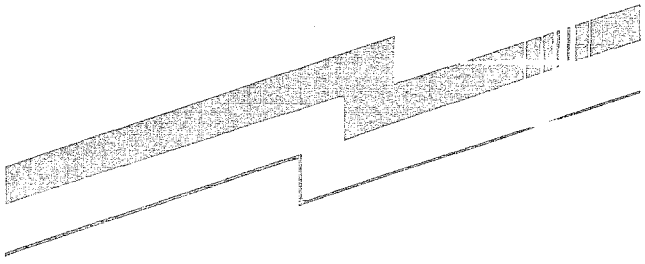

Network Security
Task Force
Report

Status Report of the Network Security Task Force for NSTAC XIII

August 1991

EXECUTIVE SUMMARY

The Network Security Task Force reports its accomplishments to date and describes plans to complete its assignment as scheduled for NSTAC XIV. The task force continues to work closely with Government entities responding to direction from the Policy Coordinating Committee on National Security Telecommunications and Information Systems.

Primary efforts have focused on identifying a mechanism for security information exchange concerning risks and remedies and recommmending steps to improve flow of Government information to industry about threat to the public switched network (PSN). The task force has established three activities: (1) a Network Security Information Exchange (NSIE) activity consisting of industry network security subject matter experts; (2) an Alert, Warning and Recovery activity providing "real time" notification to industry and Government about significant events regarding network security; and (3) an IES subcommittee to evaluate the above two activities and to contribute to task force conclusions and recommendations to NSTAC XIV. The industry NSIE is being established on a trial basis. The aim of the NSIE is to foster informal, collegial exchange of information -- some of it proprietary and sensitive -- concerning intrusions into software of the PSN that might (1) deny telecommunications service to national security and emergency preparedness (NS/EP) users, or (2) extract NS/EP-significant information. The Government has established a Federal NSIE to work in concert with the industry group. Although separate organizations, both groups will meet together regularly to exchange information on vulnerabilities, risks and trends. In event-driven situations, they will assist the alert/warning/ recovery activities to mitigate the effects of network security events on the PSN. Charters and membership lists for the two NSIEs are included in report appendices. The existing joint industry-Government National Coordinating Center (NCC) is supporting the Alert, Warning and Recovery activity, assisted by technical advice from NSIE members. Task force evaluation of the two activities will be undertaken after some experience on which to base recommendations to NSTAC XIV.

In a separate effort, the task force is in the process of addressing charges to recommend to Government R&D needed for commercially applicable tools and to comment on standards activities. Task force subgroup members have preliminarily identified six areas that need R&D and perhaps new standards to improve NS/EP telecommunications network security in the current PSN and in which the Government may have contributions to offer. A dialogue with Government has begun to determine what Federal Agencies/Departments have accomplished in the identified "need" areas and which Government developments might be commercially applied or adapted. In addition the task force is addressing the Generally Accepted System Security Principles (GSSP) concept recently proposed in a National Research Council report.

TABLE OF CONTENTS

SECTION 1 - INTRODUCTION

Since the National Security Telecommunications Advisory Committee (NSTAC) was established, several NSTAC task forces have addressed security of US telecommunications. In early 1990, Government requested that NSTAC address potential disruption of national security and emergency preparedness (NS/EP) telecommunications through manipulation of software in the public switched network (PSN). An NSTAC task force evaluated the vulnerability of the current PSN to intrusions that might (1) deny telecommunications service to NS/EP users, or (2) extract NS/EP-significant information.

The task force concluded recent intrusions into the PSN confirm "hackers" have significant capabilities to penetrate key switching and signalling system elements. Individual companies are aware and are taking action; the task force provided service suppliers with a checklist of steps that, when followed, would substantially enhance the security of their own networks. The task force reported that "until there is confidence that strong, comprehensive security programs are in place, the telecommunications industry should assume that a motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the PSN and monitor or disrupt the telecommunications serving NS/EP users."*

The NSTAC in December 1990 approved the task force report and directed a follow-on Network Security task force (see Membership in Appendix A) to complete the following for consideration by NSTAC XIV in mid-1992:

1) Identify a mechanism and provide an implementation plan for security information exchange concerning risks and remedies

2) Recommend steps to Government agencies that will improve the flow of Government information about threat to industry

3) Recommend to the Government research and development (R&D) needed for commercially applicable security tools, and

4) Evaluate existing industry-wide standards activities for network security and make recommendations.

