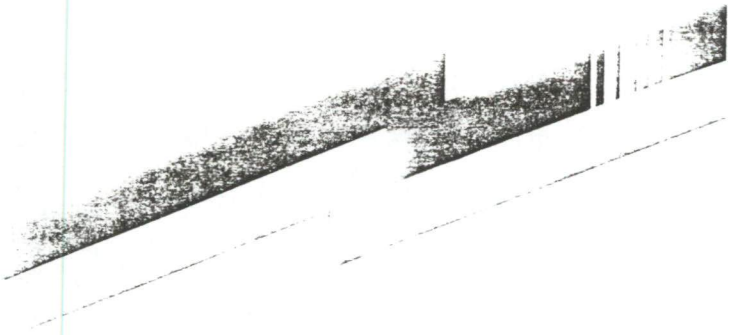


National Security
Telecommunications
Advisory Committee

DEC 15 1992

The President
The White House
Washington, D.C. 20500

Dear Mr. President:

Enclosed is the executive report from the fourteenth meeting of your National Security Telecommunications Advisory Committee (NSTAC XIV), held July 17, 1992. At our business session in the Old Executive Office Building, we received final reports from our Network Security and Enhanced Call Completion Task Forces and the NSTAC is forwarding recommendations to you regarding the Government's support of network security standards and the Government's potential use of enhanced call completion capabilities. Our Industry Executive Subcommittee (IES) also reported on its activities concerning backup power for Government-owned telecommunications equipment requiring Telecommunications Service Priority (TSP) and the IES' examination of the adequacy of Federal and state command center capabilities. In addition, the IES reported on its progress in assessing issues which the changing global environment could potentially generate with respect to National Security and Emergency Preparedness (NS/EP) telecommunications.

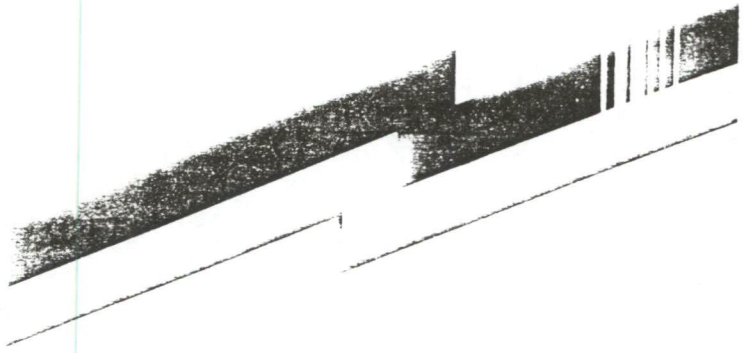
The NSTAC also met in executive session and received threat assessment briefings in the National Military Command Center from subject matter experts. We appreciate these high level briefings as they give us valuable national level perspectives that enable us to provide you with more informed advice regarding contemporary NS/EP telecommunications issues. The Committee also celebrated its tenth anniversary over a luncheon with General Scowcroft, and we very much appreciated his comments and recognition of the NSTAC's importance to the National Security Strategy and our contributions to strengthening National Security Policy.

On behalf of the NSTAC members, I would like to thank the Department of Defense staff for their interest and hospitality, and to commend the Executive Office of the President, and Lieutenant General Short, Manager, NCS, and his staff, for their most valuable and sustained support of the NSTAC process.

Finally, I want to take this opportunity to thank you, Mr. President, on behalf of all our current and former NSTAC members, for your strong leadership and support of our key NSTAC initiatives over the past years. Your endorsement of programs resulting from the NSTAC process have significantly enhanced our Nation's ability to communicate and respond to national crises and emergencies such as DESERT SHIELD/DESERT STORM and Hurricanes Andrew and Iniki. We gratefully wish you Godspeed in all your future endeavors.

Sincerely,

R.E. Allen,
Chairman



National Security
Telecommunications
Advisory Committee

DEC 15 1992

Honorable Brent Scowcroft
Assistant to the President for
National Security Affairs
The White House
Washington, D.C. 20500

Dear General Scowcroft:

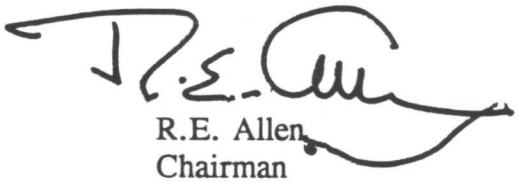
Enclosed is the executive report I am submitting from the fourteenth meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XIV), held July 17, 1992. Executive Order 12382 directs that NSTAC reports be submitted to the President and to the Secretary of Defense in his capacity as Executive Agent, National Communications System.

On behalf of the NSTAC members, I once again want to thank you for hosting the NSTAC Executive Session in the Indian Treaty Room, and for the time you took out of your busy schedule to help celebrate our tenth anniversary and recognize the NSTAC's importance to the National Security Strategy and its contributions to strengthening National Security Policy.

The NSTAC XIV Business Session resulted in approved final reports from its Network Security and Enhanced Call Completion Task Forces and recommendations to the President regarding the Government's support of network security standards and the Government's potential use of enhanced call completion capabilities. The NSTAC directed its Industry Executive Subcommittee (IES) to establish a Network Security Standards Oversight Group to work with the standards community and encourage development of network security standards for the public switched networks. The NSTAC also directed its IES to establish an ad hoc group to continue supporting the Government in developing its enhanced call completion requirements. The NSTAC's Energy Task Force efforts with Department of Energy and the National Communications System will be concluded and reported at NSTAC XV in May 1993.

The NSTAC appreciates the strong support, assistance, and cooperation it continues to receive from you and the National Security Council staff.

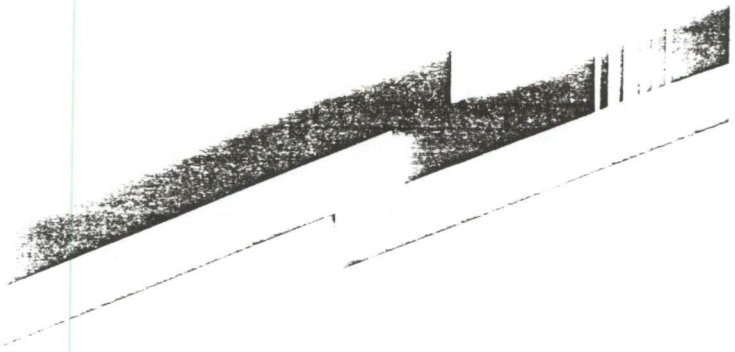
Sincerely,



R.E. Allen
Chairman

1 Enclosure:
NSTAC XIV Report to the President

Copy to:
NSTAC Members
LTG Short
COL Linhares



National Security
Telecommunications
Advisory Committee

DEC 15 1992

Honorable Richard B. Cheney
Secretary of Defense
The Pentagon
Washington, D.C. 20301

Dear Mr. Secretary:

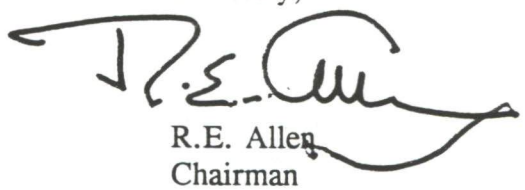
Enclosed is the executive report from the fourteenth meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XIV), held July 17, 1992. Executive Order 12382 directs that NSTAC reports be submitted to the President and to you in your capacity as Executive Agent, National Communications System.

On behalf of the NSTAC members, I would like to sincerely thank you and Deputy Secretary Atwood for hosting the executive breakfast in your dining room and for arranging the special threat assessment briefings for us in the National Military Command Center that morning. The briefings provided us with valuable national level perspectives that will help us provide informed advice to the President regarding contemporary national security and emergency preparedness telecommunications issues.

The NSTAC XIV Business Session resulted in approved final reports from its Network Security and Enhanced Call Completion Task Forces and recommendations to the President regarding the Government's support of network security standards and the Government's potential use of enhanced call completion capabilities. The NSTAC directed its Industry Executive Subcommittee (IES) to establish a Network Security Standards Oversight Group to work with the standards community and encourage development of network security standards for the public switched networks. The NSTAC also directed its IES to establish an ad hoc group to continue supporting the Government in developing its Enhanced Call Completion requirements. The NSTAC's Energy Task Force joint efforts with the Department of Energy and the National Communications System will be concluded and reported at NSTAC XV in May 1993.

