Director for SCI			
	Duncan Moore Associate Director for TECH			Duncan Moore Associate Director for TECH			
	Rosina Bierbaum Associate Director for ENV			Rosina Bierbaum Associate Director for ENV			
	Exec Secretary, NSTC/PCAST			Exec Secretary, NSTC/PCAST			
	Barbara Ferguson Asst Dir, Budget & Admin			Barbara Ferguson Asst Dir, Budget & Admin			
	Jeff Smith Executive Assistant			Jeff Smith Executive Assistant			
	Holly Gwin Chief of Staff/General Counsel			Holly Gwin Chief of Staff/General Counsel	HG	10/24	✓
	Betty Fountain Special Assistant			Betty Fountain Special Assistant	bf	10/24	✓
	Neal Lane Director			Neal Lane Director	NL	10/25	✓

Attach all enclosures and incoming correspondence to draft and final packages.

Attach envelopes only to the final package.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

October 24, 2000

ACTION

MEMORANDUM FOR SAMUEL R. BERGER

FROM: JEFFREY HUNKER

SUBJECT: Convergence of Internet and Telecommunications Systems

Currently, the Internet operates over a 'packet data' network, while voice calls are carried over a largely separate 'public switched network (PSN).' However, industry and government experts predict that these two largely distinct networks will merge sometimes in the 2003-2005 period, and evolve into a next generation network (NGN) combining voice and data. This convergence may have significant implications for ensuring National Security/Emergency Preparedness (NS/EP) communications.

Executive Order 12472 gives oversight of NS/EP communications primarily to NSC and OSTP, with a smaller role for OMB. All three offices have met and agreed that the impending convergence of voice and data networks makes it important to examine the implications of this convergence for NS/EP communications.

The attached memo will create a Convergence Task Force to identify the policy, legal, technical, and security issues of convergence on the ability of the government to assure NS/EP communications for the President, and a process for resolving these issues. It directs that a report be made to you and the Assistant to the President for Science and Technology by January 1 of next year.

RECOMMENDATION

That you sign the attached memorandum.

Attachment
Tab I Berger/Lane Memorandum on NS/EP

THE WHITE HOUSE

WASHINGTON

MEMORANDUM FOR THE SECRETARY OF DEFENSE
THE SECRETARY OF COMMERCE
DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
ADMINISTRATOR, GENERAL SERVICES ADMINISTRATION

SUBJECT: National Security and Emergency Preparedness (NS/EP) Communications under Convergence of the Voice and Data Networks

Executive Order 12472 gives oversight of National Security/Emergency Preparedness (NS/EP) communications to the NSC, OSTP and OMB. The impending convergence of the voice and data networks makes it important to examine the implications of this convergence for NS/EP communications.

Industry and government experts predict that the Internet and Public Switching Network (PSN) networks - now largely distinct - will merge sometime in the 2003-2005 period, and evolve into a next generation network (NGN) combining voice and data. This convergence may have significant implications for ensuring NS/EP communications under all circumstances.

The President's National Security Telecommunications Advisory Committee (NSTAC) highlighted the impact of the convergence of the voice and data networks on National Security and Emergency Preparedness (NS/EP) Communications in their May 2000 report, *Information Technology Progress Impact Task Force Report on Convergence*. The report notes that under the existing systems, the Public Switching Network (PSN) gives priority to NS/EP Communications, and prioritizes service restoration should the network fail. The report further notes that these capabilities are technology dependent and will not transition from the PSN to the NGN without modification. The NSTAC explicitly recommends that the President "promptly determine precise functional NS/EP requirements for Convergence and the NGN."

The NSC and OSTP, in consultation with OMB, will convene a Convergence Task Force (CTF) to identify the policy, legal, technical, and security issues of convergence on ability of the government to assure NS/EP communications for the President, and a process for resolving them. The CTF will consider the

following in their efforts, and will issue a report to the Assistant to the President for National Security Affairs and the Assistant to the President for Science and Technology by January 1, 2001 that lays out the critical issues in these four areas, and recommends a process for resolving them.

