Terry - FYI:
Material as distributed at
the University Presidents meeting
10/19/2000

National Security Council
The White House

Visit of NSA Centers of Academic Excellence University Presidents and Information Assurance Representatives

19 October 2000
1330-1600 hours

Eisenhower Executive Office Building
Room 552

NIETP
National INFOSEC Education and Training Program

Candidate Discussion Points

1. The need for strong advocacy for cyber education
2. Fulfilling requirements for trained IS/IT workers
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

Agenda

1330-1350	Richard A. Clarke *Special Assistant to the President and National Coordinator for Security, Infrastructure Protection and Counter-terrorism, National Security Council*
1350-1410	Dr. Neal Lane *Assistant to the President and Director, Office of Science and Technology Policy*
1410-1430	Dr. John Hunt *Deputy Assistant Director, Education and Human Resources, National Science Foundation*
1430-1500	Carol Okin *Director of Employment Services, Office of Personnel Management*
1500-1600	Discussion

Draft IT Job Profile

SELECT BOTH GENERAL AND TECHNICAL COMPETENCIES BASED ON THE LEVEL OF THE POSITION TO BE FILLED. THE TOTAL NUMBER OF COMPETENCIES SELECTED IS TYPICALLY 4-8.

GENERAL COMPETENCIES:

FUNDAMENTAL: (All levels) Arithmetic; Learning; Memory; Reading; Writing

COMMUNICATION/COLLABORATION: (All levels) Customer Service; Interpersonal Skills; Oral Communication; Teamwork

(Journey and above) Influencing/Negotiating; Leadership; Teaching Others

BUSINESS ACUMEN: (All levels) Attention to Detail; Decision Making; Mathematical Reasoning; Planning and Evaluating; Problem Solving; Reasoning; Technology Application

(Journey and Above) Organizational Awareness

(Senior Expert) Managing Human Resources; Strategic Thinking; Vision

PERSONAL AWARENESS: (All levels) Flexibility; Integrity/Honesty; Self-Esteem; Self-Management; Stress Tolerance

INNOVATION/RESULTS: (Intermediate and above) Creative Thinking; Information Management

(Senior Expert) Financial Management

TECHNICAL COMPETENCIES:

GENERAL IT: (All levels) Standards; Telecommunications

(Intermediate and above) Hardware; IT Architecture; Infrastructure Design; Operations Support; Systems Integration; Technology Awareness

SPECIALIZED IT: (All levels) Computer Languages; Information Assurance; Network Management; Systems Life Cycle; Systems Testing and Evaluation; Web Technology

(Intermediate) Configuration Management; Data Management; Database Administration; Database Management Systems; Distributed Systems; IT Performance Assessment; Multimedia Technologies; Operating Systems; Process Control; Technical Documentation

(Journey and above) Capacity Management; Computer Forensics; Encryption; Information Systems/Network Security; Information Systems Security Certification;

IT Strategic Policy, Planning, and Management; Knowledge Management; Logical Systems Design; Project Management; Requirements Analysis; Software Development; Software Engineering; Software Testing and Evaluation

COMPETENCIES IN RELATED AREAS: Administration and Management; Business Process Reengineering; Capital Planning and Investment Assessment; Contracting; Cost-Benefit Analysis; Education and Training; Engineering and Technology; Human Factors; Organizational Development; Product Evaluation; Quality Assurance; Risk Management

WORK LEVEL DESCRIPTORS AND ASSESSMENT OPTIONS: *(SEE KEY LIST BELOW)*

ENTRY: *Tasks range from the simple and elementary through the somewhat difficult; tasks are performed under immediate to general supervision, with limited opportunity for the exercise of independent judgment.*

INTERMEDIATE: *Tasks range from the moderately difficult to the considerably difficult; tasks are performed under supervision that allows for considerable to wide latitude that allows for the exercise of independent judgement.*

JOURNEY: *Tasks range from the highly difficult to the complex; they are performed under little supervision that allows for ample latitude for the exercise of independent judgment.*

SENIOR EXPERT: *Tasks are of a highly complicated nature calling for the exercise of independent judgment and little or no supervision.*

Note: For use in conjunction with new IT Functional Specialty Titles.

COMPETENCY ASSESSMENT AND INDICATOR OF PROFICIENCY OPTIONS: Applicants must demonstrate proficiency in all of the competencies you identified as important from the relevant clusters above, based on the level of the position to be filled. Choose assessment option(s) that cover **all** of the competencies you identified as important for the position.

ASSESSMENT OPTIONS:

A. Assessment Center
B. Crediting Plan/Rating Schedule
C. Structured Interview
D. Work Sample Assessment
E. Test

INDICATORS OF PROFICIENCY: (a source of evidence of a candidate's proficiency level on a specific competency; they can be incorporated into the assessment options)

A. Agency Certification Program
B. Education e.g., coursework
C. Experience e.g., school, home, community, voluntary, or work experience
D. Professional Activity e.g., publication
E. Professional Certification

SELECT BOTH GENERAL AND TECHNICAL COMPETENCIES BASED ON THE LEVEL OF THE POSITION TO BE FILLED. THE TOTAL NUMBER OF COMPETENCIES SELECTED IS TYPICALLY 4-8.

GENERAL COMPETENCIES:

FUNDAMENTAL: (All levels) Arithmetic; Learning; Memory; Reading; Writing

COMMUNICATION/COLLABORATION: (All levels) Customer Service; Interpersonal Skills; Oral Communication; Teamwork

(Journey and above) Influencing/Negotiating; Leadership; Teaching Others

BUSINESS ACUMEN: (All levels) Attention to Detail; Decision Making; Mathematical Reasoning; Planning and Evaluating; Problem Solving; Reasoning; Technology Application

(Journey and Above) Organizational Awareness

(Senior Expert) Managing Human Resources; Strategic Thinking; Vision

PERSONAL AWARENESS: (All levels) Flexibility; Integrity/Honesty; Self-Esteem; Self-Management; Stress Tolerance

INNOVATION/RESULTS: (Intermediate and above) Creative Thinking; Information Management

(Senior Expert) Financial Management

TECHNICAL COMPETENCIES:

GENERAL IT: (All levels) Standards

(Intermediate and above) IT Architecture; Infrastructure Design; Systems Integration

SPECIALIZED IT: (All levels) Information Assurance; Network Management; Systems Life Cycle

(Intermediate) IT Performance Assessment

(Journey and above) Computer Forensics; Encryption; Information Systems/Network Security; Information Systems Security Certification; IT Strategic Policy, Planning and Management

COMPETENCIES IN RELATED AREAS: Administration and Management; Cost-Benefit Analysis; Risk Management

WORK LEVEL DESCRIPTORS AND ASSESSMENT OPTIONS: *(SEE KEY LIST BELOW)*

ENTRY: *Tasks range from the simple and elementary through the somewhat difficult; tasks are performed under immediate to general supervision, with limited opportunity for the exercise of independent judgment. Assessment Options: A, B, C, D, E Indicators of Proficiency: A, B, C, D*

INTERMEDIATE: *Tasks range from the moderately difficult to the considerably difficult; tasks are performed under supervision that allows for considerable to wide latitude that allows for the exercise of independent judgement. Assessment Options: A, B, C, D, E Indicators of Proficiency: A, B, C, D, E*

JOURNEY: *Tasks range from the highly difficult to the complex; they are performed under little supervision that allows for ample latitude for the exercise of independent judgment. Assessment Options: A, B, C, D, E Indicators of Proficiency: A, B, C, D, E*

SENIOR EXPERT: *Tasks are of a highly complicated nature calling for the exercise of independent judgment and little or no supervision. Assessment Options: A, B, C, D Indicators of Proficiency: B, C, D, E*

Note: For use in conjunction with new IT Functional Specialty Titles.

COMPETENCY ASSESSMENT AND INDICATOR OF PROFICIENCY OPTIONS: Applicants must demonstrate proficiency in all of the competencies you identified as important from the relevant clusters above, based on the level of the position to be filled. Choose assessment option(s) that cover **all** of the competencies you identified as important for the position.

ASSESSMENT OPTIONS:

A. Assessment Center
B. Crediting Plan/Rating Schedule
C. Structured Interview
D. Work Sample Assessment
E. Test

INDICATORS OF PROFICIENCY: (a source of evidence of a candidate's proficiency level on a specific competency; they can be incorporated into the assessment options)

A. Agency Certification Program
B. Education e.g., coursework
C. Experience e.g., school, home, community, voluntary, or work experience
D. Professional Activity e.g., publication
E. Professional Certification

GENERAL COMPETENCIES

1. **Administration and Management** – Knowledge of planning, coordination, and execution of business functions, resource allocation, and production.
2. **Arithmetic** – Performs computations such as addition, subtraction, multiplication, and division correctly using whole numbers, fractions, decimals, and percentages.
3. **Attention to Detail** – Is thorough when performing work and conscientious about attending to detail.
4. **Conflict Management** – Manages and resolves conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact.
5. **Creative Thinking** – Uses imagination to develop new insights into situations and applies innovative solutions to problems; designs new methods where established methods and procedures are inapplicable or are unavailable.
6. **Customer Service** – Works with clients and customers (that is, any individuals who use or receive the services or products that your work unit produces, including the general public, individuals who work in the agency, other agencies, or organizations outside the Government) to assess their needs, provide information or assistance, resolve their problems, or satisfy their expectations; knows about available products and services; is committed to providing quality products and services.
7. **Decision Making** – Makes sound, well-informed, and objective decisions; perceives the impact and implications of decisions; commits to action, even in uncertain situations, to accomplish organizational goals; causes change.
8. **Education and Training** – Knowledge of teaching, training, research, making presentations, lecturing, testing, and other instructional methods.
9. **Engineering and Technology** – Knowledge of engineering concepts, principles, and practices, and of equipment, tools, mechanical devices, and their uses to produce motion, light, power, technology, and other applications.
10. **External Awareness** – Identifies and understands economic, political, and social trends that affect the organization.
11. **Financial Management** – Prepares, justifies, and/or administers the budget for program areas; plans, administers, and monitors expenditures to ensure cost-effective support of programs and policies; assesses financial condition of an organization.
12. **Flexibility** – Is open to change and new information; adapts behavior or work methods in response to new information, changing conditions, or unexpected obstacles; effectively deals with ambiguity.
13. **Information Management** – Identifies a need for and knows where or how to gather information; organizes and maintains information or information management systems.
14. **Influencing/Negotiating** – Persuades others to accept recommendations, cooperate, or change their behavior; works with others towards an agreement; negotiates to find mutually acceptable solutions.
15. **Integrity/Honesty** – Contributes to maintaining the integrity of the organization; displays high standards of ethical conduct and understands the impact of violating these standards on an organization, self, and others; is trustworthy.