The NSTAC charged the task force to work closely with, and in support of, the Government Network Security Subgroup (GNSS). The GNSS was established in 1990 by the Office of the Manager, National Communications System (OMNCS), responsive to direction from the Policy Coordinating Committee on National Security Telecommunications and Information Systems (PCC-NSTIS)**. The GNSS is chaired by the Deputy Manager of the NCS and has representatives from Federal departments, agencies, and other entities that have

---

* Report of the Network Security Task Force, November 1990, National Communications System, Arlington, VA, Executive Summary, page i.

** Memo, Chairman of the PCC-NSTIS to the Manager, NCS; April 23, 1990

particular responsibilities relevant to network security: the OMNCS; the Central Intelligence Agency (CIA); the Defense Intelligence Agency (DIA); the Federal Bureau of Investigation (FBI); the Federal Communications Commission (FCC); the General Services Administration (GSA); the National Institute of Standards and Technology (NIST); the National Security Agency (NSA); the National Security Council (NSC); the Office of Science and Technology Policy (OSTP); the Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence (OSD-C3I); and the United States Secret Service (USSS).

The purpose of this document is to report to NSTAC XIII the activities and accomplishments to date of the task force and describe task force plans to complete its assignment as scheduled for NSTAC XIV.

SECTION 2 - STATUS OF THE EFFORT

2.1 ESTABLISHMENT OF AN OPERATIONAL TRIAL OF SECURITY INFORMATION EXCHANGE

2.1.1 Task Force Approach

In addressing the first two tasks assigned by NSTAC -- that is, defining a mechanism for security information exchange and improving flow of information about threat -- the task force established three activities:

- A Network Security Information Exchange activity (NSIE) consisting of network security subject matter experts from operations and security divisions of service providers and vendors in industry.
- An Alert, Warning and Recovery activity providing "real time" notification to industry and Government about significant events regarding network security.
- An IES subcommittee, chaired by the Task Force Chairman, to evaluate the above two activities and to contribute to task force conclusions and recommendations to NSTAC XIV.

Prior to establishing these activities, the task force deliberated the functions to be performed, information to be exchanged, and constraints that must be dealt with. In February a subgroup was authorized to explore options for implementing an information exchange. Advised by the subgroup and OMNCS legal counsel, the task force, in coordination with the GNSS, chose to create an NSIE rapidly, on a trial basis, by establishing two separate NSIE organizations -- one of representatives from NSTAC member companies, the other of representatives from the GNSS. Although separate organizations, both groups will meet together regularly to exchange information on vulnerabilities, risks, and trends. In event-driven situations, they will assist the alert/warning/recovery activities to mitigate the effects of network security events on the PSN.

The industry NSIE is being established on a trial basis. The charter of the NSTAC, as an advisory body to the President, precludes establishment under the NSTAC of a permanent, standing operational entity. Experience with the trial NSIE should provide insight into an appropriate longterm solution.

The OMNCS and the GNSS, working closely with the task force, established a Federal Government NSIE to work in concert with the NSTAC NSIE. The resulting Government-industry liaison in joint NSIE activities is expected to improve the flow of threat information to industry, and keep Government in touch with efforts ongoing in industry to address network security.

Details of NSIE implementation were developed in concert with GNSS and OMNCS personnel, and unified crafting of complementary charters for Government and NSTAC NSIEs was completed within a few months.

A letter to IES members on 17 May announced the formation of the "initial/temporary" NSTAC NSIE as a means to respond to NSTAC tasking, and asked for responses by interested parties by 10 June. In coordination with the task force, the Funding and Regulatory Working Group developed nondisclosure agreements to protect proprietary information of NSTAC member companies who participate. The NSTAC NSIE was established under the aegis of the task force. In parallel, the Government NSIE was established under the aegis of the GNSS. An initial NSTAC NSIE meeting, held jointly with the Government NSIE, was held on June 25-6, 1991. A second meeting was held on September 11-12.