- Determine the "precise functional NS/EP requirements for Convergence and the NGN," and any other pertinent concerns in these four areas necessary to ensure that the President and the National Leadership have uninterrupted access to NS/EP communications in times of crisis.
- Examine what types of communication should fall under the rubric of NS/EP communications.
- Consult, to the extent necessary and allowable by law, with the NSTAC and other private sector bodies as the CTF deems necessary or desirable.

The NSC and OSTP will contact your office to arrange for appropriate representation from your agency on the CTF. The initial meeting will be chaired by the NSC (Dr. Jeffrey Hunker) and OSTP (Dr. Gerald Epstein).

Please contact Dr. Terry Kelly, OSTP Senior National Security Officer (202-456-6057), or Dr. Jeffrey Hunker, NSC Senior Director for Critical Infrastructure (202-456-9351), if you wish to discuss this prior to the meeting.

Samuel Berger
Assistant to the President
for National Security Affairs

Neal Lane
Assistant to the President
and Director, Office of
Science and Technology

cc:
Assistant Secretary of Defense, C3I
Commissioner, Federal Technology Services
Assistant Secretary of Commerce, Communications and Information
Defense Commissioner, FCC
Associate Director (FEMA), Information Technology
Manager, NCS

THE WHITE HOUSE

WASHINGTON

October 18, 2000

MEMORANDUM FOR THE HONORABLE ARTHUR L. MONEY
ASSISTANT SECRETARY OF DEFENSE FOR
COMMAND, CONTROL, COMMUNICATIONS &
INTELLIGENCE

LIEUTENANT GENERAL HARRY D. RADUEGE, JR.
MANAGER, NATIONAL COMMUNICATIONS SYSTEM

SUBJECT: Continuation of the Alert and Coordination Network

Thank you for your quick response to my letter of August 17, 2000, on the Alert and Coordination Network. I think your recommendation is exactly on target – the NCS is the logical place for this capability to reside and it would fit best as a component of the National Telecommunications Coordination Network. The NCS, through the NCC, alone has both the technical ability and contacts with the telecommunications industry to make this work. I appreciate your willingness to take on this additional operational and financial responsibility.

Neal Lane
Assistant to the President
for Science and Technology

NATIONAL COMMUNICATIONS SYSTEM
OFFICE OF THE MANAGER
701 SOUTH COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2198

IN REPLY REFER TO: Operations Division (N3)

OCT 9 2000

MEMORANDUM FOR ASSISTANT TO THE PRESIDENT FOR SCIENCE AND TECHNOLOGY

THROUGH: Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

SUBJECT: Continuation of the Alert and Coordination Network (ACN)

1. In response to your August 17, 2000, memorandum regarding the impact of the loss of the National Telecommunications Alliance (NTA) ACN, I share your concerns and requested the Manager of the National Coordinating Center for Telecommunications (NCC) research the matter and propose a course of action. After checking with NTA and NCC member companies, we have verified that none of the current membership wishes to be responsible for the day-to-day maintenance, but all are in favor of continuing to participate in the ACN. Additionally, all current participants support the NCC administering the day-to-day operation of the ACN.

2. Although several options for ensuring the continuation of the ACN functionality were considered, recommend that we incorporate the ACN into the National Communications System's National Telecommunications Coordination Network (NTCN) and conduct the day-to-day management oversight at the NCC. This option is operationally preferable since it would continue the existing capability, and incorporate the management of the ACN and NTCN into a single entity. The NCC would administer both operations with in-house staffing and limited contracted support. The OMNCS is in the process of identifying the necessary funding and contract vehicles to operate the system. With your concurrence, we would assume the maintenance of the ACN starting January 1, 2001.

HARRY D. RADUEGE, JR.
Lieutenant General, USAF
Manager

Epstein ✓
Kelly

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

MEETING WITH UNIVERSITY PRESIDENTS

Date:	October 19, 2000
Time:	1:30 PM– 2:10 PM
Location:	Room 303 OEOB
From:	Gerald Epstein

1. Purpose: The purpose of this visit is for the NSC to encourage the universities (participants at Tab C) to better organize themselves to be strong advocates for Information Security/Information Assurance education. NSC will use this opportunity to update them on the status of national cyber educational initiatives (i.e., Scholarship for Service – SFS – and the Institute), and provide an opportunity for discussion with government agencies on current IA education issues.