16. **Interpersonal Skills** – Shows understanding, friendliness, courtesy, tact, empathy, concern, and politeness to others; develops and maintains effective relationships with others; may include effectively dealing with individuals who are difficult, hostile, or distressed; relates well to people from varied backgrounds and different situations; is sensitive to cultural diversity, race, gender, disabilities, and other individual differences.
17. **Leadership** – Influences, motivates, and challenges others; adapts leadership styles to a variety of situations.
18. **Learning** – Uses efficient learning techniques to acquire and apply new knowledge and skills; uses training, feedback, or other opportunities for self-learning and development
19. **Legal, Government and Jurisprudence** – Knowledge of laws, legal codes, court procedures, precedents, legal practices and documents, government regulations, executive orders, agency rules, government organization and functions, and the democratic political process.
20. **Managing Human Resources** – Plans, distributes, coordinates, and monitors work assignments of others; evaluates work performance and provides feedback to others on their performance; ensures that staff are appropriately selected, utilized, and developed, and that they are treated in a fair and equitable manner.
21. **Mathematical Reasoning** – Solves practical problems by choosing appropriately from a variety of mathematical and statistical techniques.
22. **Memory** – Recalls information that has been presented previously.
23. **Mental Visualization** – Sees things in the mind by mentally organizing and processing symbols, pictures, graphs, objects, or other information (for example, sees a building from a blueprint, or sees the flow of work activities from reading a work plan).
24. **Oral Communication** – Expresses information (for example, ideas or facts) to individuals or groups effectively, taking into account the audience and nature of the information (for example, technical, sensitive, controversial); makes clear and convincing oral presentations; listens to others, attends to nonverbal cues, and responds appropriately.
25. **Organizational Awareness** – Knows the organizations mission and functions, and how its social, political, and technological systems work and operates effectively within them; this includes the programs, policies, procedures, rules, and regulations of the organization.
26. **Planning and Evaluating** – Organizes work, sets priorities, and determines resource requirements; determines short- or long-term goals and strategies to achieve them; coordinates with other organizations or parts of the organization to accomplish goals; monitors progress and evaluates outcomes.
27. **Problem Solving** – Identifies problems; determines accuracy and relevance of information; uses sound judgment to generate and evaluate alternatives, and to make recommendations.
28. **Public Safety and Security** – Knowledge of the military, weaponry, and intelligence operations; public safety and security operations; occupational health and safety; investigation and inspection techniques; or rules, regulations, precautions, and prevention techniques for the protection of people, data, and property.
29. **Reading** – Understands and interprets written material, including technical material, rules, regulations, instructions, reports, charts, graphs, or tables; applies what is learned from written material to specific situations.

30. **Reasoning** – Identifies rules, principles, or relationships that explain facts, data, or other information; analyzes information and makes correct inferences or draws accurate conclusions.
31. **Self-Esteem** – Believes in own self-worth; maintains a positive view of self and displays a professional image.
32. **Self-Management** – Sets well-defined and realistic personal goals; displays a high level of initiative, effort, and commitment towards completing assignments in a timely manner; works with minimal supervision; is motivated to achieve; demonstrates responsible behavior.
33. **Strategic Thinking** – Formulates effective strategies consistent with the business and competitive strategy of the organization in a global economy. Examines policy issues and strategic planning with a long-term perspective. Determines objectives and sets priorities; anticipates potential threats or opportunities.
34. **Stress Tolerance** – Deals calmly and effectively with high stress situations (for example, tight deadlines, hostile individuals, emergency situations, dangerous situations).
35. **Teaching Others** – Helps others learn through formal or informal methods; identifies training needs; provides constructive feedback; coaches others on how to perform tasks; acts as a mentor.
36. **Teamwork** – Encourages and facilitates cooperation, pride, trust, and group identity; fosters commitment and team spirit; works with others to achieve goals.
37. **Technical Competence** – Uses knowledge that is acquired through formal training or extensive on-the-job experience to perform one's job; works with, understands, and evaluates technical information related to the job; advises others on technical issues.
38. **Technology Application** – Uses machines, tools, or equipment effectively; uses computers and computer applications to analyze and communicate information in the appropriate format.
39. **Vision** – Understands where the organization is headed and how to make a contribution; takes a long-term view and recognizes opportunities to help the organization accomplish its objectives or move toward the vision.
40. **Writing** – Recognizes or uses correct English grammar, punctuation, and spelling; communicates information (for example, facts, ideas, or messages) in a succinct and organized manner; produces written information, which may include technical material, that is appropriate for the intended audience.
41. **Contracting/Procurement** - Knowledge of various types of contracts, techniques for contracting or procurement, and contract negotiation and administration. conduct and understands the impact of violating these standards on an organization, self, and others; chooses an ethical course of action; is trustworthy.

TECHNICAL COMPETENCIES

1. **Accessibility** - Knowledge of tools, equipment, and technologies (for example, voice recognition, screen readers) used to help individuals with disabilities use computer equipment and software.
2. **Artificial Intelligence** - Knowledge of principles, methods, and tools to design systems that perform human intelligence functions (for example, expert systems, knowledge-based systems).
3. **Business Process Reengineering** - Knowledge of methods, metrics, tools, and techniques of Business Process Reengineering.
4. **Capacity Management** - Knowledge of the principles and methods for monitoring, estimating, and reporting actual performance or the performance capability of information systems or components.
5. **Capital Planning and Investment Assessment** - Knowledge of the principles and methods of capital investment analysis and business case analysis including best practices assessment and return on investment analysis.
6. **Computers and Electronics** – Knowledge of electric circuit boards, processors, chips, and computer hardware and software, including applications and programming.
7. **Computer Languages** - Knowledge of computer languages and their applications.
8. **Computer Forensics** - Knowledge of tools and techniques used in data recovery and preservation of electronic evidence (for example, chain of evidence rules).
9. **Configuration Management** - Knowledge of the principles and methods for planning and managing the implementation, updating, and integration of information system components, including software, controlling future releases, and documenting information and physical characteristics of an information system or product.
10. **Cost-Benefit Analysis** - Knowledge of the principles and methods of cost-benefit analysis, including the time value of money, present value concepts, cost accounting, business economics, and quantifying the tangible and intangible benefits.
11. **Data Management** - Knowledge of the principles, procedures, and tools of data management, such as modeling techniques, data backup and recovery, data dictionaries, data mining, data warehousing concepts, data disposal/remenance management, and data standardization processes.
12. **Database Administration** - Knowledge of the principles, methods, and tools for automating, developing, implementing, and administering database management systems, such as logical and physical design, space allocation, and performance monitoring.
13. **Database Management Systems** - Knowledge of database management systems and their applications.
14. **Distributed Systems** - Knowledge of the principles, theoretical concepts, and tools underlying distributed systems.
15. **Electronic Commerce (e-Commerce)** - Knowledge of principles and methods of electronic transactions (for example, requests, orders).
16. **Embedded Computers** - Knowledge of specifications and uses of embedded computers including appropriate programming languages.
17. **Encryption** - Knowledge of procedures, tools, and applications used to keep data or information secure (for example, public key infrastructure, point-to-point encryption, smart cards).

18. **Hardware** - Knowledge of specifications, uses, and types of hardware components.
19. **Hardware Engineering** - Knowledge of the principles, methods, and tools for designing, developing, and testing computer or computer-related equipment.
20. **Human Factors** - Knowledge of human factors principles, methods, tools, and applications, for example Graphic User Interface Design.
21. **Information Assurance** - Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
22. **Information Resources Strategy and Planning** - Knowledge of the principles, methods and techniques of information technology (IT) assessment, planning, management, monitoring and evaluation, such as IT baseline assessment, interagency functional analysis, contingency planning and disaster recovery.
23. **Information Systems Security Certification** - Knowledge of principles, methods, and tools for evaluating information systems security features against a set of specified security requirements, includes developing certification and accreditation plans and procedures, documenting deficiencies, reporting corrective actions, and recommending changes to improve the security of information systems.
24. **Information Systems/Network Security** - Knowledge of methods for developing, evaluating, coordinating, and disseminating security tools and procedures; ensuring, protecting, and restoring the security of information systems and network services and capabilities; identifying and eliminating information system vulnerabilities to inadvertent disclosure, modification, destruction, or denial of service.
25. **Information Technology Architecture**- Knowledge of architectural methodologies for information systems or applications design and development.
26. **Information Technology Performance Assessment** - Knowledge of the principles, methods and tools for conducting performance assessments of information technology systems (for example, customer surveys, system performance measures, and the Government Performance and Results Act).
27. **Infrastructure Design** - Knowledge of the architecture and typology of software, hardware, and networks, including LANS, WANS, and telecommunication systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.
28. **Knowledge Management** - Knowledge of the business value of information and the processes for making data available and useful to decision-makers.
29. **Logical Systems Design** - Knowledge of principles and methods for designing user interfaces, data inputs, system processes/outputs, business logic components, and productivity tools (e.g. CASE).
30. **Modeling and Simulation** - Knowledge of modeling and simulation tools and techniques to characterize systems of interest, support decisions involving requirements, evaluate design alternatives, support training, or support operational preparation.
31. **Multimedia Technologies** - Knowledge of the principles, methods, tools, and techniques of multimedia technologies and their applications.
32. **Network Management** - Knowledge of the operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals, including operational performance monitoring, estimating, and reporting; configuration management; fault detection and isolation; security management; and corrective action.