2.1.2 The Network Security Information Exchange.

In the NSTAC NSIE, eight NSTAC companies are providing one or two subject-matter experts in network operations and computer security. The aim is to foster informal, collegial exchange of information -- some of it proprietary and sensitive -- on threats, incidents, vulnerabilities, remedies and risks concerning software manipulation of the PSN. The NSIE will also periodically assess security of the PSN including trends, successes, and evolving threats. These activities will be carried out in periodic NSIE meetings, usually held jointly with the Government NSIE.

In another mode of operation, if a significant attack should take place on the PSN, or if such an attack appears imminent, the NSIE experts will convene to foster a concerted response by affected companies. Procedures for convening the group in real time are being developed.

For further detail about NSIE purpose and objectives, functions, membership and operating principles, see the Charter of the NSTAC NSIE, reproduced in Appendix B; the list of NSTAC NSIE Members in Appendix C; the Federal Government NSIE Charter, developed in concert with the NSTAC NSIE Charter, in Appendix D; and the Government Members in Appendix E.

2.1.3 Alert, Warning and Recovery.

The task force and GNSS agreed that the existing joint industry-Government National Coordinating Center (NCC) should support the real time function of protecting against significant attacks on network software. The NCC's mission is to assist in the initiation, coordination, restoration and reconstitution of NS/EP telecommunications services or facilities. It operates under the Manager, NCS, to provide for the rapid exchange of information and expedite NS/EP telecommunications responses. The NCC has assumed its role in the joint NSTAC/NCS approach to real time situations. Operating procedures have been defined for linking the NCC and NSIEs on occasions where network security-related notifications are involved.

2.2 PROGRESS ON R&D AND STANDARDS CHARGES

2.2.1 Task Force Approach

The task force sees the 3rd and 4th areas of their charge -- that is, recommending to Government R&D needed for commercially applicable tools and evaluating standards activities -- as so interrelated that they are best addressed together. Accordingly, the task force has determined it will pursue the following methodology:

- o Identify what network security areas need further R&D
- o Determine what is already being addressed by Government, and
- o Make recommendations on government R&D and on public network standards.

2.2.2 Identifying Areas of Need

Task force subgroup members have preliminarily identified areas that need R&D and perhaps new standards to improve NS/EP telecommunications network security in the current public switched network and in which the Government may have contributions to offer. A letter soliciting Government response was mailed on 18 June 1991 and a meeting with interested parties was held on 11 July 1991. A dialogue with Government has begun to determine what Federal Agencies/Departments have accomplished in the identified "need" areas and which Government developments might be commercially applied or adapted. Six areas initially proposed for discussion are:

1. Mechanisms for easy, portable control of access to a network element
2. A development to introduce an appropriate level of "suspicion" among trusted elements of the PSN
3. Solutions for reliable recovery from damage to software and databases: if you have a problem, how do you get well?
4. Means to adequately partition memory, or otherwise isolate network element software from databases that are more broadly accessed
5. Means to analyze all events in a network and highlight questionable situations, e.g. exception reports; and, at a broader level,
6. Tools to plan an architecture toward a long-term more secure network

In addition the task force is addressing a concept put forward in a recent National Research Council report*, that of Generally Accepted System Security Principles (GSSP).

---

* Computers at Risk, National Research Council, National Academy of Sciences, 1991.

SECTION 3 - PLANS FOR FUTURE TASK FORCE ACTIVITIES

The task force expects to complete its full assignment, including response in all four areas described on page 1, report its findings and make recommendations for consideration of the Principals at NSTAC XIV in the summer of 1992.

3.1. PLANS FOR NSIE AND OVERSIGHT ACTIVITIES

The task force believes that the first 4 meetings of the NSIE, expected to be completed by January or February of 1992, will provide a basis for deriving task force recommendations to the NSTAC's Industry Executive Subcommittee (IES) when they meet in late spring 1992. As the NSIE has met only twice so far, the task force has not yet undertaken to assess NSIE activities.