2. Background: On Thursday, October 19, from 1:30 – 4:00 PM, the NSC (Richard Clarke) will host the Presidents of the eleven Universities recognized by NSA as Centers of Excellence in Information Assurance Education will meet in the OEOB, Room 552. NSC has asked you to speak for 10 minutes, and answer questions for 10 additional minutes from 1:50 PM – 2:10 PM. (See Talking Points at Tab A, and Agenda at Tab B.)

   The Centers of Excellence in Information Assurance Education program is an innovative NSA attempt to recognize and encourage programs in this new and important field (Tab D contains information on this program). You may recall that the first seven universities to enter the program were recognized at the Colloquium for Information Systems Security Education, which you addressed on May 25, 2000.

   One item of particular interest to the University Presidents is the study NSIA started during the Summer of 2000, to look at solutions to the problem of an insufficient number of Information Assurance researchers and programs at our academic institutions. This project is ongoing, but we can now say that we have collected a significant quantity of constructive input from academia, industry, government, and nontraditional sources such as the white-hat hacker community. Under my current plan, these results will be available before the end of the calendar year as a compendium of input and ideas, but not as concrete policy recommendations. They are meant to motivate creative thought into ways to solve the problem, not to prescribe solutions.

Attachments:

Tab A	Talking Points
Tab B	Agenda for October 19, 2000
Tab C	Attendance List
Tab D	Background on the Centers of Academic Excellence in Information Assurance Education Program
Tab E	Executive Summary of NSIA's Academic Researcher Study

A

Talking Points / Q's and A's
University Presidents Event
Thursday, October 19, 2000
1:30-2:10 PM

- Thank you for coming together to discuss this important topic. As Dick just indicated, our educational systems plays a vitally important role in generating the information security workforce we will need in the coming years.

- In addition to making sure that the nation has a sufficient supply of information security practitioners, I am also keenly interested in making sure that we will be able to produce the next generation of information security researchers. In fact, since we last met at the colloquium in May, Jerry Epstein's office has been in touch with many of your faculty to ask for their ideas on how to solve this problem.

- We at OSTP think this is a very important issue. However, since it will be the next Administration that submits the Fiscal Year 2002 budget request to Congress, we will not be able to translate this into a budget initiative. However, we will be working hard to make sure that this issue is at the top of the next OSTP's and Administration's agenda.

- We need to make sure that the nation will have the people who can do this research.

- You on the front lines know far better than I do the challenges we face in maintaining the academic pipeline of graduate students and faculty in the face of industry's voracious appetite for personnel.

- Our national science and technology policy has long recognized that sponsoring research in our colleges and universities earns double dividends – we not only generate the science and technology that we need, but we also train the graduate students and support the faculty members on whom we rely to educate our technical workforce. *[FYI: Should be careful not to imply to this audience – which will likely include four-year colleges -- that only research universities are responsible for educating the workforce]*

- Therefore, if we have a sufficiently challenging -- and sufficiently well-supported – university research agenda in information security, we will not only build the science and technology base that we need to protect our critical infrastructures, but we will also help attract, retain, and maintain the skills of the graduate students and faculty members who might otherwise be lured out of academia and into industry.

- At OSTP, we have the mission of coordinating the Federal Government's R&D effort in critical infrastructure protection. The President's FY2001

budget request contains over $600 million of R&D in critical infrastructure protection (CIP), constituting about a third of the total $2 billion CIP request.

- A particularly important component of the President's FY2001 budget request is his request to establish an Institute for Information Infrastructure Protection to support key research and technology development projects that would not otherwise be done by the private sector or the government. However, right now key pieces of this coordinated legislative proposal are in jeopardy, to include the Institute.

- Whenever the Institute is established – be it this fiscal year or in FY 2002 – one of its objectives should be to support a significant component of its research in multi-year programs at academic institutions. Doing so would provide opportunities for graduate student support and a sufficiently stable research environment to justify and support faculty hiring.