33. **Object Technology** - Knowledge of the principles, methods, tools, and techniques of object technology, including object-oriented languages, analysis, and design methodologies.
34. **Operating Systems** - Knowledge of computer network, desktop, and mainframe operating systems and their applications.
35. **Operations Support** - Knowledge of procedures to troubleshoot, recover, adjust, modify, and improve systems to ensure production or delivery of products and services, including tools and mechanisms for distributing new or enhanced software.
36. **Organizational Development** - Knowledge of the principles of organizational development and change management theories and their application in an information technology environment.
37. **Process Control**- Knowledge of process control applications and procedures including the design, development, and maintenance of associated software, hardware, and systems.
38. **Product Evaluation** - Knowledge of methods for researching and analyzing external products to determine their potential for meeting organizational standards and business needs.
39. **Project Management**- Knowledge of methods, principles or tools for managing IT projects, including acquisition/procurement management.
40. **Quality Assurance** - Knowledge of principles, methods and tools of quality assurance.
41. **Requirements Analysis** - Knowledge of principles and methods to identify, analyze, specify, design, and manage the client's functional and infrastructure requirements; includes translating functional requirements into technical requirements used for logical design or presenting alternative technologies or approaches.
42. **Risk Management** - Knowledge of methods and tools used for risk assessment and mitigation of risk to information systems and data.
43. **Software Development** - Knowledge of the principles, methods, and tools for designing, developing, and testing software in a given environment (e.g. computer applications, operating systems-level software, compilers, and network distribution software). Knowledge of the uses of commercial off-the-shelf (COTS) software applications.
44. **Software Engineering** - Knowledge of software development methodology, paradigms, and tools; software requirements analysis; the software lifecycle; software reusability; and software reliability metrics.
45. **Software Testing and Evaluation** - Knowledge of principles, methods, and tools for analyzing and developing test and evaluation procedures.
46. **Standards** - Knowledge of information systems standards that either are compliant with or derived from other industrial, Government, and international standards and guidelines.
47. **Systems Integration** - Knowledge of principles, methods, and procedures for optimizing, integrating, and installing information system components.
48. **Systems Life Cycle** - Knowledge of Systems Life Cycle Management concepts used to plan, develop, implement, operate, and maintain information systems.
49. **Systems Testing and Evaluation** - Knowledge of principles, methods, and tools for analyzing development and technical characteristics of IT systems; identifying critical operational issues; defining, documenting, implementing, executing, and reporting results of systems tests and evaluations.
50. **Technical Documentation** - Knowledge of procedures for developing technical and operational support documentation.

51. **Technology Awareness** – Monitors and evaluates developments and new applications of information technology (hardware, software, telecommunications); applies emerging technologies to business processes; applies and monitors implementation of information systems to meet organizational requirements.
52. **Telecommunications** – Knowledge of transmissions, broadcasting, switching, control, and operation of telecommunications systems.
53. **Web Technology** - Knowledge of the principles and methods of web technologies, tools and delivery systems.

DRAFT

New Information Technology (IT) Parenthetical Specialty Titles

1. Communications and Network Services - This specialty covers the planning, analysis, design, development, testing, quality assurance, configuration, implementation, integration, maintenance, and/or management of networked systems used for the transmission of information in voice, data, and/or video formats. Functions include analyzing and defining network requirements, defining and maintaining physical network architecture and infrastructure, configuring and optimizing network servers, hubs, routers, and switches, analyzing network workload, monitoring network capacity and performance, diagnosing and resolving problems, making adjustments to ensure proper load balancing, developing backup and recovery procedures, installing, testing, maintaining, and upgrading network operating systems software, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to as network administrator, LAN/WAN administrator, network analyst, network designer, network engineer, communications analyst, data communications specialist, or communications engineer.

2. Customer Support - This specialty covers planning and delivery of customer support services including installation, troubleshooting, user assistance, and/or training. Functions may include diagnosing and resolving problems in response to customer reported incidents, researching trends and patterns of problems, developing and maintaining problem tracking databases, installing, troubleshooting, and maintaining hardware and software, performing backup and recovery operations, providing user training, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to as technical support specialist, user support specialist, help desk representative, and maintenance specialist.

3. Data Management - This specialty covers planning, development, implementation, and administration of systems for the acquisition, storage, and retrieval of data. Functions may include analyzing and defining data requirements and specifications, designing, developing, implementing, modifying, and managing databases, ensuring the accuracy and accessibility of data sources, analyzing and planning for anticipated changes in data capacity requirements, developing and administering data standards, policies, and procedures, defining data flow and developing data flow diagrams, building and maintaining data dictionaries, developing physical data models, developing and implementing data mining and data warehousing programs, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to as database developer, database administrator, data analyst, data administrator, data architect, storage specialist, and data warehouse specialist.

4. Information Systems Security - This specialty covers planning, analysis, development, implementation, maintenance, and enhancement of systems, programs, policies, procedures, and tools to ensure the integrity, availability, and confidentiality of information systems. Functions may include developing policies and procedures to ensure systems reliability and accessibility and to prevent and defend against unauthorized access to networks, systems, and data, conducting risk and vulnerability assessments of planned and installed systems, conducting security evaluations, audits, and reviews, developing contingency plans and disaster recovery procedures, participating in network and systems design to ensure implementation of appropriate security policies, and assisting in the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes. Also may include developing and implementing programs to ensure that users understand and adhere to security policies and procedures. Includes positions commonly referred to as information security analyst/specialist and information assurance analyst/specialist.

5. Policy, Planning, and Management - This specialty covers a wide range of activities that typically extend and apply to an entire organization or major components of an organization. This includes strategic planning, capital planning, workforce planning, policy and standards development, budgeting, knowledge management, information architecture, infrastructure planning and modeling, investment analysis, auditing, and information security. Functions may include assessing policy needs and developing policies to govern IT activities, providing policy guidance to IT management, staff, and customers, coordinating the review of IT functions and processes to determine policy priorities, developing and maintaining strategic plans, defining current and future business environments, preparing IT budgets, identifying and addressing IT workforce issues, such as recruitment, retention, and training, conducting audits of IT programs and projects, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to enterprise resource planner, IT training officer, IT policy and planning analyst, IT program management specialist, and IT auditor.

6. Software Engineering, Applications - This specialty covers the design, development, modification, installation, implementation, and support of new or existing applications software. Functions may include analyzing systems requirements, writing code, validating data acquisition and output media/formats, designing user interfaces, working with users to test and debug applications, assuring software and systems quality and functionality, integrating hardware and software components, writing and maintaining program documentation, evaluating new and improved software applications and programming technologies, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to as programmer, programmer analyst, applications developer, software engineer, software developer, and software quality assurance specialist.

7. Software Engineering, Systems Software - This specialty covers the planning, installation, implementation, configuration, and maintenance of operating systems software. Functions may include analyzing systems requirements, evaluating and selecting operating systems software, modifying, testing, debugging, installing, and maintaining compilers, assemblers, and utilities, integrating hardware and software components, monitoring and fine-tuning operating systems performance, evaluating new and improved operating systems programming technologies, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to as systems programmer, mainframe programmer, and software engineer.

8. Systems Administration - This specialty covers planning and coordination of the installation, testing, operation, troubleshooting, and maintenance of hardware and software systems. Functions may include planning and scheduling the installation of new or modified hardware/software, allocating systems resources, managing accounts, network rights, and access to systems and equipment, administering passwords, monitoring the performance, capacity, availability, serviceability, and recoverability of installed systems, implementing security procedures and tools, resolving hardware/software interface and interoperability problems, ensuring systems functionality, integrity, and efficiency, maintaining systems configuration, managing the installation and integration of system patches, updates, and enhancements, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to as systems administrator, site administrator, and UNIX/SOLARIS systems administrator.

9. Systems Analysis - This specialty covers planning and analysis of work processes leading to the application of information systems to meet user requirements. Functions may include conducting needs analyses to define opportunities for new or improved applications, consulting with users to identify requirements, conducting feasibility studies and trade-off analyses, preparing business cases, defining systems scope and objectives, developing cost estimates, developing overall functional and technical requirements and specifications, evaluating and recommending sources for systems components, ensuring the integration and implementation of applications, databases, networks, and systems, evaluating and providing consultation in the development of business and e-commerce applications, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to as systems analyst, business analyst, e-business/e-commerce specialist, equipment analyst, and hardware analyst.

10. Web Development - This specialty covers planning, design, development, testing, implementation, and management of internal and external web sites. Functions may include determining overall web site design and structure, monitoring web site functionality, security, and integrity, troubleshooting and resolving problems, reviewing, testing, and integrating web pages, collecting and analyzing web site statistics, evaluating new web applications, providing technical advice to web content providers, and ensuring the rigorous application of information security/information assurance policies, principles, and practices. Includes positions commonly referred to as webmaster, web specialist, web developer, and web architect.

11. General - This covers positions not classifiable in any of the other specialties, e.g., positions in new or rapidly evolving specialty areas. Please Note – Regardless of the nature of the work assigned, the position must include responsibility for ensuring the rigorous application of information security/information assurance policies, principles, and practices.

EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

WASHINGTON, D.C. 20502

PHONE CALL TO DEPUTY SECRETARY OF DEFENSE RUDY DELEON

Date: Prior to October 25, 2000
Time: TBD
Location: Phone Call

From: Gerald Epstein

I. Objectives

To encourage Mr. DeLeon to restore $15M in FY01 funding to the Defense Infrastructure and Interdependencies Program, which addresses the key issue of critical infrastructure interdependencies R&D.

II. Background

- The Joint Program Office for Special Technical Countermeasures (JPO-STC) in DoD runs a Joint Vulnerability Analysis Program that does excellent Critical Infrastructure Protection (CIP) R&D and operational analysis for the DoD. It contains two sub-programs of particular interest for Critical Infrastructure Protection.

- The first program, the Commercial Infrastructures Program (also called "commercial assessment and analysis work" in a letter from Sec DeLeon to Dick Clarke – see Tab C), performs analyses and assessments of critical civil infrastructures in the vicinity of military installations. It is funded.

- The second program, the Defense Infrastructure and Interdependencies Program, about which you are calling, is not funded (both programs are discussed in more detail in Tab B).