The NSTAC appreciates the staff support, technical assistance, and cooperation it continues to receive from you and from the Manager and staff of the National Communications System.

Sincerely,



R.E. Allen
Chairman

1 Enclosure:
NSTAC XIV Report to the President

Copy to:
NSTAC Members
LTG Short
COL Linhares

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC)

Executive Report

NSTAC XIV - July 17, 1992

The fourteenth meeting of the National Security Telecommunications Advisory Committee (NSTAC XIV) was held on July 17, 1992, at the Old Executive Office Building in Washington D.C. At its business session, the Committee reviewed the activities and results of three active task forces and its Industry Executive Subcommittee (IES). The Committee also paid respects to the passing of one of its original principals, Mr. Bill McGowan, of MCI.

Lieutenant General Alonzo E. Short, Manager, National Communications System, and Director of the Defense Information Systems Agency, congratulated the Committee, on the NSTAC's tenth anniversary, and addressed the significance of their accomplishments with respect to the National Level Program that was formulated based upon NSTAC input to the Government. He paid tribute to the Government-industry National Coordinating Center in its handling of telecommunications emergencies under diverse emergency conditions, and recognized current efforts that provide for the exchange of network security information concerning the newest potential network enemy, the electronic intruder (or computer hacker). General Short also provided an update on the progress of Government programs and initiatives influenced by the NSTAC, such as the Telecommunications Service Priority (TSP) System, the National Transportable Telecommunications Capability (NTTC) initiative, and National Coordinating Center (NCC) activities. General Short challenged the NSTAC to consider, for NSTAC issue identification and action, potential threats to the telecommunications networks over the next ten years, in view of the Government's increasing dependence on commercial communications systems. He noted that of particular concern to the Government is the evolution and planned interconnection of the domestic and, ultimately, international Signalling System 7's, and the need for the developing "firewalls" to mitigate disruptions in any network having significant impact on other networks.

The NSTAC XIV findings and recommendations are summarized below. Attached to this report are the list of Committee members present for the meeting (Attachment 1), the NSTAC recommendations to the President (Attachment 2), and the NSTAC charges to its IES (Attachment 3). The summary of the NSTAC XIV business session (Attachment 4) and a compilation of the reports approved by the Committee (Attachment 5), are also provided.

NETWORK SECURITY

The Network Security Task Force completed its work assigned at NSTAC XII and XIII which was to identify a mechanism to improve network security information exchange, recommend a method to improve the flow of network security intelligence to industry, recommend the network research and development that is needed, and make recommendations on industry-wide network security standards.

In response to these NSTAC charges, the task force (1) continued activities with the previously established Network Security Information Exchange (NSIE), (2) reviewed six research and development (R&D) and standards areas having an impact on network security, and (3) provided its final report, with findings and recommendations, to the Committee.

The NSTAC will establish a Network Security Standards Oversight Group (NSSOG) to work with the standards community to encourage the development of a single, consistent set of network security standards for the public switched network (PSN). The NSTAC will continue to support the NSIE at least through May 1993.

ENHANCED CALL COMPLETION

The Enhanced Call Completion (ECC) Task Force, established to investigate ways to improve NS/EP call completion rates during periods of stress to the PSN, completed the tasks assigned by NSTAC XII, and provided their final report, conclusions, and recommendations to the NSTAC.

From its deliberations, the task force noted that the ability to transport an NS/EP call through the PSN depends on the development of an NS/EP call identifier capability that would support preferential treatment for NS/EP calls. Further, the task force noted that the High Probability of Completion (HPC) Standard, being considered by the Exchange Carriers Standards Association (ECSA), was crucial to providing enhanced call completion. An additional task force concern was the potential need for the Federal Communications Commission (FCC) to examine and rule on preferential treatment for government organizations with respect to ECC services.

INDUSTRY EXECUTIVE SUBCOMMITTEE REPORT

OPERATIONS WORKING GROUP ISSUES

The NSTAC's Industry Executive Subcommittee (IES) reported on the results of its Operations Working Group's (OWG's) examination of the importance of having user provided backup emergency power for customer premises equipment that is connected to systems supported by the Telecommunications Service Priority (TSP) System. The OWG reported that the OMNCS will continue to address this issue by including it as part of the TSP System user training. The OWG also reviewed existing Government command center operations and concluded that Federal and state command centers were adequate. Further, the OWG found that while upgrades to some of the centers might be beneficial, the cost and benefit tradeoffs would not be sufficient to warrant the upgrades.

JOINT INDUSTRY-GOVERNMENT PLANNING

The subject of the NSTAC and OMNCS roles in joint Industry-Government planning has been the subject of significant discussion during the past year. In response to the NSTAC and the Assistant to the President for National Security Affairs, the IES conducted meetings to identify issues for resolution by NSTAC, and discussed processes for identifying and rank ordering such issues and for developing a plan of action for the NSTAC. Subsequently, the IES and the OMNCS convened an ad hoc group composed of members from the IES, the OMNCS assistant managers, amd the Deputy Manager, NCS to review the OMNCS NS/EP telecommunications strategy, consider issues previously generated by the OMNCS and the IES's Operations and Plans Working Groups, and further, to consider the budgetary impact of those issues prior to recommending them for action by the NSTAC and the OMNCS. Issues found to be impractical due to budgetary constraints are to be noted but not recommended for action.

ENERGY

The Energy Task Force has partially completed its NSTAC XIII assigned work by developing qualifying criteria and a process for identifying the NS/EP telecommunications facilities requiring priority electric service restoration and back-up power refueling. Lists of telecommunications industry facilities, by State, will be provided to the Department of Energy (DOE) to help implement an electric service priority restoration program at state and local levels. The task force is continuing its review of the President's National Energy Strategy (NES), as it relates to NS/EP telecommunications requirements, and will consider making recommendations to DOE for inclusion in the planned 1993/1994 NES publication.

ATTACHMENT I

NSTAC XIV
MEMBERS IN ATTENDANCE

Mr. Robert E. Allen	AT&T
Mr. Norman R. Augustine	Martin Marietta
Mr. Kent M. Black	Rockwell International
Mr. Bruce L. Crockett	COMSAT
Mr. Gerald W. Ebker	IBM
Mr. D. Travis Engen	ITT
Mr. William T. Esrey	Sprint
Mr. George H. Heilmeier	Bellcore
Mr. William J. Hilsman	IMM
Mr. Arthur E. Hitsman	Boeing
Mr. Edward E. Hood, Jr.	GE
Mr. William R. Hoover	CSC
Mr. Frederick F. Jenny	UNISYS
Mr. Charles R. Lee	GTE
Mr. John N. McMahon	Lockheed
Mr. Richard D. McCormick	US WEST
Mr. Bert C. Roberts, Jr.	MCI
Mr. Charles E. Robinson	PTI
Mr. Paul G. Stern	NTI

ATTACHMENT 2

NSTAC RECOMMENDATIONS TO THE PRESIDENT

NSTAC XIV - JULY 17, 1992

Network Security

The Government should establish a focal point for coordination on network security standards.

The Executive Office should publicly support the NSTAC network security initiative.

Enhanced Call Completion

The Government should take the following steps to enhance call completion for NS/EP users:

- Take advantage of existing and emerging services, features, and capabilities in the Public Switched Network
- Continue to support the near-term adoption of the High Probability of Completion standard by the Exchange Carriers Standards Association T1 Committee
- Investigate the NS/EP advantages of a calling name delivery service
- Work with NSTAC's Funding and Regulatory Working Group to investigate potential regulatory issues
- Sponsor industry Enhanced Call Completion forums to further define Enhanced Call Completion and resolve implementation issues

The Government should use the Enhanced Call Completion Task Force report as a reference for modifying or implementing current or future services and technologies

ATTACHMENT 3

NSTAC CHARGES TO ITS INDUSTRY EXECUTIVE SUBCOMMITTEE (IES)

NSTAC XIV - JULY 17, 1992

Network Security

- Oversee the Network Security Information Exchange (NSIE) and make recommendations about Network Security Information Exchange follow-on
- Establish and oversee the NSTAC Network Security Standards Oversight Group
- Continue involvement in Research and Development information exchange
- Represent the NSTAC on NSIE matters to the FCCs Network Reliability Council; Manager, NCS; and Government Network Security Subgroup
- Support other network security issues as required
- Deactivate the Network Security Task Force

Enhanced Call Completion

- Establish an ad hoc group to work with Government to:
  - Advocate and support approval of the High Probability of Completion standard
  - Investigate potential Enhanced Call Completion regulatory issues with the Funding and Regulatory Working Group
  - Implement Enhanced Call Completion network capabilities
- Deactivate the Enhanced Call Completion Task Force

ATTACHMENT 4

SUMMARY OF THE NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE BUSINESS SESSION

July 17, 1992

CALL TO ORDER. Mr. Robert Allen, Chairman of the Board and Chief Executive Officer of AT&T, and Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), called the 14th NSTAC meeting to order at 11:30 a.m. in the Old Executive Office Building, Washington, D.C. Mr. Allen thanked the Executive Office of the President for hosting the meeting.