- One area I would like to highlight which I am sure is important to you and will undoubtedly influence the research agenda for the Institute is the growing convergence of the traditionally "applied" research field of information security and the traditionally "basic" research in information technology. At OSTP, we are significantly involved in both of these areas, and we are starting to see a significant overlap as the need for information security that is an integral part of information SYSTEMS becomes increasingly evident. I expect to see a greater interaction, both in the government and in the research community, between these communities.

- I hope the next time we meet, or when you meet with my successor, we will be able to provide you a briefing on the Institute's first year's progress.

Q: Will your Academic Researcher Study provide any policy recommendations?

A: Right now we are limiting it to idea generation. I want to get the full scope of the ideas from the field out for consideration. We will certainly have to address this issue with government policy and programs, but that is the next step.

Q: Your Academic Researcher Study includes recommendations that NSF be restructured to better serve the needs of the Information Assurance/Critical Infrastructure Assurance research needs. When do you anticipate this happening?

A: Right now no such reorganization is being considered. This study in its current state contains many great ideas from the field, but no policy

proposals. The next step must be to work with Dick's staff and the incoming Administration to decide what contained in this document is wise, and work towards its adoption. We are not yet there.

Q: What kind of reaction are you getting from the Hill on the Institute?

A: It is reasonable to expect that when the Administration proposes to do something new, the burden of proof will be on us to make the case for it. We are working hard to make sure that the Institute will be able to work effectively with academia and industry. There have been some discussions about the Institute on the Hill, but we did not get the proposal to the Hill early enough in the congressional cycle. We will continue to discuss it with the relevant Congressional committees, and we hope they will see the light and fund it this year. If not, I anticipate that whoever wins the election in November, their new Administration will try again next year. This idea is just that important.

Q: How about the provision in the Defense Authorization bill to create an Institute for Defense Computer Security and Information Protection?

A: We entirely support the intent of this provision. However, we have some questions about whether an Institute housed in DoD will be able to establish the kind of partnership with industry that is essential to solving this problem, given that a great many of the relevant firms have no experience, and possibly little interest, in dealing with the Department of Defense. The problem is a national one, not one of defense alone. We have discussed this issue with the Department of Defense, and are working on solutions.

Q: Some in the National Security Community have voiced concerns about foreign nationals doing research in sensitive technologies at Universities in the US. Some consider information assurance and IT to be such sensitive technologies. Are we going to see attempts to restrict the research that we are allowed to pursue if we have foreign nationals in our programs (which we all do)?

A: No. I strongly believe that research and education in our colleges and universities must be open to all, and that we need also to continue collaborative efforts with our colleagues overseas. Understand, however, that job and scholarship opportunities in the government and other selected sectors may be limited for foreign nationals enrolled in or graduating from your universities – for example the Scholarship for Service program is open to US citizens only. Although it is a mark of

strength that the United States continues to attract scholars from around the world, I do think we need to improve our efforts to attract U.S. citizens into science and technology in general, and to information security in particular.

Agenda

1330-1350	Richard A. Clarke, National Coordinator for Security, Infrastructure Protection and Counter-terrorism, National Security Council
1350-1410	Dr. Neal Lane, Director, Office of Science and Technology Policy
1410-1430	TBD, National Science Foundation
1430 – 1500	Carol Oaken, Director of Employment Services, Office of Personnel Management
1500-1600	Discussion

Discussion Points

1. The need for strong advocacy and involvement by higher education
2. Responsibility for fulfilling workforce requirements
3. How to engage underrepresented institutions in cyber education
4. Faculty development: Recruitment and capacity building
5. Federal Cyber Service Experiences: Developing strong ties to IA community through workshops and summer training opportunities

[redacted]

C

List of Participants

NSC Meeting with University Presidents

Carnegie Mellon University:

Dr. Jeffrey Edward Thieret, Program Manager, CMU Institute for Survivable Systems (CISS)

Dr. Barbara Laswell, Technical Manager, Training, Practices & Development

Florida State University:

Dr. Anne Rowe, Associate Dean, College of Arts & Sciences

Dr. Yvo G. Desmedt, Professor of Computer Science, and Director, Security and Assurance in Information Technology Lab (SAIT)

George Mason University:

Dr. Alan Merten, President

Dr. Lloyd Griffiths, Dean, School for Information Technology and Engineering

Dr. Sushil Jajodia, Director, Secure Information Systems

Idaho State University:

Dr. David Wendt, Special Assistant to the President

Dr. Corey Schou, Professor and Associate Dean, College of Business and Director, Center for Decision Support and the SIMPLOT Decision Support Center

Iowa State University:

Dr. Howard Neal Shapiro, Vice Provost for Undergrad Programs and Professor for Mechanical Engineering

Dr. James Davis, Associate Professor, Electrical and Computer Engineering, and Co-Director of the Information Systems Security Laboratory

Information Resources Management College of National Defense University:

AMB Robin Lynn Raphel, Vice President, National Defense University

Dr. Donita McGeary, Associate Dean of Faculty and Academic Programs

Dr. John Michel, Professor, Systems Management

James Madison University:

Dr. Linwood Howard Rose, President

Dr. Malcolm Graham Lane, Department Chair and Professor, Computer Science

Naval Postgraduate School:

Dr. Daniel C. Boger, Dean, Computer and Information Sciences and Operations

Dr. Cynthia Irvine, Director, NPS Center for INFOSEC Studies and Research

CAPT James Stilson Newman, USN

Purdue University:

Dr. Edward Coyle, Assistant Vice President for Communications & Computing, Purdue Research Foundation

Dr. Eugene H. Spafford, Professor and Director of CERIAS

University of California at Davis:

Dr. Karl Levitt, Professor, Department of Computer Science

University of Idaho:

Dr. Robert A. Hoover, President

Dr. Deborah Ann Frincke, Associate Professor, Computer Science

University of Illinois at Urbana-Champaign:

Dr. Roy Campbell, Professor of Computer Science

University of Tulsa:

Dr. Robert William Lawless, President

Dr. John Chandler Hale, Associate Professor of Computer Science

Dr. Sujeet Shenoi, Professor of Computer Science

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: ISSO-080-99
7 October 1999

Subject: Centers of Academic Excellence in Information Assurance Education
2nd Annual Call for Applications

Dear Colleagues:

The National Security Agency announced the establishment of a program to recognize Centers of Academic Excellence in Information Assurance Education in November 1998. The program is intended to reduce vulnerabilities in the National Information Infrastructure by promoting higher education in information assurance and producing a growing number of professionals with information assurance expertise in various disciplines. The program was developed in the spirit of Presidential Decision Directive 63, Policy on Critical Infrastructure Protection, May 1998, which reflects an important role for the academic community in securing our Nation's critical information infrastructure.

As a result of the first program offering, seven universities were designated as Centers of Academic Excellence in Information Assurance Education. The distinguished universities are: George Mason University, Idaho State University, Iowa State University, James Madison University, Purdue University, University of California at Davis, and University of Idaho. I had the honor of recognizing these universities for their achievements during a formal presentation at the 3rd Annual Conference of the National Colloquium for Information Systems Security Education on 25 May 1999, at the IBM Executive Conference Center in Palisades, NY.

Applications for the 2nd annual program offering are now being accepted, and we welcome your participation in this important program. Enclosed you will find the program overview, application procedures, and criteria for designation as a Center of Academic Excellence in Information Assurance Education. Program information can also be found at

http://www.nsa.gov:8080/isso/programs/coeiae/index.htm.
Applications are due to the program office by 8 December 1999. Should you desire additional information, contact the National Information Systems Security Education and Training Program office on (410) 854-6206.

Sincerely,

MICHAEL J. JACOBS
Deputy Director
for
Information Systems Security

Introduction | **Announcement of the Program**
Application Procedures | **Criteria for Measurement** | **NIETP Page**
About the ISSO | **Programs** | **Partnerships** | **Opportunities** | **INFOSEC Home** | **NSA Home**

For assistance in using our products and services, please contact the
NSA INFOSEC Service Center (NISC): 1-800-688-6115

National INFOSEC Education and Training Program

Centers Of Academic Excellence in Information Assurance Education

(Graduate and Undergraduate Levels)

Criteria for Measurement

Revised October 7, 1999

Following are basic criteria for measuring academic excellence in providing Information Assurance (IA) education:

1. The academic program at the university is tied to National Security Telecommunications and Information Systems Security Standards (NSTISSI Standards, http://www.nstissc.gov).
   Overall Point Value: 10 Minimum Required / 15 Maximum Available

   a. Overall curriculum mapped to NSTISSI 4011.
      Point Value: Up to 5 points
   b. Individual courses mapped to NSTISSI 4012, 4013, 4014, and subsequent NSTISSC Training Standards.
      Point Value: Up to 2 points per course / Maximum 10 points

2. The academic program demonstrates IA is not treated as a separate discipline, but as a multidisciplinary science with the body of IA knowledge incorporated into various disciplines.
   Overall Point Value: 10 Minimum Required / 20 Maximum Available

   a. Evidence IA is taught as modules in existing courses.
      Point Value: Up to 2 points per course / Maximum 10 points
   b. IA concentration programs require non-technical courses of study (ethics, policy, legal, human performance, math, business).
      Point Value: Up to 2 points per course / Maximum 10 points

3. The academic program demonstrates how the university encourages the practice of IA, not merely that IA is taught.
   Overall Point Value: 10 Minimum Required / 25 Maximum Available

   a. Copy of university or departmental IA security plan.

Point Value: Up to 10 points

b. Evidence of IA Awareness Program for faculty and students.
Point Value: Up to 10 points
c. University appointed Information Systems Security Officer.
Point Value: 5 points

4. The academic program encourages research in IA.
Overall Point Value: 15 Minimum Required / 30 Maximum Available

a. Programs with IA concentrations have thesis, dissertation, or project requirements.
Point Value: 10 points
b. Individual IA courses require research paper(s) or projects(s).
Point Value: 10 points
c. Non-IA courses encourage papers in IA topics or projects.
Point Value: 2 points per course / Maximum 10 points

5. The IA curriculum reaches beyond the normal geographic borders of the university. (Web site for sharing IA resources and / or internet classes outside normal borders.)
Overall Point Value: 15 Minimum Required / 45 Maximum Available

a. IA curriculum web site.
Point Value: 10 points
b. Use of distance education technology and techniques to deliver IA courses.
Point Value: 20 points
c. Sponsorship of regional or national IA curriculum workshops, colloquia, etc.
Point Value: 15 points

6. It is clearly demonstrated that the faculty is active in IA practice and research, and contributes to IA literature.
Overall Point Value: 15 Minimum Required / 30 Maximum Available

a. Published papers on IA topics within refereed journals.
Point Value: 2 points per paper / Maximum 10 points
b. Faculty awarded grants for IA education and / or research development.
Point Value: 2 points per grant / Maximum 10 points
c. Faculty and or student presentations on IA topics at regional or national conferences.
Point Value: 2 points per presentation / Maximum 10 points

7. The university library and reference systems / materials contain state of the art IA resources.
   Overall Point Value: 15 Minimum Required / 30 Maximum Available

   a. Evidence of access to current INFOSEC educational text books, monographs, etc.
      Point Value: Up to 15 points
   b. Evidence of archive or access to historical IA documents.
      Point Value: Up to 15 points

8. Academic program has declared concentrations in IA.
   Overall Point Value: 0 Minimum Required / 30 Maximum Available

   a. Concentration on IA at the BS level.
      Point Value: 5 points
   b. Concentration on IA at the MS level.
      Point Value: 10 points
   c. Concentration on IA at the Ph.D. level.
      Point Value: 15 points

9. The university has a declared center for IA education.
   Overall Point Value: 0 Minimum Required / 25 Maximum Available

Total MINIMUM Point Requirement = 90

Total MAXIMUM Points Available = 250

MINIMUM POINTS REQUIRED TO QUALIFY AS COE=100

Introduction | Announcement of the Program
Application Procedures | Criteria for Measurement | NIETP Page

About the ISSO | Programs | Partnerships | Opportunities | INFOSEC Home | NSA Home

For assistance in using our products and services, please contact the
NSA INFOSEC Service Center (NISC): 1-800-688-6115

DRAFT NSIA ACADEMIC RESEARCHER STUDY

PURPOSE

To examine options for increasing the number of people both graduating with advanced degrees and teaching and performing basic research in the field of information security/assurance and critical infrastructure protection (ISA/CIP).