- This second program was originally funded through a supplemental appropriation in FY99. These funds carried it through the end of FY00. OSTP identified it as important during the Critical Infrastructure Protection R&D process, and OMB gave DoD $15M in new FY01 money specifically for this program. It is important because it is one of the only efforts that examines infrastructure interdependencies, is one of our R&D IWG's highest priorities, and is developing methodologies to examine these.

- Then Deputy Secretary of Defense Hamre zeroed this $15M line. We believe this was due to a misunderstanding of what the intent of the

program was – there is some indication that he thought it was a SAIC study rather than an attempt to develop a critical approach to solving an important problem.

- I called Sec Hamre's office this past January to urge that funding be restored, and was told essentially that Sec Hamre did not like the JPO.

- **OMB intends to address FY01 funding for this program during the FY02 budget hearing they will hold with DoD on critical infrastructure protection programs on October 27. Specifically, they know where the money was moved to and will ask DoD to reprogram it. I recommend you support this.**

Attachments:

Tab A	Talking Points
Tab B	Program Background
Tab C	DeLeon Letter to Richard Clarke

TALKING POINTS FOR YOUR PHONE CALL
WITH DEPUTY SECRETARY OF DEFENSE RUDY DELEON

- Rudy, I wanted to talk to you about a program DoD has run for the last 2 years – JPO-STC's Defense Infrastructure and Interdependencies Program.

- This is a very important piece of our national critical infrastructure protection R&D program, but OMB tells me it is not funded in FY01.

- I know the JPO-STC has done some great work looking at these issues around your forts and bases here in the US, and that this effort is fully funded – I believe you have corresponded with Dick Clarke on this.

- But this second half of the JPO's CIP effort, the Defense Infrastructure and Interdependencies program, is also tremendously important to the national effort. It is just about the only program that focuses on developing an understanding of, and methodologies for analyzing the interdependencies across infrastructure sectors.

- This is the truly hard piece of the infrastructure protection mission – really the key technical piece to understanding the effects that an outage in any one infrastructure will have on all other infrastructures.

- OMB tells me that they are going to bring this up in the October 27 budget hearing on critical infrastructure protection programs they are holding with your folks to look at FY02 funding, and that they will recommend you reprogram FY01 funds to cover this.

10/12/00

- I want you to know that I believe this program is particularly important. It was identified by OSTP's CIP interagency process as one of our highest R&D priorities – and as a result, OMB provided $15M in new funds to the Department to carry it out.

- Frankly, it is difficult to motivate agencies to work to develop cross-departmental R&D efforts if we cannot provide resources to those programs that we identify as our highest priorities.

- I hope you will support this reprogramming. Let me know if my staff or I can be of any assistance to you on this.

JPO-STC Program Background

1. **JPO-STC Joint Vulnerability Analysis Program:** This is the overarching program that funds JPO-STC's CIP efforts. It contains two sub-programs. Their **Commercial Infrastructures Program** or core capability, also referred to in Sec DeLeon's letter as the "commercial assessment and analysis work" is funded. Their **Defense Infrastructure and Interdependencies Program** is not considered in Sec DeLeon's letter, and is not funded.

2. **Commercial Infrastructures Program**: This is JPO-STC's "core capability" and it centers around a well established analysis and assessment process that determines (via integration of various network models and data) the critical commercial infrastructure nodes and links that support military sites of interest. This core capability, funded via Navy channels:

   - establishes interagency teams (unique to DoD),
   - determines critical nodes and links of commercial networks of power, telecommunications (some interdependencies),
   - is US focused,
   - is tied to the specific missions/tasks of the military sites (in other words it requires a methodology which translates commercial infrastructure disruptions into quantifiable mission impacts, to include in-theater impacts),
   - is well suited to provide options (mitigation, restoration, investment strategies) in the format of a decision support matrix, and
   - is fully funded.

3. **Defense Infrastructure and Interdependencies Program:** Besides their Core Capabilities, the JPO-STC's CIP Analysis program is important to the CIP R&D agenda. These efforts were initially funded through a supplemental appropriation in FY99 that provided funds through the end of FY 00. It's objective is to develop methodologies or capabilities which:

   - standardize defense infrastructure sector analysis and assessment from a functional/business continuity perspective (there are 10 defense infrastructure sectors which roughly match the national level sectors),
   - identify links between the infrastructure sectors (i.e. intra and inter-dependencies),
   - tie these defense assets into deliberate planning to support mission assurance and/or readiness/sustainment issues (via Operations Plans, Time Phased Force Deployment List, etc.),
   - investigate civil/industry risk management philosophies applicable to DoD/federal government processes and organizations
   - integrate mission critical DoD supporting assets with the core commercial infrastructure assets into a DoD wide view.

OMB supplied $15M in new funding for this program in FY01, which was redistributed after Deputy Secretary of Defense Hamre killed the program.

Rec'd 10-10-

DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

OCT 6 2000

MEMORANDUM FOR NATIONAL COORDINATOR FOR SECURITY, INFRASTRUCTURE PROTECTION AND COUNTER-TERRORISM

SUBJECT: Concern That CIP at JPO-STC Is Being Terminated

I agree with you that the work being done by the JPO-STC is critical to accomplishing the Critical Infrastructure Protection efforts laid out in PDD 63 and further refined in the *National Plan for Information Systems Protection.* I have confirmed that the JPO-STC commercial infrastructures assessment and analysis work that you mention is fully funded. The effort funded in the FY 1999 Supplemental will provide the methodology/processes for future analysis and assessment of defense infrastructures and for linkages to CINC warfighting plans. Future program reviews will analyze the results of this work and determine requirements for additional funding in this area.

Rudy de Leon

Kelly

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

MEETING WITH DICK CLARKE

Date: October 16, 2000
Time: 2:30 PM– 3:30 PM
Location: Room 303 OEOB

From: Gerald Epstein

I. Objectives

To agree to empanel a Convergence Task Force charged with articulating the legal, policy, technical and security issue of network convergence, and a process for addressing them. This task force is to report back to you and Sandy Berger by January 1, 2001. Your talking points are at Tab A.

II. Background

A. Technical Background:

- The NSTAC projects that the Public Telephone Switching Network and the Internet will converge sometime in the next 3-5 years, and will later evolve into the Next Generation Network (NGN).
- This convergence puts at risk current means for providing voice National Security/Emergency Preparedness (NS/EP) communications – specifically it raises legal, policy, technical and security issues.
- The NSTAC, in their *Information Technology Progress Impact Task Force Report on Convergence* (May 2000), recommended that the President "promptly determine precise functional NS/EP requirements for Convergence and the NGN."
- An interagency process for addressing these issues is needed – NSIA together with Dick Clarke's staff, recommend a Convergence Task Force be empanelled to examine this issue and report back to you and Sandy Berger by January 1, 2001. A memo recommending this process is attached at Tab B.

B. Critical Infrastructure Protection Background:

- This discussion takes place at the heart of the bigger issue of Response, Recovery and Reconstitution (R3) of Critical Infrastructures.
- R3, and reconstitution in particular, has a significant political downside – any attempt at defining government's role in reconstituting the

information network brings up the issue of regulating the Internet. Note, however, that merely ensuring a mechanism to preserve preferential government access to Internet-based communications may raise some of the same concerns.

- Dick Clarke met previously with Jerry Epstein and Terry Kelly, and agreed that the NS/EP communications convergence piece should be addressed first, and the larger issues of R3 dealt with later. In reality, they are on a somewhat parallel track.
- Finally, EO 12472 (appropriate areas highlighted) atTab B gives the OSTP, NSC and OMB oversight over NS/EP Communications. These EOP offices have taken a less than active role in this process so far. The proposed Task Force is seen by Clarke and his staff as an opportunity to reassert EOP oversight over the process.
- You should keep this discussion focused on Network Convergence and the proposed process for addressing it – divergence into the larger issue of R3 could bring up specters of government regulation of the Internet, and doom this very important process.

III. Participants

Neal Lane
Richard Clarke
Josh Gotbaum (tentative)
Gerald Epstein
Jeffrey Hunker (Clarke's staff)
Terry Kelly
Other NSC staff

Attachments

Tab A	Talking Points
Tab B	Memo on the Convergence Task Force
Tab C	EO 12472, Highlighted to indicate OSTP and NSC roles

POINTS TO BE MADE FOR MEETING WITH
RICHARD CLARKE
SENIOR DIRECTOR, TRANSNATIONAL THREATS, NSC
AND AN OMB REP (possibly JOSH GOTBAUM)

- Convergence raises some crucial technology and policy issues regarding preservation of NS/EP communications, and this task force is timely and needed.

- I want the task force to get off the ground as quickly as possible, to examine the spectrum of issues as laid out in the memo, and provide a report and recommendations that we can begin implementing, and pass on to the next administration – this should be a pretty non-partisan issue.

- Given how sensitive the issue of any government involvement in the Internet is, recommend we highlight the fact that Emergency Preparedness telecom needs are widely recognized (e.g. in the EU and Japan) as needed for public health and safety, should the topic be raised in public fora.

10/12/00

DRAFT

MEMORANDUM FOR DISTRIBUTION

SUBJECT: 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 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 will convene a Convergence Task Force (CTF) to identify the policy, legal, technical, and security issues of convergence, 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.

We ask that you designate a representative who is able to speak on behalf of your agency to participate 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, Senior National Security Officer, or Dr. Jeffrey Hunker, Senior Director for Critical Infrastructure, 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
for Science and Technology

Distribution:
Secretary of Defense
Secretary of Commerce
Administrator, GSA
Director, FEMA

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

[Executive Orders]

Executive Order 12472--Assignment of national security and emergency preparedness telecommunications functions

NOTE: The National Communications System [NCS] was established by Executive Order (EO) 12472 as a Federal interagency group assigned national security and emergency preparedness (NS/EP) telecommunications responsibilities throughout the full spec-trum of emergencies. Under the policy objectives stated in EO 12472 and National Security Decision Directive (NSDD) 97, these responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve measurable improvements in survivability, interoperability, and operational effectiveness under all conditions and seeking greater effectiveness in managing and using national telecommunication resources to support the Government during any emergency.