OPENING/GENERAL REMARKS. Mr. Allen recognized several individuals attending their first NSTAC meeting: Mr. D. Travis Engen, Executive Vice President of ITT; Mr. Richard D. McCormick, President and Chief Executive Officer of US West; Mr. John N. McMahon, President of Lockheed Missiles and Space Systems Group; Mr. C. Michael Armstrong, Chairman and Chief Executive Officer of Hughes Aircraft; Mr. Bruce L. Crockett, President and Chief Executive Officer of COMSAT; Mr. Charles R. Lee, Chairman of the Board and Chief Executive Officer of GTE; and Mr. Bert C. Roberts, Chairman and Chief Executive Officer of MCI. Mr. Allen welcomed the members of the National Communications System (NCS) Committee of Principals (COP) and Council of Representatives (COR) to the meeting and noted their key role in the joint industry-government planning process. Mr. Allen introduced a brief video honoring recently deceased NSTAC principal, Mr. Bill McGowan of MCI.

Mr. Allen then reviewed ongoing NSTAC activities. He said the Energy Task Force had partially completed its NSTAC XIII charge by developing criteria and a process for identifying critical industry telecommunication facilities that qualify for priority electric service restoration and fuel distribution. He reported that this information would be made available to the Department of Energy to aid in developing a priority electric service restoration program. Mr. Allen said that the task force would soon begin its review of the President's National Energy Strategy (NES) in relation to NS/EP telecommunication requirements and consider submitting recommendations for the planned 1993/1994 NES publication.

Mr. Allen said that at NSTAC XIII, the NSTAC agreed to reactivate the Wireless Services Task Force. Agreements are in place to designate the Office of the Manager, National Communications System (OMNCS) Office of Technology and Standards as the government focal point, in coordination with the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

Mr. Allen introduced the business session agenda, with briefings scheduled from the Network Security and Enhanced Call Completion (ECC) Task Forces and the Industry Executive Subcommittee (IES).

NETWORK SECURITY TASK FORCE. Mr. Herbert Benington, of UNISYS/Paramax, and the Network Security Task Force Chairman, presented a briefing on current task force activities. He reviewed the task force membership and the original NSTAC XII charges to the IES, and described the Network Security Information Exchange (NSIE) group functions and its activities to date.

Mr. Benington then discussed activities in the six research and development (R&D) and standards action areas: control of outside access to network elements; event control within "trusted" network segments; prevention of inappropriate access (partitioning, "firewalls"); detection of unauthorized access; recovery from software/database damage; and planning a full network security architecture.

Mr. Benington presented an updated risk assessment to the members, noting that the sensitive information in this assessment had been presented to the Principals at the issues briefing earlier that morning. Mr. Benington then outlined the task force's conclusions and recommendations. He said that effective network security continued to depend on the commitment of senior management to implement comprehensive corporate-wide security programs to reduce system vulnerabilities and maintain a high level of security awareness. He added that the continuing evolution of the PSN would require a concerted effort by carriers and vendors to develop a strong network security information exchange mechanism, analyze major network security incidents, and provide leadership in developing objectives for strong industry-wide security standards.

Mr. Benington concluded his briefing with a proposal to establish a new Network Security Standards Oversight Group (NSSOG) to work with the standards community to foster the development of a single, consistent set of network security standards for the PSN. The NSSOG would help establish and prioritize industry objectives for network security standards and would embrace architecture, design, operations, interfaces, and assurance. A representative asked about vendor and carrier participation in this group. Mr. Benington replied that the members of this group would be named by the IES and that the membership should be open to all interested NSTAC companies.

Mr. Allen thanked Mr. Benington for his briefing. The NSTAC approved the task force's report for forwarding to the President, the two proposed recommendations to the President, the IES recommendations to the NSTAC, and the proposed NSTAC XIV charges to the IES (the latter three items are found in Appendix B, as Attachments 1, 2 and 3, respectively).

ENHANCED CALL COMPLETION (ECC) TASK FORCE. Dr. Sushil Munshi, of Sprint, and the ECC Task Force Chairman, presented the task force final report and

recommendations. He reported that the task force had completed the charge it was given in December 1990 at NSTAC XII. Dr. Munshi thanked the task force members, the NCS staff, and government contractors for their role in preparing the comprehensive study of current and potential ECC capabilities in the PSN. After reviewing the ECC definition and the task force's technical approach, Dr. Munshi presented the task force's general conclusions.

In presenting his conclusions, Dr. Munshi stressed the need for developing an NS/EP call identifier capability to provide preferential treatment for NS/EP calls. Dr. Munshi said the ability to transport a call identifier within the PSN was crucial to improving call completion rates and depended on the adoption of the High Probability of Completion (HPC) standard by the Exchange Carrier Standards Association's (ECSA) T1 Committee. The ECC Task Force also concluded that a ruling by the FCC might be necessary because the NS/EP identifier would provide preferential treatment to a specific group of telecommunication users, thereby violating Section 202 of the Communications Act of 1934.

Dr. Munshi concluded his briefing by reviewing the proposed recommendations to the President regarding specific steps the Government should take to improve NS/EP users' chances for completing calls during emergency situations. Mr. Allen thanked Dr. Munshi for his briefing. NSTAC members approved the task force's report for forwarding to the President, the two proposed recommendations to the President, and the proposed NSTAC XIV charges to the IES (the latter two items are found in Appendix B, as Attachments 1 and 3, respectively).

INDUSTRY EXECUTIVE SUBCOMMITTEE. Mr. Richard Lombardi, of AT&T, and the Plans Working Group Chairman, presented a summary of the issues considered by the IES, OWG and PWG since the last NSTAC meeting. Specifically, he stated that the IES had reviewed the ECC Task Force Final Report, the Network Security Task Force Report, and Energy Task Force activities.

Mr. Lombardi reviewed two issues raised by the Operations Working Group (OWG); these issues were discussed and closed at the last IES meeting. The first issue was the need to stress the importance of backup power for customer premises equipment that supports Telecommunications Service Priority (TSP). Mr. Lombardi explained that OMNCS plans to address this issue through ongoing training provided to users of the TSP system. The second issue addressed by the OWG was a recent review of existing government emergency preparedness command center capabilities, which determined that current Federal and State facilities were adequate and no task force action was needed. Mr. Lombardi said that although some command centers would benefit from an upgrade, the cost proved to be prohibitive.

Mr. Lombardi said that in the past year, the NSTAC/OMNCS role in joint industry-government planning was the subject of significant discussion. He said that in response to both the NSTAC and the Assistant to the President for National Security Affairs, the IES had

conducted meetings to identify issues that could potentially require NSTAC action, discussed processes for identifying and prioritizing such issues, and developed a plan of action. He said the IES planned to convene an ad hoc group composed of members of both industry and the OMNCS. This group will review OMNCS strategy and coordinate NSTAC support for that strategy. The ad hoc group will also consider issues previously generated by the OWG, PWG, and the OMNCS, as well as any new issues. Additionally, the group will consider the budgetary impact of any issue before placing it on the priority action list. Issues found to be impractical from a budgetary standpoint will be noted, but not placed on the action list. Mr. Lombardi said that the ad hoc group would report its progress at the next NSTAC meeting.

In concluding his brief, Mr. Lombardi identified the ad hoc group members:

IES:
Mr. Richard Lombardi, AT&T
Mr. Carl Ripa, Bellcore
Mr. George Bolling, COMSAT
Mr. Lowell Thomas, GTE
Mr. Jack Taylor, IMM
Mr. John Hocker, Martin Marietta
Dr. John Edwards, NTI

OMNCS:
Mr. Ben Morriss, Deputy Manager
Mr. Ken Boheim, Assistant Manager NP
Dr. Dennis Bodson, Assistant Manager NT
Col Leroy Faust, Assistant Manager NE
CAPT Dennis Parsons, Assistant Manager NJ

Mr. Allen thanked Mr. Lombardi for his report.