BACKGROUND

This is a White House Office of Science and Technology Policy (OSTP) effort to examine possible solutions to the problem of insufficient numbers of researchers and professors in ISA/CIP. What follows is the view from the field – the input from experts in different fields concerned with ISA/CIP. It is meant to be a true, unedited, though synthesized reflection of their ideas, and an attempt to generate discussion and policy. It is not a statement of U.S. Government policy.

The explosion in the U.S. information technology (IT) sector and the corresponding increase in demand for Information Security (IS) specialists within the past decade has caused a severe shortage in the number of academic professionals who are teaching and performing basic research in this field. According to *Critical Foundations: Protecting America's Infrastructure*, the report of the President's Commission on Critical Infrastructure Protection (PCCIP), "There is a significant deficiency in the number of university faculty members equipped to teach information and computer security."[1] Dr. Corey Schou of Idaho State University has written, "Evidence suggests that job growth in information technology fields now exceeds the production of talent. Between 1994 and 2005, more than a million new computer scientists and engineers, systems analysts, and computer programmers will be required in the United States — an average of 95,000 per year."[2] Additionally, graduate and doctoral students in IS are being recruited out of their academic programs and into the private sector, depriving academia of future professors and researchers. Consequently, there are not enough professors currently teaching and performing basic research in IS, nor will there be enough future professors to maintain this current number.

According to *The Supply of Information Technology Workers in the United States*, "doctoral programs are critical in the production of trained workers for both the occupations involving conceptualization and advanced development, and for faculty positions that will educate the next generation of IT workers."[3]

---

[1] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: GPO, 1997), 70.

[2] Corey Schou, "Meeting the Information Assurance Crisis-Now,"

[3] Peter Freeman and William Aspray, *The Supply of Information Technology Workers in the United States* (Washington, D.C.: Computing Research Association , 1999), 71.

Additionally, "advanced researchers, such as faculty members in research universities or principal scientists in industrial research laboratories, almost always have a doctorate in an IT-related discipline, usually computer science or computer engineering (or occasionally in a closely related field such as physics, mathematics, or electrical engineering)." Doctoral level programs and researchers are essential to maintaining the critical U.S. lead in information technology, by supporting and conducting basic research and supporting students coming into the field.

ISA/CIP, as a sub-field of IT, has gained importance in the past few years, as the private-sector has become more reliant on secure information systems. Consequently, private-sector demand for IS specialists has increased. However, there are only a few academic programs dedicated to advance research in this field, in turn meaning that there is a limited pool of qualified IS specialists.[4] The demand on the part of the private sector for this limited pool means that it is extremely difficult for dedicated academic programs to recruit IS-qualified instructors and researchers.

According to various sources private-sector salaries and incentives are proving extremely attractive to IS doctoral students.[5] This has led to a further problem, the recruitment by private industry of IS doctoral students from their academic programs.[6] Referred to as a "seed-corn" problem, this means that not only is there a current shortage of educators in the field, but there will be an ongoing shortage into the future as long as there is a low number of doctoral students moving into academia.

A final problem is the emphasis of applied, short-term research over basic, long-term research. According to the President's Information Technology Advisory Committee (PITAC), "during the past decade both industry and Government have altered the balance between basic research and the later stages of technology development and commercialization," leading to "a serious decline in basic research activities."[7] As basic research is critically important to long-term scientific advances, this decline threatens the current U.S. lead in secure information systems.

Although market forces will gradually increase the number of people going into this field, they will not solve the problem. The focus of private-sector research is on applied research that emphasizes getting products to the market. According

---

[4] According to the National Security Agency, fourteen academic institutions have been labeled as "Centers of Excellence" in the teaching of information security (Vic Maconachy, National Security Agency, Interview, July 6, 2000). However, this estimate has proved controversial, with some sources stating that there are as few as five academic programs that are focused directly on information security (Gene Spafford, Purdue University, Interview, July 24, 2000).

[5] Various Interviews with respondents.

[6] Freedman and Aspray, 117.