In order to accomplish these responsibilities, the NCS must:

- *Increase survivability and interoperability of NS/EP telecommunications*
- *Provide connectivity augmentation for the public switched network (PSN)*
- *Develop a NS/EP telecommunications architecture responsive to current and future needs of the Federal Government*
- *Develop telecommunications technical and procedural standards*
- *Provide technical and analytical expertise to the National Security Telecommunications Advisory Committee (NSTAC) and subordinate groups*
- *Provide planning assistance and technical analysis to the Committee of Principals (COP) and the Council of Representatives (COR)*
- *Perform NS/EP telecommunications network performance analysis*
- *Ensure interoperability of Integrated Services Digital Networks (ISDNs)*
- *Develop emergency operations training and exercises*
- *Develop and manage NS/EP automated systems and capabilities*
- *Improve capabilities to predict impacts of natural disasters on telecommunications*
- *Analyze technological advances such as digital cellular, advanced intelligent networks (AIN), commercial satellite technologies, and wireless technologies to identify potential impacts on NS/EP telecommunications*

By the authority vested in me as President by the Constitution and laws of the United States of America, including the Communications Act of 1934, as amended (47 U.S.C.

151), the National Security Act of 1947, as amended, the Defense Production Act of 1950, as amended (50 U.S.C. App. 2061), the Federal Civil Defense Act of 1950, as amended (50 U.S.C. App. 2251), the Disaster Relief Act of 1974 (42 U.S.C. 5121), Section 5 of Reorganization Plan No. 1 of 1977 (3 C.F.R. 197, 1978 Comp.1), and Section 203 of Reorganization Plan No. 3 of 1978 (3 C.F.R. 389, 1978 Comp.2), and in order to provide for the consolidation of assignment and responsibility for improved execution of national security and emergency preparedness telecommunications functions, it is hereby ordered as follows:

Section 1. The National Communications System.

(a) There is hereby established the National Communications System (NCS). The NCS shall consist of the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals and the Manager. The NCS Committee of Principals shall consist of representatives from those Federal departments, agencies or entities, designated by the President, which lease or own telecommunications facilities or services of significance to national security or emergency preparedness, and, to the extent permitted by law, other Executive entities which bear policy, regulatory or enforcement responsibilities of importance to national security or emergency preparedness telecommunications capabilities.

(b) The mission of the NCS shall be to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in:

(1) the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this Order; and

(2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.

(c) The NCS shall seek to ensure that a national telecommunications infrastructure is developed which:

(1) Is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of

government;

(2) Is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources;

(3) Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency; and

(4) Is consistent, to the maximum extent practicable, with other national telecommunications policies.

(d) To assist in accomplishing its mission, the NCS shall:

(1) serve as a focal point for joint industry-government national security and emergency preparedness telecommunications planning; and

(2) establish a joint industry-government National Coordinating Center which is capable of assisting in the initiation, coordination, restoration and reconstitution of national security or emergency preparedness telecommunications services or facilities under all conditions of crisis or emergency.

(e) The Secretary of Defense is designated as the Executive Agent for the NCS. The Executive Agent shall:

(1) Designate the Manager of the NCS;

(2) Ensure that the NCS conducts unified planning and operations, in order to coordinate the development and maintenance of an effective and responsive capability for meeting the domestic and international national security and emergency preparedness telecommunications needs of the Federal government;

(3) Ensure that the activities of the NCS are conducted in conjunction with the emergency management activities of the Federal Emergency Management Agency;

(4) Recommend, in consultation with the NCS Committee of Principals, to the National Security Council, the Director of the Office of Science and Technology Policy, or the Director of the Office of Management and Budget, as appropriate:

a. The assignment of implementation or other responsibilities to NCS member entities;

b. New initiatives to assist in the exercise of the functions specified in Section 2; and

c. Changes in the composition or structure of the NCS;

(5) Oversee the activities of and provide personnel and administrative support to the Manager of the NCS;

(6) Provide staff support and technical assistance to the National Security Telecommunications Advisory Committee established by Executive Order No. 12382, as amended; and

(7) Perform such other duties as are from time to time assigned by the President or his authorized designee.

(f) The NCS Committee of Principals shall:

(1) Serve as the forum in which each member of the Committee may review, evaluate, and present views, information and recommendations concerning ongoing or prospective national security or emergency preparedness telecommunications programs or activities of the NCS and the entities represented on the Committee;
(2) Serve as the forum in which each member of the Committee shall report on and explain ongoing or prospective telecommunications plans and programs developed or designed to achieve national security or emergency preparedness telecommunications objectives;
(3) Provide comments or recommendations, as appropriate, to the National Security Council, the Director of the Office of Science and Technology Policy, the Director of the Office of Management and Budget, the Executive Agent, or the Manager of the NCS, regarding ongoing or prospective activities of the NCS; and

(4) Perform such other duties as are from time to time assigned by the President or his authorized designee.

(g) The Manager of the NCS shall:

(1) Develop for consideration by the NCS Committee of Principals and the Executive Agent:

a. A recommended evolutionary telecommunications architecture designed to meet current and future Federal government national security and emergency preparedness telecommunications requirements;

b. Plans and procedures for the management, allocation and use, including the establishment of priorities or preferences, of Federally owned or leased telecommunications assets under all conditions of crisis or emergency;

c. Plans, procedures and standards for minimizing or removing technical impediments to the interoperability of government-owned and/or commercially-provided telecommunications systems;

d. Test and exercise programs and procedures for the evaluation of the capability of the Nation's telecommunications resources to meet national security or emergency preparedness telecommunications requirements; and

e. Alternative mechanisms for funding, through the budget review process, national security or emergency preparedness telecommunications initiatives which benefit multiple Federal departments, agencies, or entities. Those mechanisms recommended by the NCS Committee of Principals and the Executive Agent shall be submitted to the Director of the Office of Management and Budget.

(2) Implement and administer any approved plans or programs as assigned, including any system of priorities and preferences for the provision of communications service, in consultation with the NCS Committee of Principals and the Federal

Communications Commission, to the extent practicable or otherwise required by law or regulation;

(3) Chair the NCS Committee of Principals and provide staff support and technical assistance thereto;

(4) Serve as a focal point for joint industry-government planning, including the dissemination of technical information, concerning the national security or emergency preparedness telecommunications requirements of the Federal government;

(5) Conduct technical studies or analyses, and examine research and development programs, for the purpose of identifying, for consideration by the NCS Committee of Principals and the Executive Agent, improved approaches which may assist Federal entities in fulfilling national security or emergency preparedness telecommunications objectives;

(6) Pursuant to the Federal Standardization Program of the General Services Administration, and in consultation with other appropriate entities of the Federal government including the NCS Committee of Principals, manage the Federal Telecommunications Standards Program, ensuring wherever feasible that existing or evolving industry, national, and international standards are used as the basis for Federal telecommunications standards; and

(7) Provide such reports and perform such other duties as are from time to time assigned by the President or his authorized designee, the Executive Agent, or the NCS Committee of Principals. Any such assignments of responsibility to, or reports made by, the Manager shall be transmitted through the Executive Agent.

Sec. 2. Executive Office Responsibilities.

(a) Wartime Emergency Functions.

(1) The National Security Council shall provide policy direction for the exercise of the war power functions of the President under Section 606 of the Communications Act of 1934, as amended (47 U.S.C. 606), should the President issue implementing instructions in accordance with the National

Emergencies Act (50 U.S.C. 1601).

(2) The Director of the Office of Science and Technology Policy shall direct the exercise of the war power functions of the President under Section 606(a), (c)-(e), of the Communications Act of 1934, as amended (47 U.S.C. 606), should the President issue implementing instructions in accordance with the National Emergencies Act (50 U.S.C. 1601).

(b) Non-Wartime Emergency Functions.

(1) The National Security Council shall:

a. Advise and assist the President in coordinating the development of policy, plans, programs and standards within the Federal government for the identification, allocation, and use of the Nation's telecommunications resources by the Federal government, and by State and local governments, private industry and volunteer organizations upon request, to the extent practicable and otherwise consistent with law, during those crises or emergencies in which the exercise of the President's war power functions is not required or permitted by law; and

b. Provide policy direction for the exercise of the President's non-wartime emergency telecommunications functions, should the President so instruct.

(2) The Director of the Office of Science and Technology Policy shall provide information, advice, guidance and assistance, as appropriate, to the President and to those Federal departments and agencies with responsibilities for the provision, management, or allocation of telecommunications resources, during those crises or emergencies in which the exercise of the President's war power functions is not required or permitted by law;

(3) The Director of the Office of Science and Technology Policy shall establish a Joint Telecommunications Resources Board (JTRB) to assist him in the exercise of the functions specified in this subsection. The Director of the Office of Science and

Technology Policy shall serve as chairman of the JTRB; select those Federal departments, agencies, or entities which shall be members of the JTRB; and specify the functions it shall perform.

(c) Planning and Oversight Responsibilities.

(1) The National Security Council shall advise and assist the President in:

a. Coordinating the development of policy, plans, programs and standards for the mobilization and use of the Nation's commercial, government, and privately owned telecommunications resources, in order to meet national security or emergency preparedness requirements;

b. Providing policy oversight and direction of the activities of the NCS; and

c. Providing policy oversight and guidance for the execution of the responsibilities assigned to the Federal departments and agencies by this Order.

(2) The Director of the Office of Science and Technology Policy shall make recommendations to the President with respect to the test, exercise and evaluation of the capability of existing and planned communications systems, networks or facilities to meet national security or emergency preparedness requirements and report the results of any such tests or evaluations and any recommended remedial actions to the President and to the National Security Council;

(3) The Director of the Office of Science and Technology Policy or his designee shall advise and assist the President in the administration of a system of radio spectrum priorities for those spectrum dependent telecommunications resources of the Federal government which support national security or emergency preparedness functions. The Director also shall certify or approve priorities for radio spectrum use by the Federal government, including the resolution of any conflicts in or among priorities, under all conditions of crisis or emergency; and

(4) The National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget shall, in consultation with the Executive Agent for the NCS and the NCS Committee of Principals, determine what constitutes national security and emergency preparedness telecommunications requirements.