MANAGER'S REPORT. LTG Alonzo E. Short, Jr., Manager, NCS, and Director of the Defense Information Systems Agency (DISA) praised and thanked NSTAC members for their important contributions to NS/EP telecommunications over the past 10 years. He noted that without the NSTAC, the Government would not have a National Coordinating Center (NCC) to handle a surge in communication requirements for the next mobilization; an industry group studying the benefits NS/EP users could derive from emerging technologies; or a joint industry-government mechanism already in place to exchange information on the newest potential enemy, the electronic intruder (or computer hacker).

In reflecting on past NSTAC accomplishments, LTG Short said that the most important NCS programs grew out of discussions fostered by the NSTAC. All three elements of the National Level Program -- Commercial Network Survivability (CNS), Commercial SATCOM Interconnectivity (CSI), and Government Emergency Telecommunications Service (GETS) -- had been formulated based on NSTAC inputs. He emphasized that the Government needed to remain fully apprised of NSTAC companies' current and planned technology base to ensure that the NLP continues to take advantage of

evolving technologies. LTG Short noted that recommendations from the Enhanced Call Completion Task Force on potential network capabilities, such as the NS/EP call identifier, were helping the NCS move forward on the NLP. He also said that the NSTAC investment in both the NCC and the Telecommunications Service Priority (TSP) System paid off during Operations DESERT SHIELD and DESERT STORM, and continued to support other NS/EP contingencies.

LTG Short challenged NSTAC members to consider what new threats could attack the integrity of the Nation's communications networks in the next several years, given the Government's increasing dependence on commercial communications systems. LTG Short said that collectively, the NSTAC and the NCS could reexamine and probe those issues that might pose a future threat to the Nation's well-being. In addition to recurring natural disasters, LTG Short cited some potential manmade conditions that could threaten our national security posture: security of open networks, uncertain software reliability, and equipment failures. In particular, he noted the interconnection of Signaling System 7 (SS7) networks domestically over the next year, and later internationally, as a potential vulnerability unless Government and industry continue to work together to develop "firewalls" to prevent disruptions in one network from corrupting others.

LTG Short emphasized that in today's uncertain times, a highly advanced and ubiquitous telecommunications infrastructure was vital to our welfare as a nation, to our economy and global competitiveness, and even the technical education of our children. He said that each of these areas could be framed in terms of national security and would provide an opportunity for telecommunications industry involvement. In closing, LTG Short stated that NSTAC was created to fill a gap brought about by divestiture and a continuing need for reliability in NS/EP telecommunications. Today, the NSTAC can be a bridge linking advanced telecommunications technologies to the national security requirements of the 1990's and beyond.

CLOSING REMARKS. Mr. Allen thanked the NSTAC members and their IES and task force representatives for contributing their time and expertise in support of NSTAC activities. He also thanked LTG Short and the OMNCS for their assistance in planning and preparing for NSTAC XIV. Mr. Allen announced that the next meeting of the NSTAC is scheduled for May 26 and 27, 1993.

ADJOURNMENT. Mr. Allen adjourned the business session at 12:25 p.m.

APPENDIX A

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE
MEETING ATTENDANCE
JULY 17, 1992

Name	Organization
Frank Adams	PTI
Robert E. Allen	AT&T
J. Robert Anderson	DoD
Norman R. Augustine	MMC
David Austin	NSA
Andrew C. Barrett	FCC
William B. Belford	NCS-NE
Herbert D. Benington	UNISYS/Paramax
Jerome Bevenour	AT&T
William E. Bischoff	DOS
Kent M. Black	Rockwell
Kenneth B. Boheim	NCS-NP
George H. Bolling	COMSAT
Howard D. Boyd	DVA
Steven W. Broadbent	TREAS
Robert P. Brownfield	CSC
Len Brush	NCS-NJ
Henry I. Buchanan III	USTA
Thomas J. Buckholtz	GSA
Tom Burns	MITRE
Dave Bush	AT&T
Arlington F. Campbell	NCS-AB
Frank J. Campbell	HHS
Lucien Capone Jr.	BA&H
Carmin C. Caputo	NCS-NJ
Joanne Cavalcante	NCS-NA
Michael Cleary	NCS-NJ
Mike Cohen	MITRE
William J. Cook	DoD
Roger M. Cooper	DoD
Nancy H. Correia	DOT
Michael L. Corrigan	GSA
Bruce L. Crockett	COMSAT
Allen D. Dayton	COMSAT
James E. Dolezal	DOI
Arnold E. Donahue	OMB
Dennis Doughty	BA&H
Robert L. Drummond	DISA

Name	Organization
Gerald W. Ebker	IBM
John S. Edwards	NTI
D. Travis Engen	ITT
William T. Esrey	Sprint
Patricia A. Figliola	BA&H
Luin Fitch	DOJ
George F. Flynn Jr.	GSA
Joseph J. Gancie	ITT
Donald E. Gessaman	OMB
Jorome T. Gibbon	DOC
Charles Givans	BA&H
Thomas Gooley	Hughes
Ernestine Gormsen	GTE
John G. Grimes	DoD
Richard Hayden	DOE
Eleanor Harris	MITRE
James Hastings	Sprint
George H. Heilmeier	Bellcore
Fred Herr	NCS-NJ
William J. Hilsman	IMM
Arthur E. Hitsman	Boeing
John R. Hocker	MMC
George J. Hoffman	DISA
Philip D. Hollar	MCI
Edward E. Hood	GE
William R. Hoover	CSC
Janet S. Jefferson	NCS-NJ
Frederick F. Jenny	UNISYS
Robert D. Johnson	USDA
Donald J. Jurenko	MITRE
Charles R. Lee	GTE
Robert M. Lewis	DOE
Patrick Linhares	NSC
Greta A. Lomas	DISA
Richard J. Lombardi	AT&T
Robert Marquette	OEO
Richard D. McCormick	US WEST
Berry McFarlin	NCS-NJ
Alan R. McKie	FCC
John N. McMahon	Lockheed
James Mehring	Hughes
Benham E. Morriss	NCS-NA
Sushil Munshi	Sprint
G. Jay Nelson	Sprint

Name	Organization
John F. O'Neil Jr.	OSTP
John L. Okay	USDA
Richard D. Parlow	NTIA
Dennis I. Parsons	NCS-NJ
Martin Peavyhouse	NCS-NJ
Ted S. Phillips	BA&H
D. C. Pidgeon	GE
Patricia D. Poole	NCS-NJ
James R. Porter	JS
Gordon Powell	NCS-NJ
Roger W. Reinke	NTIA
Carl V. Ripa	Bellcore
Art Roberts	MCI
Bert C. Roberts Jr.	MCI
Charles E. Robinson	PTI
Randy S. Schulz	Bellcore
M. Wayne Shiveley	DOJ
Alonzo E. Short	NCS-AA
Carl W. Smith	NCS-AR
Ed Smith	AT&T
William K. Stanley	MITRE
Robert W. Steele	Boeing
Paul G. Stern	NTI
Jack T. Taylor	IMM
Lowell E. Thomas	GTE
Harry Underhill	Bellcore
Anthony M. Valletta	DoD
Sylvia Velle	DISA
James Vick	NCS-NP
Winston J. Wade	US WEST
Ernest L. Wallace	COMSAT
Kymry Watkin	BA&H
George T. Weathers	IBM
Stanley M. Welland	GE
J. Glenn Whited	Motorola
Thomas S. Will	MCI
William H. Wunderlich	TREAS
Phyllis Young	GROSS

National Security
Telecommunications
Advisory Committee
(NSTAC)

Reports Submitted for NSTAC XIV

July 17, 1992

Reports Submitted for the Fourteenth Meeting of Network Security Telecommunications Advisory Committee (NSTAC)

July 17, 1992

- Final Report of the Network Security Task Force
  17 August 1992
- Final Report of the Enhanced Call Completion (ECC) Task Force
  July 1992

Network Security
Task Force
Report

Final Report of the Network Security Task Force

Revised

17 August 1992

Network Security
Task Force
Report

Final Report of the Network Security Task Force

Revised

17 August 1992

Final Report of the Network Security Task Force

Distribution of this report is approved within the telecommunications industry and to selected individuals.