By the early months of 1992, the three IES members monitoring the NSIE will begin to assist the task force to formulate conclusions and recommendations about (1) whether an ongoing mechanism is needed for exchange of security information; and (2) if needed, what this mechanism should be.

The NSTAC NSIE will continue to operate until NSTAC XIV in the summer of 1992, when recommendations to the NSTAC Principals will be made and, if appropriate, recommendations to the President will be proposed. If requested to do so, the NSTAC NSIE may continue to operate for a limited period beyond that time to provide a transition to a more permanent arrangement.

3.2 PLANS FOR R&D AND STANDARDS ACTIVITIES

Based on the results from identifying areas where R&D is needed, the task force will foster contact with Government organizations having relevant information to offer. If perceived by Government and industry to have value over the next half year, the final task force report will recommend ways to continue productive interaction between Government and providers/ suppliers of public telecommunications beyond the lifetime of the task force. At this writing, further actions in the area of standards are under consideration.

APPENDIX A - NETWORK SECURITY TASK FORCE MEMBERSHIP

Unisys	Herb Benington, Chair
AT&T	Dave Bush
BELLCORE	Randy Schulz
Boeing	Bob Steele
COMSAT	Al Dayton
GE	Pat Glenn
GTE	Jim Moore
ITT	Joe Gancie
McCaw	Rick McElhenie
MCI	Joe Cassano
NTI	Jack Edwards
UTI	Jay Nelson

Others

CSC	John Tittle
GTE	Lowell Thomas
Harris	Bob Domino
Martin Marietta	John Hocker
NTI	Bob Petrie

APPENDIX B - NSTAC NSIE CHARTER - MAY 1991

Section I. ESTABLISHMENT

The NSTAC Network Security Information Exchange, hereinafter referred to as the NSIE, is established under the auspices of the Network Security Task Force of the President's National Security Telecommunications Advisory Committee (NSTAC). The date of initial activity is June 1991.

Section II. PURPOSE AND OBJECTIVES

The purpose of the NSIE is to provide a working forum to identify issues involving penetration or manipulation of software and databases affecting national security and emergency preparedness (NS/EP) telecommunications. In this NS/EP context, the NSIE will monitor network security in the public switched network (PSN). Two modes of operation will be followed. An immediate and event-driven mode will consist of reaction "in real time". Another mode, longer-term and more reflective, will be implemented by meeting on a periodic basis.

In reacting immediately in an event-driven manner, the NSIE objective is:

- To mitigate the effects of network security events on the PSN

In its longer-term mode of operation, the NSIE objectives are:

- To discuss and develop recommendations for reducing vulnerabilities
- To assess network risks
- To acquire threat and risk assessments from the Government
- To inform the Government of relevant risks
- To provide expertise to the NSTAC on which network security recommendations to the President can be based

Section III. FUNCTIONS

To meet its real time objectives, the NSIE shall:

- Assess, when alert and warning indications warrant, the potential for significant degradation of PSN services and recommend measures to reduce network impact

To meet its longer-term objectives, the NSIE shall:

- o Identify lessons learned (1) about process/procedures and (2) about technology/systems
- o Exchange information and views on:
  - Threats and incidents affecting the software elements of the PSN
  - Vulnerabilities of the PSN
  - Remedies, and
  - Consequent risks to NS/EP telecommunications
- o Recommend measures to reduce vulnerabilities of the PSN
- o Periodically assess NS/EP risks, including trends, international activities, and key uncertainties, and inform senior NSTAC and Government managers

Section IV. MEMBERSHIP

Members of the NSIE shall be NSTAC Member organizations. NSTAC Member organizations initially participating shall be chosen by the NSTAC's Network Security Task Force.

Each Member may appoint two individuals to participate in the NSIE, one as Regular Representative and the second as Alternate Representative. Representatives will be subject matter experts, e.g.:

- o Telecommunications organization employees who are engaged full time in the prevention, detection, and/or investigation of telecommunications network software penetration
- o Telecommunications organization employees who have security and investigative responsibilities as a secondary or collateral function.

Voting rights are accorded to each participating Member organization.

Section V. ORGANIZATION

The Members of the NSIE will elect a Chair and a Vice Chair. The Manager, National Communications System will serve as secretariat.