[7] President's Information Technology Advisory Committee, *Information Technology Research: Investing in our Future*, 22.

to the PITAC, "American businesses, in an ever-shrinking and more highly competitive world, have devoted less and less of their precious resources to long-term R&D, directing their efforts instead to reducing costs and getting new products in the pipeline today at the expense of the future."[8] Neither is the private-sector focused on long-term basic research, nor does it have enough resources to focus on this area. Accordingly, the influence of the private-sector will not directly increase the number of researchers and educators in the IS field.

In summary, there are not enough ISA/CIP experts currently teaching and performing basic research to meet the current demand; there are not enough doctoral students currently specializing in IS and intending to pursue academic careers to meet future demand; short-term applied research is being emphasized over long-term basic research; and industry-efforts alone will not solve these problems.

[8] Ibid., 79.

SUMMARY OF RECOMMENDATIONS

The Office of Science and Technology Policy, in cooperation with other Federal efforts in the area of information technology research and education, set out to develop a list of recommendations designed to provide a solution to the shortage in ISA/CIP researchers and educators. Various members of academia, the private-sector, and government were interviewed to determine options for solving this problem. A brief summary of their recommendations follows. This list does not reflect Administration policy, but rather is input from the experts in the field.

These recommendations are designed to provide comprehensive program. Alternative recommendations were offered where possible. If implemented as a package, they will support a long-term, sustainable increase in the number of graduates with advanced degrees, teaching and performing basic research in ISA/CIP.

1. Support for ISA/CIP Education and Basic Research

A) The National Science Foundation (NSF) should hold an information-gathering workshop series, polling members of academia, industry, government, and other recognized experts to determine ISA/CIP research and education needs

B) Based on the results of the workshop series listed in the above recommendation, NSF should develop a new organization within its Directorate for Computer and Information Science and Engineering (CISE),dedicated to funding ISA/CIP basic research

C) Alternatively, the NSF should develop a joint initiative with other federal agencies, aimed at promoting and supporting basic research in ISA/CIP

D) The Centers of Academic Excellence in Information Assurance Education (CAE/IAE) Program, currently managed by the National Security Agency's INFOSEC Education and Training Program (NSA-IETP), should be reformed to account for the different focuses and competencies of ISA/CIP programs.

E) The NSA-IETP Internet site should be expanded into an ISA/CIP education "information clearinghouse."

F) The Secretary of Education should designate ISA/CIP as an "Area of National Need" for the purposes of authorizing Graduate Assistance in Areas of National Need (GAANN) funding for students in this field.

G) The Federal Government should increase its efforts at publicizing the importance of ISA/CIP.

2. Support for Students Concentrating on ISA/CIP

A) Fully fund the Federal Cyber Service (FCS) "Scholarship for Service" program

B) Fully fund the Department of Defense (DOD) Information Security Scholarship Program

C) The Department of Education should increase the student stipends currently offered under the GAANN program from $16,800 to $20,000 per student per year.

3. Support for Faculty Early Career-Development in ISA/CIP

A) The FCS "Scholarship for Service" program capacity-building track should include an Early Career Development component, modeled on the NSF CAREER Program and the National Institute's of Health's (NIH) K-22 Career Transition Award.

B) Alternatively, modify a portion of the NSF Faculty Early Career Development (CAREER) Program to allow ISA/CIP applicants who are not yet employed in a tenure-track position, but have received their first doctoral degree, to apply for and be awarded this grant on a tentative basis.

C) Either the NSA-IETP or the NSF should develop a "Best Paper" award for research conference papers concerning ISA/CIP.

4. Support for Faculty Teaching and Research in ISA/CIP

A) OSTP with support from the NSF should establish a government-funded "Presidential Distinguished Chairs in Information Security/Assurance and Critical Infrastructure Protection" ("Chair(s)") at academic institutions.

B) OSTP with support from the NSF should establish "Presidential Recognition Awards for Education and Research in ISA/CIP."

5. Support for Faculty Development in a New Area

A) Fully fund the FCS "Scholarship for Service" Faculty Development program

B) The NSF should develop an "ISA/CIP Academic Transition" award for faculty moving into the ISA/CIP field from another separate academic field. This award should be modeled on the NIH K-01 Mentored Research Scientist Development Award.

C) The annual Naval Post-Graduate School Practicum Workshop on Education in Computer Security (Practicum WECS) should be expanded.