Revised

17 August 1992

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

The Network Security Task Force was established to address means to reduce the vulnerability of the Public Switched Network (PSN), and associated operations systems, to software manipulation that results in denial of service to national security and emergency preparedness (NS/EP) users, or extraction of NS/EP-significant information.

The task force has worked closely with the Government toward identifying a mechanism for security information exchange, and has addressed needed research and development (R&D) and standards for network security. A National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchange (NSIE), meeting jointly with a Government NSIE with intent to assess risks and trends, has made substantial progress in administrative means to foster the needed environment of trust; and an exchange of information on vulnerabilities, incidents, and countermeasures has begun.

An alert, warning, and recovery function, via the existing National Coordinating Center, will provide real-time notification to industry and Government about significant network security events that could impact NS/EP users.

FINDINGS

Threat, vulnerabilities, and incidents. Hackers continue to intrude upon both voice and data segments of the PSN. Sensitive Government interests have been affected by intrusions that have adversely affected Government operations. The age and apparent motivation of intruders appear to be undergoing a gradual change, as the average age of individuals under scrutiny is in the mid- to late twenties. Financial gain appears to be increasingly dominant as a motivation. Economic intelligence-gathering is expected to continue to rise.

Hackers share information about how to intrude into PSN software, posting it on private electronic bulletin board systems. Top-level hackers exploit others to carry out their purposes. While collusion among hackers has been demonstrated in recent years, collusive intent to "take down" the PSN has *not* been demonstrated. However, the potential for targeting the PSN as a source of information for intelligence-gathering has been clearly established.

Hackers have increased sophistication in technical and operational capabilities. Penetrations continue to exploit weaknesses in security practices and in protection mechanisms. Techniques used to gain information include impersonation of company personnel ("social engineering"); digging in dumpsters; physical entry into facilities; use of dialup ports to Operations, Administration, Maintenance, and Provisioning (OAM&P) systems; defeat of access controls such as dialback modems; electronic realtime collection of logins and passwords; the use of packet and

data networks to reach and control circuit-switched traffic; and use of transparent maintenance utilities to eavesdrop. Intrusions of a type already experienced *could* result in service shutdown.

Risk update. The risk to the PSN remains difficult to quantify. It appears more substantial than the lower level of the range discussed in the "scoping" task force report issued in November 1990 [1]. Some carriers have increased their abilities to resist, but there has been a lot more cleverness and knowledge of network vulnerabilities demonstrated by those who are trying to penetrate networks directly, penetrate through another PSN network, or break through gateways. Data network interconnections between network elements of diverse systems are increasing and, without the presence of appropriate firewalls, they can extend the vulnerability of any system to other systems to which they are connected.

Architectural trends and risk. The current move to interconnect Signal Transfer Points across company boundaries potentially provides the hacker with more paths to explore, and could extend his geographic "reach" dramatically. Adequate protection against making penetration easier must be provided, in view of industry changes to reduce cost, improve performance, meet regulatory orders (e.g., 800 number portability, Open Network Architecture), and maintain competitiveness. These industry changes, which are ongoing, include higher automation throughout the system, interconnection of Signaling System 7 throughout the PSN; and high dependence on packet switched networks for network management and control. Some system-wide standards are beginning to emerge to increase network security on the PSN, but more are needed.

R&D and standards. The task force recommended to the Government what R&D is needed for commercially applicable tools. Six areas were identified that were judged to need R&D and perhaps new standards, with near-term emphasis to be in the access area. The concept of Generally Accepted System Security Principles (GSSP) was explored, with consequent identification of some Government, Bellcore, and Network Open Forum documents and drafts in process that partially address network security standards.

It appears that recent developments in U.S. Government network security strategy will foster increasing convergence between the objectives of the security requirements of the telecommunications industry and of the developments in the Federal Government. The task force believes industry and Government need to coalesce around a single set of security standards and working agreements that can be applied to reduce vulnerability in the PSN.

RECOMMENDATIONS

Recommended Action plan for the Industry Executive Subcommittee (IES). The task force recommends that the IES forward the NSTAC plan of action (below) for endorsement by NSTAC principals. For its own part, the IES should create a small network security subcommittee to: (1) oversee and support NSIE activities; (2) establish and oversee a proposed NSTAC Network Security Standards Oversight Group (NSSOG), consisting of experts with design and operations expertise and standards awareness, that will work with the standards community; (3) continue

involvement in R&D information exchange; (4) represent the NSTAC, on NSIE matters, to the Federal Communication Commission's Network Reliability Council; (5) represent the IES on matters relating to the NSIEs in dealing with the Deputy Manager, Office of the Manager, National Communications System (OMNCS), and the Government Network Security Subcommittee that he chairs; and (6) support the IES on other network security-related issues.

Proposed NSTAC plan of action. Whereas

Electronic intruders have demonstrated the capability to (1) deny, or interfere with, PSN service to targeted users, and (2) extract significant information from targeted circuits

The NSTAC is sponsoring an exchange of information among NSTAC companies on the threat, vulnerabilities, incidents, and countermeasures relating to electronic intrusions and manipulations of elements of the PSN

The NSTAC's awareness of the need to reduce network security risks in the PSN of the future has been heightened since 1990, and

As a consequence the NSTAC recognizes that the security of all networks in the PSN must not depend upon the security of the weakest interconnected network

the NSTAC will provide impetus for a concerted effort to reduce risks to the PSN from electronic intruders in current systems, to foster related information exchange conducted broadly across the telecommunications industry, and to take steps to enhance the network security of current and future systems.

As part of this initiative, the NSTAC Principals will:

1. Continue to support the NSTAC Network Security Information Exchange as needed at least until NSTAC XV in the spring of 1993. Include approval of staff and resources for exchange of information on analysis of vulnerabilities and detailed evaluation of incidents to determine root causes and evaluate countermeasures

2. Provide needed resources and staff for an NSTAC NSSOG, consisting of individuals with design and operations expertise, to work with the standards community and actively foster a single set of network security standards for the PSN

3. Endorse joint industry and Government exercises to test the capability to work together to mitigate security problems

The NSTAC Principals will further act to promote, within their own organizations, a greater level of awareness of network security.

The NSTAC will ask the President to publicly support the NSTAC initiative, and to establish a Government focal point for network security standards where coordination and unified action are required.

SECTION 1

INTRODUCTION

At the request of the Government, the National Security Telecommunications Advisory Committee (NSTAC) in March 1990 endorsed an investigation into network security to address the vulnerabilities of the Nation's telecommunications infrastructure to outside or unauthorized access. An NSTAC task force, established to scope the issue, addressed the potential for disruption of national security and emergency preparedness (NS/EP) telecommunications through manipulation of software in the Public Switched Network (PSN). It concluded that the current PSN is vulnerable to hacker intrusions and disruptions that might (1) deny telecommunications service to NS/EP users, or (2) extract NS/EP-significant information. The network security report [1] of November 1990 concluded that "the burden of protecting the public switched network falls primarily on service vendors and equipment manufacturers." It stated that individual companies were aware and were taking action; it provided service suppliers with a checklist of steps that, when followed, would substantially enhance the security of their own networks. In addition, it concluded that a broader information flow among carriers and suppliers nationwide would assist and improve network security, and the proposed follow-on NSTAC activities.

1.1 NSTAC CHARGES

At its December 1990 meeting, the NSTAC charged its Industry Executive Subcommittee (IES) to establish a follow-on Network Security Task Force to work closely with the Government to identify a mechanism for security information exchange, and to address needed research and development (R&D) and standards for network security. (For specific charges in each of these activities, see sections 2.2 and 2.3.) The NSTAC asked the IES to report its results at the NSTAC meeting in mid-1992.

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 Chairman, Policy Coordinating Committee on National Security Telecommunications and Information Systems (PCC-NSTIS) [2]. The GNSS is chaired by the Deputy Manager of the NCS and has representatives from Federal departments, agencies, and other entities that have particular responsibilities relevant to network security:

- 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 (OASD/C3I)
- The U.S. Secret Service (USSS)

1.2 STATUS AT NSTAC XIII

At the thirteenth meeting of the NSTAC on 3 October 1991, the task force presented an interim report [3] summarizing its progress and plans for completion of its work by the NSTAC XIV meeting in July 1992. A list of task force participants in appendix A.