The Network Security Task Force, working with the National Coordinating Center (NCC), will develop initial operating procedures. These procedures may be modified on the basis of operational experience.

Section VI. OPERATING PRINCIPLES

The operating principles of the NSIE are as follows.

In operating in real time, i.e. providing subject matter expertise in event-driven situations, the NSIE will coordinate with the NCC as appropriate:

- NSIE points of contact for each company will be notified, by the company's NCC representative, of any pertinent information that has been provided to the NCC from other sources.

- Alternatively, the NSIE, or its representatives, can be the source of pertinent information that initiates NCC-related alert, warning and response procedures.

The operating principles for the longer term, i.e. in assembling on a periodic basis in a more reflective mode, will be as follows:

- Due to the sensitive nature of the information that may be discussed at NSIE meetings, attendance will be limited.

- Recording devices of any kind will not be permitted at NSIE meetings unless specifically authorized by the group.

- A nondisclosure arrangement will be needed among representatives and meeting attendees.

- Summary meeting notes will be prepared, will be marked proprietary as required by the content, and will be limited in distribution.

- In performing its functions the NSIE shall:

  - Invite the Government to participate as appropriate in assessing the potential for significant degradation of PSN services due to intrusion events

  - Regularly meet jointly with the Federal Government NSIE to exchange information on threats, vulnerabilities, remedies, and risks

- For NSIE meetings that are joint with the Government NSIE, the attendees and agendas will be jointly agreed to by the Chairs of the two groups.

The NSIE will operate within the requirements of all applicable state or Federal laws concerning the disclosure of information.

APPENDIX C - NSTAC NSIE MEMBERSHIP

UTI	G. Jay Nelson, Chair William Donsal Lewis
NTI	James Edward Fulford, Jr., Vice Chair Robert E. Petrie
AT&T	J.R. Dalton Robert C. Rencher, Jr.
Bellcore	Hank M. Kluepfel Carl G. Showalter
GTE	James E. Moake David A. Fiasco
Martin-Marietta	M. Duane Heidel
McCaw	Jack Farley
MCI	Robert E. Wilson Bruce A. Wells

APPENDIX D - FEDERAL GOVERNMENT NSIE CHARTER, 6/25/91

Section 1. ESTABLISHMENT

The Federal Government Network Security Information Exchange, hereinafter referred to as the NSIE, is a subordinate activity of the Government Network Security Subgroup. The Government Network Security Subgroup was established under the auspices of the Manager, National Communications System, in response to tasking from the National Security Council's Policy Coordinating Committee for National Security Telecommunications and Information Systems. The date of initial activity of the NSIE is June 1991.

The Government NSIE is meant to complement the NSIE of the President's National Security Telecommunications Advisory Committee (NSTAC). If the NSTAC NSIE is deactivated the need for continued operation of the Government's NSIE will be evaluated at that time.

Section II. PURPOSE AND OBJECTIVES

The purpose of the NSIE is to provide a working forum to identify issues involving penetration or manipulation of software and databases affecting national security and emergency preparedness (NS/EP) telecommunications. In this NS/EP context, the NSIE will assess and make recommendations concerning network security on the Public Switched Network (PSN). Two modes of operation will be followed. An immediate and event-driven mode will consist of reaction "in real time." Another mode, longer-term and more reflective, will be implemented by meeting on a periodic basis.

In reacting immediately in an event-driven manner, the NSIE objective is:

- To mitigate the effects of network security events on NS/EP needs served by the PSN.

In its longer-term mode of operation, the NSIE objectives are:

- To assess network risks and develop approaches for reducing vulnerabilities
- To provide threat, vulnerability and risk assessments based on information from Government sources to the NSTAC NSIE
- To acquire relevant risk information from the NSTAC NSIE
- To assist the NSTAC NSIE by providing expertise to the NSTAC on network security, and
- To provide advice to the Government Network Security Subgroup on network issues.

Section III. FUNCTIONS

To meet its real time objectives, the NSIE, separately or in coordination with the NSTAC NSIE, will:

- o Assess, when alert and warning indications warrant, the potential for significant degradation of PSN services to NS/EP needs and recommend approaches to reduce network impact on NS/EP needs.