(d) Consultation with Federal Departments and Agencies. In performing the functions assigned under this Order, the National Security Council and the Director of the Office of Science and Technology Policy, in consultation with each other, shall:

(1) Consult, as appropriate, with the Director of the Office of Management and Budget; the Director of the Federal Emergency Management Agency with respect to the emergency management responsibilities assigned pursuant to Executive Order No. 12148, as amended; the Secretary of Commerce, with respect to responsibilities assigned pursuant to Executive Order No. 12046; the Secretary of Defense, with respect to communications security responsibilities assigned pursuant to Executive Order No. 12333; and the Chairman of the Federal Communications Commission or his authorized designee; and

(2) Establish arrangements for consultation among all interested Federal departments, agencies or entities to ensure that the national security and emergency preparedness communications needs of all Federal government entities are identified; that mechanisms to address such needs are incorporated into pertinent plans and procedures; and that such needs are met in a manner consistent, to the maximum extent practicable, with other national telecommunications policies.

(e) Budgetary Guidelines. The Director of the Office of Management and Budget, in consultation with the National Security Council and the NCS, will prescribe general guidelines and procedures for reviewing the financing of the NCS within the budgetary process and for preparation of budget estimates by participating agencies. These guidelines and procedures may provide for mechanisms for funding, through the budget review process, national security and emergency preparedness telecommunications initiatives which benefit multiple Federal departments, agencies, or entities.

Sec. 3. Assignment of Responsibilities to Other Departments and Agencies.

In order to support and enhance the capability to satisfy the national security and emergency preparedness telecommunications needs of the Federal government, State and local governments, private industry and volunteer organizations, under all circumstances including those of crisis or emergency, the Federal departments and agencies shall perform the following functions:

(a) Department of Commerce. The Secretary of Commerce shall, for all conditions of crisis or emergency:

(1) Develop plans and procedures concerning radio spectrum assignments, priorities and allocations for use by Federal departments, agencies and entities; and
(2) Develop, maintain and publish policy, plans, and procedures for the control and allocation of frequency assignments, including the authority to amend, modify or revoke such assignments, in those parts of the electromagnetic spectrum assigned to the Federal government.

(b) Federal Emergency Management Agency. The Director of the Federal Emergency Management Agency shall:

(1) Plan for and provide, operate and maintain telecommunications services and facilities, as part of its National Emergency Management System, adequate to support its assigned emergency management responsibilities;

(2) Advise and assist State and local governments and volunteer organizations, upon request and to the extent consistent with law, in developing plans and procedures for identifying and satisfying their national security or emergency preparedness telecommunications requirements;

(3) Ensure, to the maximum extent practicable, that national security and emergency preparedness telecommunications planning by State and local governments and volunteer organizations is mutually supportive and consistent with the planning of the Federal government; and

(4) Develop, upon request and to the extent consistent with law and in consonance with regulations promulgated by and

agreements with the Federal Communications Commission, plans and capabilities for, and provide policy and management oversight of, the Emergency Broadcast System, and advise and assist private radio licensees of the Commission in developing emergency communications plans, procedures and capabilities.

(c) Department of State. The Secretary of State, in accordance with assigned responsibilities within the Diplomatic Telecommunications System, shall plan for and provide, operate and maintain rapid, reliable and secure telecommunications services to those Federal entities represented at United States diplomatic missions and consular offices overseas. This responsibility shall include the provision and operation of domestic telecommunications in support of assigned national security or emergency preparedness responsibilities.

(d) Department of Defense. In addition to the other responsibilities assigned by this Order, the Secretary of Defense shall:

(1) Plan for and provide, operate and maintain telecommunications services and facilities adequate to support the National Command Authorities and to execute the responsibilities assigned by Executive Order No. 12333; and

(2) Ensure that the Director of the National Security Agency provides the technical support necessary to develop and maintain plans adequate to provide for the security and protection of national security and emergency preparedness telecommunications.

(e) Department of Justice. The Attorney General shall, as necessary, review for legal sufficiency, including consistency with the antitrust laws, all policies, plans or procedures developed pursuant to responsibilities assigned by this Order.

(f) Central Intelligence Agency. The Director of Central Intelligence shall plan for and provide, operate, and maintain telecommunications services adequate to support its assigned responsibilities, including the dissemination of intelligence within the Federal government.

(g) General Services Administration. Except as otherwise assigned by this Order, the Administrator of General Services, consistent with policy guidance provided by the Director of the Office of Management and Budget, shall ensure that Federally owned or managed domestic

communications facilities and services meet the national security and emergency preparedness requirements of the Federal civilian departments, agencies and entities.

(h) Federal Communications Commission. The Federal Communications Commission shall, consistent with Section 4(c) of this Order:

(1) Review the policies, plans and procedures of all entities licensed or regulated by the Commission that are developed to provide national security or emergency preparedness communications services, in order to ensure that such policies, plans and procedures are consistent with the public interest, convenience and necessity;

(2) Perform such functions as required by law with respect to all entities licensed or regulated by the Commission, including (but not limited to) the extension, discontinuance or reduction of common carrier facilities or services; the control of common carrier rates, charges, practices and classifications; the construction, authorization, activation, deactivation or closing of radio stations, services and facilities; the assignment of radio frequencies to Commission licensees; the investigation of violations of pertinent law and regulation; and the initiation of appropriate enforcement actions;

(3) Develop policy, plans and procedures adequate to execute the responsibilities assigned in this Order under all conditions or crisis or emergency; and

(4) Consult as appropriate with the Executive Agent for the NCS and the NCS Committee of Principals to ensure continued coordination of their respective national security and emergency preparedness activities.

(i) All Federal departments and agencies, to the extent consistent with law (including those authorities and responsibilities set forth in Section 4(c) of this Order), shall:

(1) Determine their national security and emergency preparedness telecommunications requirements, and provide information regarding such requirements to the Manager of the NCS;

(2) Prepare policies, plans and procedures concerning telecommunications facilities, services or equipment under their management or operational control to maximize their capability of responding to the national security or emergency preparedness needs of the Federal government;

(3) Provide, after consultation with the Director of the Office of Management and Budget, resources to support their respective requirements for national security and emergency preparedness telecommunications; and provide personnel and staff support to the Manager of the NCS as required by the President;

(4) Make information available to, and consult with, the Manager of the NCS regarding agency telecommunications activities in support of national security or emergency preparedness;

(5) Consult, consistent with the provisions of Executive Order No. 12046, as amended, and in conjunction with the Manager of the NCS, with the Federal Communications Commission regarding execution of responsibilities assigned by this Order;
(6) Submit reports annually, or as otherwise requested, to the Manager of the NCS, regarding agency national security or emergency preparedness telecommunications activities; and

(7) Cooperate with and assist the Executive Agent for the NCS, the NCS Committee of Principals, the Manager of the NCS, and other departments and agencies in the execution of the functions set forth in this Order, furnishing them such information, support and assistance as may be required.

(j) Each Federal department or agency shall execute the responsibilities assigned by this Order in conjunction with the emergency management activities of the Federal Emergency Management Agency, and in regular consultation with the Executive Agent for the NCS and the NCS Committee of Principals to ensure continued coordination of NCS and individual agency telecommunications activities.

Sec. 4. General Provisions.

(a) All Executive departments and agencies may issue such rules and

regulations as may be necessary to carry out the functions assigned under this Order.

(b) In order to reflect the assignments of responsibility provided by this Order,

(1) Sections 2-414, 4-102, 4-103, 4-202, 4-302, 5-3, and 6-101 of Executive Order No. 12046, as amended, are revoked;

(2) The Presidential Memorandum of August 21, 1963, as amended, entitled "Establishment of the National Communications System", is hereby superseded; and

(3) [Deleted]

(c) Nothing in this Order shall be deemed to affect the authorities or responsibilities of the Director of the Office of Management and Budget, or any Office or official thereof; or reassign any function assigned any agency under the Federal Property and Administrative Services Act of 1949, as amended; or under any other law; or any function vested by law in the Federal Communications Commission.
[Sec. 4(b)(3) amends Executive Order 12046 of Mar. 27, 1978, Chapter 47. The amendment has been incorporated into that order.]

Sec. 5. This Order shall be effective upon publication in the Federal Register.3

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

DEFENSE SCIENCE BOARD BRIEFING
DATE: SEPTEMBER 26, 2000
TIME: 1:30 PM – 3:30 PM
LOCATION: ROOM 422

FROM: GERALD EPSTEIN

I. Origin of the Action

The Defense Science Board completed three summer studies in areas of interest to OSTP. I had asked DSB to come by to brief us on these studies. The chairs of each of the summer studies will be briefing us on Responding to Biological Terrorism, Unconventional Nuclear Threats (e.g., smuggled weapons), and Information Operations. Craig Fields, Chairman of the Defense Science Board, will be accompanying them.

II. Background

I briefed the Unconventional Nuclear Threats Panel on the Weapons of Mass Destruction Group's R&D Subgroup. However, that group has been concentrating on chemical and biological threats; we have not devoted much effort to date on the nuclear threat. The DSB has conducted previous summer studies on the biological threat and on information operations. I am not aware of work they have done recently on unconventional nuclear attack.

Craig Fields, the Chairman of the DSB, was appointed in December 1994 and reappointed in January 1997; he is a former Director of DARPA. Roger Hagengruber is a Vice President of Sandia National Laboratory; I do not know the affiliation or respective summer studies for the other participants.

III. Participants

DSB	Craig Fields, DSB Chairman
	Roger Hagengruber, chairman, Unconventional Nuclear Threats study
	Brian Hughes
	Robert Jamison

09/25/00

	George Poste
	Lawrence Wright
	Alan Rudolph
	Darr Lafon
OSTP	Gerald Epstein
	Terry Kelly
	Ed Hildebrand
	Vic Teplitz

Attachment
Tab A Talking Points

09/25/00

Talking Points for DSB Briefing

- Appreciate your coming to brief us today. All three of the studies I understand you will be describing today are areas that we are quite interested in, in our role as coordinators across the Executive Branch both for Weapons of Mass Destruction Preparedness R&D and for Critical Infrastructure Protection R&D.