The task force stated that its primary efforts to that point had focused on identifying a mechanism for security information exchange concerning risks and remedies and recommending steps to improve flow of Government information to industry about threat to the PSN. The task force had 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 to provide "real-time" notification to industry and Government about significant events regarding network security; and (3) an IES/task force subcommittee to evaluate the above two activities and contribute to network security conclusions and recommendations for NSTAC XIV.

Network Security Information Exchange. The industry NSIE had only recently been created, set up on a trial basis under the auspices of the task force. The aim of the NSIE is to foster an informal, collegial exchange of information--some of it proprietary and sensitive--concerning potential or actual intrusions into software of the PSN that might (1) deny telecommunications service to NS/EP users, or (2) extract NS/EP-significant information. The Government had established a Federal Government NSIE group to work in concert with the industry group. Although separate organizations, both groups have very similar charters and were expected to meet together regularly to exchange information on vulnerabilities, risks, and trends. Charters and membership lists for the two NSIEs were appended to the report.

In event-driven situations, the NSIEs are to assist the alert, warning, and recovery activities as required to mitigate the effects of network security events on the PSN. The already existing joint

industry-Government National Coordinating Center (NCC) had been designated to coordinate the alert, warning, and recovery activity, assisted by technical advice from NSIE members. The informal exchange of network security information in the NSIE and the network security alert, warning, and recovery activity in the NCC were yet to be undertaken. Some experience with the two activities was expected to form the basis for future recommendations to NSTAC XIV.

R&D and standards. In a separate effort, the task force had begun addressing charges to (1) recommend to Government what R&D is needed for commercially applicable tools, and (2) comment on standards activities with regard to network security. A list of R&D and Standards Subgroup participants is in appendix B. Subgroup members had tentatively identified six areas that were judged to need R&D and perhaps new standards to improve NS/EP telecommunications network security in the current PSN, and in which areas the Government might have contributions to offer. A dialogue with Government was under way to determine what agencies/departments had accomplished in the identified "need" areas and which Government developments might be commercially applied or adapted. In addition, the task force had begun to explore the existence of, or possibility for achieving, a set of Generally Accepted System Security Principles (GSSP) proposed earlier in a National Research Council report [4].

After hearing the interim report, the NSTAC charged its IES to continue Network Security Task Force activities as charged, and report to NSTAC XIV.

1.3 PURPOSE AND ORGANIZATION OF REPORT

1.3.1 Purpose

The purpose of this document is to report the accomplishments to NSTAC XIV (to date) of the current Network Security Task Force. The report focuses particularly on those activities carried out since the last meeting of the NSTAC in September 1991, NSTAC XIII.

1.3.2 Organization of the Report

Section 2 of this report summarizes the findings and conclusions of the task force. Within section 2: section 2.1 describes the progress on providing real-time notification to industry and Government about significant events regarding network security; section 2.2 describes the progress and achievements of the NSIE activities; section 2.3 describes the task force's evaluation of the NSIE-related activities, including potential follow-on mechanisms; section 2.4 describes the progress on evaluating Government R&D and standards for commercially applicable tools; section 2.5 is an update of the risk assessment first undertaken in the 1990 NSTAC report to the President; and section 2.6 summarizes task force conclusions regarding work the task force has been unable to complete in the timeframe regarded as adequate at the time of NSTAC XIII.

Section 3 contains the recommendations to the IES on (1) further work that is needed in promoting network security, and (2) methods that should be utilized to accomplish that work.

Section 4 contains the plan of action proposed by the task force for endorsement by the NSTAC.

SECTION 2

FINDINGS

2.1 ALERT, WARNING AND RECOVERY ACTIVITY

2.1.1 Background

The task force and the OMNCS have concurred that the NCC is the agency to carry out the process of alerting the broader NS/EP community, whenever a network security event might require action in that community to mitigate its effects. The NCC routinely facilitates cooperation when NS/EP user service outages require coordination among industry and Government member organizations. The charter of the NCC is sufficiently broad to include reaction to network security events within its purview.

2.1.2 Accomplishments

Since NSTAC XIII, personnel from both the NCC and the NSIE have determined precisely what procedures should be followed in passing information from one group to another. An early issuance of bulletins has led to procedure modifications to support the intended information exchange without negative side effects. The expectation of the task force is that coordination of the NCC and NSIE activities will continue to be conducted as described in the following paragraphs.

When an NSIE group is made aware of information that should be disseminated beyond the NSIE representatives, it will act to inform individuals beyond the immediate NSIE circle. In most situations, dissemination will be limited to corporate employees who need to know the information in order to take actions that improve the secure functioning of their own company's network.

Beyond this level of information-sharing, whenever general actions by service vendors can improve the security of service for its NS/EP users, the NCC may be asked to assist in information dissemination. In such a circumstance, the NSIE will supply the NCC with alert, warning, and recovery messages to be broadcast to NS/EP users. The NCC will issue these messages to its regular list of message recipients.

Further, the NCC will initiate coordination with the NSIEs whenever a service outage potentially appears to be a network security event--that is, involving the security of PSN element software. In such a circumstance, the NCC will notify both NSIE chairmen as to the nature of the outage. NSIE representatives will confer to help determine whether or not the outage is, in fact, the result of an intrusion. If it is determined to be intrusion-related, the NSIE will investigate the event in parallel with the NCC.

2.2 NETWORK SECURITY INFORMATION EXCHANGE

2.2.1 Review of Pertinent NSTAC Charges

The NSTAC charges to the IES included charges in four areas. In the first two areas, covering joint efforts toward further security information exchange the charges were to:

Work closely with and in support of the GNSS to:

1. Identify a mechanism for security information exchange, and produce an implementation plan

2. Recommend how to improve flow of threat information to industry

2.2.2 Task Force Approach

The task force established the NSTAC NSIE, as reported to NSTAC XIII, under its auspices on a trial basis in order to gain experience. Based on the experience gained, the task force could recommend whether, or how, to establish a permanent information exchange outside the NSTAC. Charters and membership lists for the two NSIEs are included in the interim task force report to NSTAC XIII [3].

Since the time of the interim report to NSTAC XII, the NSIE has continued to meet on a bimonthly basis. In all, the task force's industry NSIE has met jointly with the Government NSIE seven times, and has met separately two times. The task force has undertaken to assess the NSIE activities, and is assaying an updated estimate of the risk to the networks from outside and unauthorized intrusions. The task force has further fostered contact with Government organizations having relevant information to offer in the network security R&D and standards areas.

2.2.3 Accomplishments of the Joint NSIEs

Over the past nine months, the NSIE has continued to make progress in meeting its objective to encourage the open exchange of network security information among selected Government and industry entities. Administrative machinery has been developed; an "alert, warning and recovery process" has been established and exercised; and an information exchange on threats, vulnerabilities, incidents, and remedies has begun.

Nondisclosure arrangements. The NSIE's objective requires the exchange of sensitive and proprietary information among the participants. A prerequisite to achieving the NSIE's chartered objective was a nondisclosure agreement, to be signed by all participants. The intent of the agreement is to assure the participants that company private and proprietary information will be kept in confidence within the NSIE community. The Funding and Regulatory Working Group drafted a unique Government/industry nondisclosure agreement for this purpose, which was signed without modification by all industry participants. Legal counsel for Government agency

participants suggested modification of the wording of the nondisclosure agreement, and Government and industry legal counsels conferred to redraft sections of the agreement through consensus. Among those who asked to participate, only the General Services Administration was unable to sign the redrafted nondisclosure agreement, and subsequently voluntarily ceased participation in the joint NSIE meetings.

Security clearances. In order to facilitate flow of some sensitive Government information to the NSTAC NSIE, the Government requested that all participants have a full Secret-level security clearance. Provisions were made for each NSIE member representative without a clearance to have a special DOD limited security clearance only for the purpose of NSIE meetings. Subsequently, all NSIE member representatives without security clearances have submitted the necessary paperwork for full Secret-level clearances.

Procedures and distribution control. Another administrative aspect dealing with the proper dissemination of NSIE information constituted a significant initial effort for the NSIE organization. Bellcore offered to submit three advisory bulletins to the NSIE as a test of how the NSIE might distribute information to NSIE members. It became evident from this first effort that the NSIE would need to expend significant energies to ensure the proper control and distribution of NSIE information. Much of the NSIE's focus during the first several meetings was concerned with:
(1) how to secure the sharing of sensitive information, especially during event-driven consultations; (2) who should receive what kinds of information and who would prepare electronic messages; and (3) how to label sensitive information to assure proper control of its dissemination.