To meet its longer-term objectives, the NSIE will:

- o Identify lessons learned about (1) processes/procedures and (2) technology/systems
- o Exchange information and views on:
  - Threats and incidents affecting the software elements of the PSN
  - Vulnerabilities of the PSN
  - Remedies, and
  - o Consequent risks to NS/EP telecommunications
- o Assess vulnerabilities of the PSN as they relate to NS/EP needs
- o Annually assess NS/EP risks, including trends, international activities, and key uncertainties, and inform the Government Network Security Subgroup, which will, as appropriate, make the assessment available to the NSTAC in support of its chartered responsibilities to advise the President on telecommunmications issues.

Section IV. MEMBERSHIP

Members of the NSIE shall be the Central Intelligence Agency (CIA); the Defense Intelligence Agency (DIA); the Federal Bureau of Investigation (FBI); the General Services Administration (GSA); the National Institute of Standards and Technology (NIST); the National Security Agency (NSA); the Office of the Manager, National Communications System (OMNCS); the Office of the Secretary of Defense for Command, Control, Communications and Intelligence (OSD-C3I); and the United States Secret Service (USSS). The Federal Communications Commission (FCC) will designate a nonvoting liaison representative to the NSIE to participate in meetings as appropriate wherein the exchange of information between the FCC and NSIE would be mutually beneficial.

Each Member may appoint up to two individuals, preferably with each representing a different functional group within the agency, to participate in the NSIE. Representatives will be subject matter experts, e.g.:

- o Federal organization employees who are engaged in the prevention, detection, and/or investigation of computer penetration, especially telecommunications network software penetration,

- o Federal organization employees who have telecommunications network security and investigative responsibilities as a secondary or collateral function.

Voting rights are accorded to each participating Member organization.

Section V. ORGANIZATION

The Members of the NSIE will elect a Chair and a Vice Chair. The Manager, National Communications System, will serve as secretariat.

The NSIE, working with the National Cooordinating Center (NCC), will develop initial operating procedures. These procedures may be modified on the basis of operational experience.

Section VI. OPERATING PRINCIPLES

The operating principles of the NSIE are as follows:

In operating in its real time mode, i.e., providing subject matter expertise in event-driven situations, the NSIE will coordinate with the NCC as appropriate:

- o NSIE points of contact for each Government organization will be notified by the NCC of any information judged pertinent that has been provided to the NCC from any other sources.

- o Alternatively, the NSIE or its representatives will provide to the NCC any pertinent information that could initiate NCC-related alert, warning and recovery procedures.

The operating principles for the longer term, i.e., in meeting on a periodic basis in a more reflective mode, will be as follows:

- o Due to the sensitive nature of the information that may be discussed at NSIE meetings, attendance will be limited.

- Recording devices of any kind will not be permitted at NSIE meetings unless specifically authorized by the group.

- In order to share and discuss industry proprietary and sensitive information, some form of nondisclosure arrangement may be needed among representatives and others attending the meetings.

- Summary meeting notes will be prepared, will be marked proprietary/classified as required by the content, and will be limited in distribution.

- In performing its functions the NSIE will:

  - Participate as appropriate with the NSTAC NSIE in assessing the potential for significant degradation of PSN services due to intrusion events, and

  - Regularly meet jointly with the NSTAC NSIE to exchange information on threats, vulnerabilities, remedies, and risks.

- For NSIE meetings that are joint with the NSTAC NSIE, the attendees and agendas will be jointly agreed to by the Chairs of the two groups.

The NSIE will operate within the requirements of all applicable Federal laws concerning the disclosure of information.

APPENDIX E - FEDERAL GOVERNMENT NSIE MEMBERSHIP

OMNCS	Frederick W. Herr, Chair
FBI	James C. Settle, Vice Chair
CIA	W. Allen Day
DIA	Stanley R. Young
GSA	George F. Flynn
OSD(C3I)	J. Robert Anderson
NIST	Dennis D. Steinauer
NSA	Robert A. Cavaluchi
USSS	Thomas R. Moyle Dave Boll