- We have this room until 3:30, although I'm not sure I will be able to spend that long with you.

- I expect it will quite often be the case that a DSB Summer Study is of considerable interest here. It would certainly be helpful for us if, to the extent possible when you complete a study, that you give us a heads up. It may not always be the case that we are involved in that area, but I'm sure that there will be additional occasions where we would benefit greatly from your experience.

- Of course, we are also happy to provide whatever assistance we can as you conduct your studies

09/25/00

EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

WASHINGTON, D.C. 20502

DEFENSE SCIENCE BOARD BRIEFING
DATE: SEPTEMBER 26, 2000
TIME: 1:30 PM – 3:30 PM
LOCATION: ROOM 422

FROM: GERALD EPSTEIN

I. Origin of the Action

The Defense Science Board completed three summer studies in areas of interest to OSTP. I had asked DSB to come by to brief us on these studies. The chairs of each of the summer studies will be briefing us on Responding to Biological Terrorism, Unconventional Nuclear Threats (e.g., smuggled weapons), and Information Operations. Craig Fields, Chairman of the Defense Science Board, will be accompanying them.

II. Background

I briefed the Unconventional Nuclear Threats Panel on the Weapons of Mass Destruction Group's R&D Subgroup. However, that group has been concentrating on chemical and biological threats; we have not devoted much effort to date on the nuclear threat. The DSB has conducted previous summer studies on the biological threat and on information operations. I am not aware of work they have done recently on unconventional nuclear attack.

Craig Fields, the Chairman of the DSB, was appointed in December 1994 and reappointed in January 1997; he is a former Director of DARPA. Roger Hagengruber is a Vice President of Sandia National Laboratory; I do not know the affiliation or respective summer studies for the other participants.

III. Participants

DSB	Craig Fields, DSB Chairman Roger Hagengruber, chairman, Unconventional Nuclear Threats study Brian Hughes Robert Jamison

09/25/00

George Poste
Lawrence Wright
Alan Rudolph
Darr Lafon

OSTP

Gerald Epstein
Terry Kelly
Ed Hildebrand
Vic Teplitz

Attachment
Tab A Talking Points

09/25/00

A

Talking Points for DSB Briefing

- Appreciate your coming to brief us today. All three of the studies I understand you will be describing today are areas that we are quite interested in, in our role as coordinators across the Executive Branch both for Weapons of Mass Destruction Preparedness R&D and for Critical Infrastructure Protection R&D.

- We have this room until 3:30, although I'm not sure I will be able to spend that long with you.

- I expect it will quite often be the case that a DSB Summer Study is of considerable interest here. It would certainly be helpful for us if, to the extent possible when you complete a study, that you give us a heads up. It may not always be the case that we are involved in that area, but I'm sure that there will be additional occasions where we would benefit greatly from your experience.

- Of course, we are also happy to provide whatever assistance we can as you conduct your studies

09/25/00

cc: Kelly Epstein

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

REMARKS AT NSTAC CHAIR CHANGE CEREMONY
DATE: SEPTEMBER 25, 2000
TIME:5:00 – 5:30
LOCATION:ROOSEVELT ROOM

FROM: GERALD EPSTEIN

I. Origin of the Action

Dick Clarke, as the EOP focal point for the National Security Telecommunications Advisory Committee (NSTAC), has pulled this event together to emphasize the importance of the NSTAC and the role these CEOs play.

II. Background

The NSTAC was founded after the divestiture of ATT to ensure that a single body could represent the private sector telecommunication providers on issues of National Security and Emergency Preparedness (NS/EP). NSTAC is a Presidentially appointed FACA committee that is composed almost exclusively of CEOs of major telecommunication and related companies who dedicate resources to work with the government to ensure NS/EP Communications are available. The Secretary of Defense is the executive agent for NS/EP communications, and the National Communications System (NCS) provides staff support for the NSTAC. Over the past several years, membership on NSTAC has broadened from the original long-haul telecommunications providers to include firms such as Microsoft and Cisco that are major providers of information technology hardware, software, and services.

This ceremony is to recognize the service of the outgoing chair of the NSTAC, Van Hunnicutt, CEO of Computer Sciences Corporation (CSC), and welcome the incoming chair, Dan Burnham, CEO of Raytheon. Sandy Berger will preside, and you will be asked to speak for five minutes (see talking points at Tab A). This change of leadership ceremony provides an opportunity to note the change in the telecommunications sector, and the NS/EP telecommunications mission, as the telecommunications network merges with the information network, and as

we take a broader view of the full breadth of information services that may be required by the NS/EP community.

III. Agenda

The formal agenda has not yet been published, but will follow the general outline below

Opening remarks	Sandy Berger
Remarks	Van Hunnicutt
Remarks	Dan Burnham
Remarks	Neal Lane
Closing remarks	Sandy Berger

We will provide you with a copy of the formal agenda and list of participants as soon as we receive them from the NSC.

Attachments
Tab A Talking Points

Talking Points for the NSTAC Chair Turn-over

- I am very happy to be here to thank Van for the great work he has done while NSTAC Chair, and to welcome Dan – I am looking forward to working with you.

- The NSTAC has filled an absolutely critical role, not only as the owners and operators of the vast telecommunications, and increasingly Internet-based infrastructures that we rely on to perform critical communications functions during national emergencies, but also as the supplier of invaluable technical expertise and the source of great ideas for what our S&T community needs to focus on.

- The President and I both recognize the commitment that the NSTAC members have made in resources and your personal time to provide advice on these very important issues. It is greatly appreciated.

- Your Widespread Outage Report from 1997 woke many people up to new threats to our telecommunications infrastructure. Your Impact Task Force Report on Convergence of the Voice and Data networks clearly laid out the scope of both the technical and policy challenges we face as we enter a truly digital communications landscape. And your efforts on technology transfer – to include the Task Force Meeting on R&D Exchange we are jointly hosting in Tulsa Thursday and Friday – are great examples of public/private cooperation and partnership. These all make clear how vital your contribution has been and will continue to be for the future not only of National Security and Emergency Preparedness Communications, but for our future in a very technologically sophisticated world. These are only a few examples of the great service you have provided the President and the Nation – there are many many more that I do not have time to cover in detail.

- We will all continue to rely on you for help and guidance in this field where you bring such great knowledge and experience to the table – particularly in this period of rapid technological change. Indeed, this transition in NSTAC leadership is symbolic of the transition facing the entire telecommunications sector as our voice network and our data networks converge, and as NS/EP telecommunications requirements come to be viewed with a wider spectrum of information services.

- Let me close, then, by once again thanking you, Van, for your leadership and the contributions you have made. And, welcoming you, Dan – I have every confidence that the future of NSTAC under your leadership will be as bright and productive as it has been this past session.

09/22/00

T. Kelly
OSTP
6014

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

September 22, 2000

ACTION

MEMORANDUM FOR SAMUEL R. BERGER

THROUGH: RICHARD A. CLARKE

FROM: PAUL B. KURTZ

SUBJECT: National Security Telecommunications Advisory Committee (NSTAC) Chair Turnover - Scenario Paper

Please see attached scenario paper, remarks, and background material for the NSTAC chair turnover meeting at 5:00, September 25 in the Roosevelt Room.

The objective is to thank Computer Science Corporation's CEO Van Honeycutt for chairing NSTAC over the past two years and to welcome Raytheon's CEO Dan Burnham as the new chair.

The event should last 20 to 25 minutes.

Attachments
Tab A Scenario and Participants Paper
Tab B Remarks
Tab C Background Material on NSTAC

NSTAC Chair Turnover Scenario/Participants
September 25, 2000, 5:00 PM
The Roosevelt Room

Scenario:

5:00 SRB arrives in Roosevelt Room

5:05 SRB Welcomes Mr. Van Honeycutt and Mr. Dan Burnham using the attached remarks

- SRB presents plaque to Van thanking him for his service to NSTAC (photo)
- SRB presents ceremonial gavel to Mr. Burnham (photo)
- Offer Van and Dan opportunity to make remarks.

5:15 SRB calls on Rudy de Leon for comment

5:20 SRB calls on Neal Lane to close event

5:25 SRB departs

Participants:

Private Industry

Dan Burnham	CEO Raytheon, *incoming* NSTAC Chair
Van Honeycutt	CEO Computer Sciences Corporation (CSC), *outgoing* NSTAC Chair
John Grimes	Raytheon
Milt Cooper	CSC, President Federal Sector
Guy Copeland	CSC
Lawrence Shuman,	National Telecom Alliance
Margo Briggs	CEO ESAT

DOD

Rudy de Leon	Deputy Secretary of Defense
Linton Wells	Principal Deputy Assistant Secretary, OSD C3I

LTGEN Ruduege	Director Defense Information Service Agency (DISA), and Manager of National Communications System (NCS)
Diann McCoy	Deputy Manager NCS
Fred Herr	Division Chief, NCS
Capt Maldonado	Aide to LTGEN Rudeuge

OSTP

Neil Lane

NSC

Richard Clarke
Paul Kurtz

Dick Clarke's **NSTAC Remarks**

--I'M PLEASED TO BE HERE TODAY TO PRESIDE OVER THE CHANGE IN CHAIR OF THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE—"NSTAC." I WANT TO WELCOME VAN HONEYCUTT OF CSC, DAN BURNHAM OF RAYTHEON AND OUR OTHER DISTINGUISHED GUESTS.

--NSTAC'S MISSION IS CRITICAL TO OUR NATIONAL SECURITY. SINCE 1982, WHEN NSTAC WAS FORMED UNDER EXECUTIVE ORDER, SENIOR INDUSTRY LEADERS HAVE PROVIDED EXCELLENT ANALYSIS AND ADVICE TO THE PRESIDENT AND EXECUTIVE BRANCH ON NATIONAL SECURITY AND TELECOMMUNICATIONS.

--VAN HAS ABLY SERVED OUR NATION AS CHAIR OF NSTAC SINCE SEPTEMBER, 1998. PRIOR TO THAT VAN SERVED AS VICE CHAIR OF NSTAC FOR 2 YEARS.