The result was a set of NSIE distribution procedures that clearly identifies information as NSIE proprietary, where appropriate, identifies the source of the information, defines what level of distribution control the information is to be afforded, and identifies contact information for additional information.

To assist in the logistics of information distribution and communications during a security event, the NSIE developed a protected NSIE Bulletin Board System (BBS). Managed and operated under the auspices of the NCS, it: (1) provides a method of distribution of protected NSIE information; (2) is a repository for NSIE security information; (3) provides a protected communications capability for NSIE members to communicate among themselves; and (4) is the historical audit log for security events.

Sharing sensitive information. Beyond accomplishing the above necessary preliminaries, industry has begun to share information about specific vulnerabilities and generic modes of attack currently being experienced. The Government shared information to date (1) about the threat, within existing constraints related to classification, and (2) about intruder prosecutions, as constrained by judicial and privacy regulations.

Since last reporting cycle, no actual network security event has taken place that required the event-driven conferencing of the NSIEs in support of the NCC. However, an exercise program is

under way that has tested the NSIE BBS, resulting in improvements to it; further, an exercise is planned that will include interaction with the NCC.

2.3 EVALUATION AND GOVERNANCE OF THE NSIE

In February 1991, the Network Security Task Force established a panel of three IES members to monitor the NSIE and to assist the Task Force in formulating 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.

2.3.1 Assessment of NSIE Activities to Date

The panel, the task force, and the NSTAC NSIE all agree on the following conclusions regarding progress in establishing and evaluating the NSIE process:

1. Extensive progress has been made in developing the administrative machinery required for information exchange. This includes executed nondisclosure agreements; security clearances; procedures for handling sensitive information; and a protected bulletin board.

2. A process has been established for Government/industry coordination in real time in case there is a major event threatened or under way that might be attributable to computer criminals attacking the software of the PSN. This alert, warning, and recovery process involves both the industry and government NSIEs and the NCC. A set of exercises is under way to test this process.

3. The extent of information exchange on threats, vulnerabilities, incidents, and remedies has generally been significantly lower than the panel and task force had expected to achieve at this stage in the process. The main exception has been information provided by the law enforcement members (FBI and Secret Service) of the Government NSIE. The relatively low level of information exchange achieved to date can be attributed to a number of factors:

    a. The distraction of establishing the administrative machinery including the real-time function

    b. Delays in executing all nondisclosure agreements and security clearances (the latter has constrained inputs from intelligence agencies)

    c. Time needed to build trust and confidence that sensitive information will be adequately safeguarded

    d. Delay in developing a mutual understanding on the obligations of individual member companies as to what kinds of information should be provided, and

e. Support for event-driven situations still being preoperative; not all staffing for NSIE BBS has been committed or exercised.

4. Until a significantly higher than current level of information exchange is achieved, the NSIE efforts will be less rewarding than could be anticipated. Also, experience with successful information exchange is needed to guide the design and membership of an operational NSIE that is not under NSTAC sponsorship.

5. Accordingly, the NSTAC NSIE should continue to operate as presently constituted as an experimental information exchange under NSTAC auspices, at least until NSTAC XV.

2.3.2 NSIE Continuance Under NSTAC Until NSTAC XV

The panel and task force have considered several organizational arrangements for governance and evaluation of the NSTAC NSIE pending the report to NSTAC XV.

The key functions that need to be performed are to:

- Monitor the entire NSIE process and provide support or direct initiatives that will improve effectiveness of the process

- Represent the IES on matters relating to the NSIEs in dealing with the Deputy Manager, OMNCS, and the GNSS, which he chairs

- Evaluate, in conjunction with the GNSS, the effectiveness of the NSIE process, in particular the NSTAC NSIE

- Act as a core group to initiate migration of the industrial component out from NSTAC sponsorship, if there is consensus that an industrial NSIE is desirable.

Options considered. The organizational arrangements considered for performing these functions included:

- Continue using the current or a follow-on Network Security Task Force. The task force already exists and has been directing the NSTAC NSIE. The current task force, or a follow-on task force with membership adjustments as required, could complete the effort to evaluate the NSIE and identify a permanent mechanism for information exchange. However, without additional charges, performing the above functions may not challenge and justify a task force. The most onerous function above will be the last one; this needs to be undertaken by the organizations that will be founding members of the independent NSIE.

- Assign responsibility for the NSIE and the above functions to either the Plans or Operations Working Group. Establish a small panel of IES members within the group

with a chair to lead and represent the panel. The disadvantage of this approach is that the current NSIE members are represented in both the working groups.

- Assign responsibility for the NSIE and the above functions to a small panel of IES members with a chair to lead and represent the panel. A panel of four to six members would be adequate. However, any company represented on the NSIE should be allowed to join the panel.

The task force and NSIE panel concluded that the third alternative is most desirable.

2.4 R&D AND STANDARDS ACTIVITIES

2.4.1 Review of Pertinent NSTAC Charges

The NSTAC charges to the IES in the third and fourth areas--recommending to Government R&D that is needed for commercially applicable tools, and evaluating standards activities--from NSTAC XII were:

> Work closely with, and in support of, the GNSS to address the following:
>
> 3. Recommend what network research and development is needed
>
> 4. Examine activities on industry-wide standards for network security and make recommendations

2.4.2 Task Force Approach

To meet the above charges the task force carried out actions that were recommended by the earlier task force, namely to:

> . . . examine, in a joint effort with the Government, what network security areas need further research and development relative to the public switched networks, in order to facilitate the development of commercially applicable security tools. As part of this process, the task force should:
>
> Identify and prioritize needs of the PSN for technical developments
>
> Meet with the Government and present an industry view of what is needed to be developed
>
> Determine what is already being addressed by the Government
>
> Make recommendations on what Government and industry should focus on in the future.

. . . investigate existing industry-wide standards activities for network security, determine whether shortfalls exist, and make recommendations as appropriate [1].

2.4.3 Accomplishments of R&D and Standards Subgroup

Establishing a dialogue. The first of four joint industry-Government R&D and standards meetings was held in April 1991, organized by the R&D and Standards Subgroup of the task force. At that meeting, industry representatives briefed the following subjects: the elements and vulnerabilities of the PSN, with potential impact of attack on each such element; certain carriers' network security activities; a major organization's overview of R&D and standards activities; and network security from a switch vendor's point of view. The informational briefings were followed by a Government and industry panel discussion of the issues.

PSN areas of need and Government research. Following the April meeting, six areas for exploration were identified by the subgroup. These are areas that appear to need further research and development that is commercially applicable to the PSN. The six areas, in which Government may have contributions to make, are:

Area 1. A mechanism for easy, portable control of access to a network element, ideally uniform across industry

Area 2. A development to introduce an appropriate level of "suspicion" among trusted elements of the PSN

Area 3. Solutions for reliable recovery from damage to software and databases: if you have a problem, how do you get well?

Area 4. Means to adequately partition memory, or otherwise isolate network element software from databases that are more broadly accessed

Area 5. Means to analyze all events in a network and highlight questionable situations, e.g., exception reports

Area 6. Tools to plan an architecture toward a long-term, more secure network

Action areas proposed to the task force were to identify the six R&D needs to Government, with near-term emphasis to be in the access area; and to explore/support the GSSP by first determining whether NIST was planning to implement such a concept.

A second joint industry/Government meeting was held on 11 July 1991 to informally clarify and interpret industry's statement of the six areas proposed for R&D. The discussion helped identify Government projects and research that correspond to these areas.

A third meeting was held, in September 1991 with Government agencies invited to brief a joint industry-Government audience about: (1) applicable developments that are completed, (2) those requiring modest modification to be commercially applicable, (3) developments underway, and (4) developments planned. The meeting was an occasion for representatives from NIST and NSA to touch on activities broadly ranging over the six areas. Task force comments on each area follow:

Area 1, control of access into network elements from the outside, depends largely on proper password practices, which are difficult to enforce. Smart cards or other token devices could be used in remote access control and would represent a substantial improvement over common practice in the telecommunications industry. Such devices represent state of the art, and applications of token devices to network access and are being researched by NIST and NSA.

Area 2, a development to better control events among the network segments, presents a different and more difficult challenge. The situation in current PSN systems was described earlier by the task force:

> Once a craftsperson passes an entrance security check and remotely enters one system, access to another system is typically not blocked. Therefore, if an intruder penetrates defenses at any point of entry, few internal barriers or challenges are raised. Penetration of any "weak link" in the "chain" of network nodes can permit broad access within the network, even from a remote dial-up location [1].