-- NSTAC'S ACCOMPLISHMENTS UNDER VAN'S LEADERSHIP ARE NOTABLE. VAN LED INDUSTRY

EFFORTS TO FORM AN INFORMATION SHARING AND ANALYSIS CENTER TO MONITOR AND RESPOND TO CYBER THREATS. THIS WAS THE FIRST MONITORING CENTER WITH BOTH INDUSTRY AND GOVERNMENT PARTICIPATION.

--VAN ALSO HELPED ESTABLISH A GROUP IN NSTAC TO ADDRESS TELECOMMUNICATIONS ISSUES RELATED TO THE INTERNET AND LED NSTAC DURING A HIGHLY SUCCESSFUL Y2K TRANSITION.

ON BEHALF OF THE PRESIDENT I WANT TO THANK YOU VAN FOR YOUR DEDICATION AND PERSONAL SERVICE AND PRESENT YOU WITH THIS PLAQUE PREPARED BY THE NATIONAL COMMUNICATIONS SYSTEM.

(PRESENT PLAQUE TO VAN. PHOTO)

--DAN, YOU HAVE YOUR WORK CUT OUT FOR YOU. YOU -AND ALL OF US—NEED TO WORK IN INTERNET TIME, WHERE AN INTERNET YEAR IS JUST 2-3 MONTHS OF OLD 'BEFORE INTERNET TIME.'

--THE IT REVOLUTION HAS CREATED TREMENDOUS OPPORTUNITIES BUT, AS THE PRESIDENT HAS STATED, *"OUR FOES HAVE EXTENDED THE FIELDS OF BATTLE - FROM PHYSICAL SPACE TO CYBERSPACE... RATHER THAN INVADING OUR BEACHES OR LAUNCHING BOMBERS, THESE ADVERSARIES MAY ATTEMPT CYBER ATTACKS AGAINST OUR CRITICAL MILITARY SYSTEMS AND OUR ECONOMIC BASE."*

--A FEW MONTHS AGO A STUDENT IN THE PHILIPPINES LAUNCHED A COMPUTER VIRUS THAT IN JUST HOURS SPREAD THROUGH MORE THAN 10 MILLION COMPUTERS AND CAUSED BILLIONS OF DOLLARS IN DAMAGE. THIS ATTACK WAS NOT SOPHISTICATED. WE MUST EXPECT, PLAN, AND PREPARE FOR SIMILAR OR MORE SOPHISTICATED ATTACKS ON OUR TELECOMMUNICATIONS INFRASTRUCTURE.

--IN THIS NEW ENVIRONMENT OF BOTH OPPORTUNITY AND THREAT, NSTAC'S ROLE WILL BECOME EVEN MORE IMPORTANT.

--IN THE NEXT FEW YEARS WE EXPECT "CONVERGENCE" IN THE COMMUNICATIONS INDUSTRY. I UNDERSTAND IN THE INDUSTRY'S LEXICON—CONVERGENCE IS REFERRED TO AS "VOICE OVER IP" WITH VOICE COMMUNICATIONS CARRIED OVER THE INTERNET. WE EXPECT THIS ISSUE TO HAVE A SERIOUS IMPACT ON COMMUNICATIONS SYSTEMS RELATED TO OUR NATIONAL SECURITY. WITH CONVERGENCE, AS WELL AS OTHER TECHNICAL AND STRUCTURAL CHANGES IN THE TELECOMMUNICATIONS INDUSTRY, WE WILL RELY UPON YOU, DAN, AND NSTAC TO PROVIDE US WITH INDUSTRY'S BEST ADVICE AS TO HOW TO MAINTAIN RELIABLE, SECURE COMMUNICATIONS.

--DAN I THANK YOU FOR VOLUNTEERING FOR THIS IMPORTANT MISSION AND WISH YOU LUCK IN THIS ENDEAVOR.

--TO MARK THE BEGINNING OF YOUR TENURE AS CHAIR OF THE NSTAC I PRESENT YOU THIS GAVEL.

(PRESENT GAVEL TO DAN. PHOTO.)

OFFER VAN AND DAN OPPORTUNITY TO COMMENT.

--I WOULD LIKE TO CALL ON THE DEPUTY SECRETARY DE LEON FOR COMMENTS.

--TO CLOSE I CALL ON NEAL LANE TO MAKE SOME REMARKS. (end)

The President's National Security Telecommunications Advisory Committee (NSTAC)

FACT SHEET

Revised 8/4/00

RECENT & ACTIVE ISSUES

- ? Information Sharing
- ? Education, Training, and Awareness
- ? Network Convergence
- ? R&D Exchange
- ? Information Assurance
- ? Infrastructure Protection
- ? Cyber Security & Crime
- ? Network Security
- ? Widespread Telecommunications Service Outages
- ? Intrusion Detection
- ? National Coordinating Mechanism
- ? Telecommunications Legislation and Regulation
- ? Information Sharing and Analysis Center for Telecommunications

PREVIOUSLY ADDRESSED ISSUES

- ? Y2K Technology Problem
- ? NS/EP Implications of Internet Technologies
- ? National Information Infrastructure
- ? Information Systems Security
- ? Wireless Services
- ? Common Channel Signaling
- ? Telecommunications Facility Protection
- ? Telecommunications Electric Service Priority
- ? Enhanced Call Completion
- ? International NS/EP Telecommunications
- ? Telecommunications Systems Survivability
- ? Telecommunications Service Priority and Carrier Liability
- ? Physical Security
- ? Intelligent Networks
- ? Network Security Information Exchange
- ? Commercial Satellite Survivability
- ? National Telecommunications Management Structure
- ? Commercial Network Survivability
- ? Electromagnetic Pulse
- ? National Coordinating Center for Telecommunications

PURPOSE: The NSTAC provides industry-based analyses and recommendations to the President and the executive branch regarding policy and enhancements to national security and emergency preparedness (NS/EP) telecommunications.

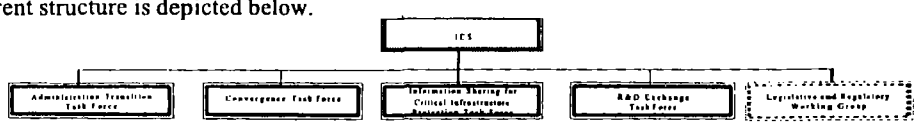
BACKGROUND: The President created the NSTAC by Executive Order (E.O.) 12382 in September 1982 to advise him on matters regarding NS/EP telecommunications. Four issues provided impetus for the establishment of the NSTAC: (1) divestiture of AT&T, (2) increased Government reliance on commercial communications, (3) potential impact of new technologies on NS/EP telecommunications, and (4) growing importance of command, control, and communications to military and disaster response modernization. The NSTAC is composed of up to 30 Presidentially appointed industry leaders (usually chief executive officers) representing various elements of the telecommunications industry (see reverse). In its advisory role to the President, the NSTAC provides industry-based analyses and recommendations on a wide range of policy and technical issues related to telecommunications, information systems, information assurance, infrastructure protection, and other NS/EP concerns. Having first met in 1982, the NSTAC meets approximately every 9 months to report on its activities and provide recommendations to the President.

LEADERSHIP: Assisting the President in NS/EP telecommunications matters are the Vice President; the Assistant to the President for National Security Affairs; the Secretary of Defense [designated as the Executive Agent, National Communications System (NCS)]; the Assistant to the President for Science and Technology; the Director, Office of Management and Budget; and the Manager, NCS/Director, Defense Information Systems Agency (designated as the NSTAC's Executive Secretary). The positions of NSTAC Chair and Vice Chair rotate among current members. Currently, the NSTAC Chair is Van B. Honeycutt, Chairman, President and CEO of Computer Sciences Corporation, and the Vice Chair is vacant.

NATIONAL COMMUNICATIONS SYSTEM: The President's NSTAC works cooperatively with the NCS, an interagency consortium of Federal departments and agencies that serves as a focal point for industry/Government NS/EP telecommunications planning. Originally created in 1963 as a result of critical communications delays during the Cuban Missile Crisis, the NCS was expanded in 1984 by E.O. 12472. The current membership includes 22 Government departments and agencies. The NCS coordinates and plans NS/EP telecommunications to support response to any crisis or disaster.

NSTAC ACTIVITIES AND ACCOMPLISHMENTS: Many NSTAC activities are the genesis for technical reports, recommendations to the President, and NS/EP operational programs. For example, the National Coordinating Center for Telecommunications (NCC), an industry/Government coordination center for day-to-day operational support to NS/EP telecommunications, began as an NSTAC recommendation. More recently, the NCC has established an Information Sharing and Analysis Center (ISAC) function as part of its NS/EP telecommunications mission. The Telecommunications Service Priority (TSP) System, once an NSTAC issue, is also now an operational program. TSP is the regulatory, administrative, and operational authority that enables priority provisioning and restoration of telecommunications services for Federal, State, and local government users, as well as nongovernmental users. Also originating from NSTAC activities, an industry-based Network Security Information Exchange (NSIE) was created and meets regularly with a Government NSIE to address the threat posed to the public network as a result of electronic exploitation of system vulnerabilities.

NSTAC'S INDUSTRY EXECUTIVE SUBCOMMITTEE (IES): The primary working body of the NSTAC is the IES, which consists of representatives appointed by each NSTAC Principal. The current structure is depicted below.



The IES holds regular working sessions to consider issues, analyses, or recommendations for presentation to the NSTAC. When an issue requires examination, the IES tasks the appropriate working group to address it. The Administration Transition Task Force will develop a White Paper to inform the next Administration about NSTAC. The Convergence Task Force addresses NS/EP implications related to the security and reliability of converged networks and the Next Generation Network (NGN). The Information Sharing for Critical Infrastructure Protection Task Force develops recommendations to facilitate further progress toward goals contained in Presidential Decision Directive 63. The R&D Exchange Task Force will help develop an agenda for a September 2000 event on the security and reliability of converged networks. The Legislative and Regulatory Working Group is active only when a task force asks it to examine the legal and regulatory aspects of a current issue.