An NSA-sponsored research effort on the subject of "Mutual Suspicion" was briefed and was subsequently chosen by the group for more detailed and focused consideration at the next R&D Subgroup meeting. Mutual Suspicion for Telecommunications Systems [5] is referred to in the next section and described in more detail in appendix C.

Area 3, providing solutions to reliable recovery, is difficult in telecommunications systems because of the substantial turnover of information in databases that sustain operations. Increasing the frequency of backing up databases, or the efficiency and safety of backup storage, are among the primary solutions, which may be unique to each company's systems.

Area 4, means to isolate network element software from accessible databases, is an area being researched in a range of projects that address multilevel security in computers, directly or indirectly. NSA briefed a number of research projects that could be pursued in small exchange groups with industry representatives, as desired.

Area 5, analysis of network events, is being researched by a number of groups nationwide. Whether in real time, or "after the fact" in audits, appropriate anomaly detection would improve the capabilities to detect intrusions in the PSN. Comprehensive analysis of audit data may require expert systems to reduce the amount of audit data retained and flag relevant information for prompt analysis by humans. Blocking of intrusions through automated anomaly detection means would require sophisticated systems in order to keep from denying authorized actions.

Area 6, tools for use in a long-term, more secure architecture, can evolve from research and development in any of the areas already mentioned. Standards for the development of such tools, such as the GSSP, would allow vendors to focus on developing products that simplify secure internetworking and eliminate unnecessary modifications and multiple testing of equipment models.

Focusing on a priority area. A fourth R&D and Standards Subgroup meeting in January 1992 focused on area 2, or *a development to introduce an appropriate level of suspicion among trusted elements of the PSN*. At this meeting, the Government sponsored a more detailed presentation [5] about work on "mutual suspicion" being conducted under contract to NSA. This is a concept for distributed, heterogeneous systems and networks. It provides a set of principles and guidelines for secure-system design, and for evaluation of systems and networks. It provides suggestions for looking at processing, communications, and management. Suggestions are centered around the importance of several types of access control, and the principle that access control should be governed by authentication uncertainty. The mutual suspicion concept is discussed in greater detail in appendix C.

Generally Accepted System Security Principles (GSSP). In the process of exploring the GSSP concept, the task force determined that:

- NIST has produced a draft Minimum Security Functionality Requirements (MSFR) document [6] that addresses computer system security requirements in general
- A companion document will be issued on assurance aspects of the same subject. It will be made consistent with the Information Technology Security Evaluation Criteria (ITSEC) document and a related manual on evaluation that are currently being worked by Britain, France, Germany, and the Netherlands
- Bellcore's document, FA-NWT-000815 [7], addresses the narrower and more specific topic of requirements for telecommunications network element security
- Bellcore's TA-STS-001194 [8] addresses Operations Systems security requirements
- Bellcore's TA-STS-001080 [9] addresses Operating Environment security requirements

The task force finds that the NIST and Bellcore documents, if made consistent one with another, could be considered a good start toward the development of a consistent stream of network security standards.

2.4.4 Recent Developments in U.S. Government Network Security Strategy

The Report of the Network Security Task Force to NSTAC XII in November 1990 commented: "Current Government sponsored security research is generally not commercially applicable, is restricted in its use, and is not application-oriented." The task force concludes that concerted actions on the part of several Government agencies since the time of that report have largely

overtaken this observation. In particular, new relationships and approaches to information security (INFOSEC) have been initiated by the Defense Information Systems Agency (DISA), NIST, and NSA.

Until several years ago, U.S. Government computer security policies, plans, and practices centered on NSA's "Rainbow Series" and, in particular, the "Orange Book" [10]. These activities were the result of a DOD Computer Security Initiative started in the late 1970s. Under this initiative, the DOD hoped to achieve high levels of computer security on commercially available computer hardware and software products. DOD would specify the security functionality and "trustworthiness" for commercial products; industry would produce the products motivated by their market value; and DOD would certify that the commercial off-the-shelf (COTS) products conformed to the DOD specifications.

By the early to mid-1980s, it was clear that this approach was not succeeding. As recognized recently by a leader at NSA: "The DOD represents only a small share of the overall market for information systems, so very little incentive exists for commercial vendors to provide advanced system security features to satisfy DOD needs. Also, even where trusted products are available, there is very little actual purchasing of these by DOD elements because of higher cost and a lack of understanding of how to use the trusted products in building secure systems [11]."

Although these problems were evident 6-8 years ago, it has taken almost this much time for a new approach to clearly evolve in the Federal Government. There are three key interrelated elements:

- A new Defense-Wide Information Systems Security Program (DISSP) Office has been established with DISA, as the lead agency for establishing security policies, requirements and architectures; and NSA assisting in INFOSEC technology, threat assessment, and risk analysis [12].

- NSA has established system engineering of security as a priority driving thrust in its efforts, and under it has subordinated the certification of security components and products to an appropriate supporting role.

- NIST's charter covers security for unclassified but sensitive information within the Federal Government and NSA will retain responsibility for protecting classified national security information. However, it is likely that NSA will defer to NIST for lower-assurance evaluations (for example, below the Orange Book B2 level).

2.4.5 Convergence in Requirements and Developments

The task force concludes that this new Federal posture will foster increasing convergence between the security requirements of the telecommunications industry and developments in the Federal Government. For example:

- The systems orientation being jointly stressed by DISA and NSA should increase identification and communication of security needs and solutions common to the Federal Government and private industry. For example, activities on mutual suspicion are discussed above and in appendix C.

- The role of NIST in specifying minimum security standards should facilitate common international standards for commercial devices. There is promising cooperation between NIST and European standards bodies where NIST is taking the lead on minimum security functionality and the Europeans the lead on assurance measures. Bellcore's current intention to adopt these standards could have a decisive effect on commercial vendors.

The task force concludes that industry and Government should work together to coalesce around a single set of standards that addresses network security in the public switched network. The set of standards must explicitly address internetworking among different network infrastructures.

This process should have as its objective that telecommunications companies, NIST, and the standards committees work toward consensus on producing mutually consistent standards. The stream of standards that are evolving should culminate in a single, consistent set of network security standards, one that is as small as possible. With a coordinated, minimized set of network security standards in place, future systems can be better integrated so that:

- Users will be aided in selecting appropriate security standards for their systems

- Equipment vendors will be able to focus security developments in fewer channels and thus increase their efficiency of effort

- Service vendors, users, and auditors will be assisted in evaluating compliance with security requirements

The task force further concludes that the exchange of information about Government R&D in the areas identified by the task force has been beneficial to both Government and industry. Another joint Government and industry meeting or set of meetings, held within six months to a year with the objective of continuing progress in this area, is regarded as desirable.

2.5 RISK ASSESSMENT

2.5.1 Background

The conclusions of the task force presented at NSTAC XIII addressed the threat to the PSN, its vulnerabilities to intrusions, and the consequent risk for denial of service to NS/EP users. This report to NSTAC XIV updates the task force assessment of the risk. It was arrived at by reviewing recent specifics on threat and vulnerabilities to identify certain trends.

The prior threat assessment contained in the November 1990 task force report described the hacker threat as targeting the PSN, having sophisticated technical and operational capabilities, using "social engineering" or impersonation as a tool, having a hierarchical information-sharing network including international ties, and individuals with known ties to adversary groups.

Such an adversary group, with sufficient resources to allow the exploitation of the information being disseminated within the hacker network, was regarded as a more serious (potential) threat than hackers motivated primarily by intellectual pursuits. The risk was judged to be highly uncertain because of lack of information about a number of factors, which were spelled out in the report.

2.5.2 Updated Risk Assessment

Threat. Hackers continue to intrude upon both voice and data segments of the PSN. Sensitive Government interests have been affected by intrusions that have adversely affected Government operations.

Although the PSN is best known for its voice service, the network today also includes the public packet switched networks (PPSNs). The original nationwide PPSNs, TYMNET and TELENET, have changed ownership and trade names several times. There are other public data networks as well, e.g., those of Westinghouse, GE, AT&T, and each Regional Bell Operating Company. The public data networks are linked with foreign data networks for global interconnection. These data nets are linked to voice circuits and are interwoven within the PSN.

Hackers have increased sophistication in technical and operational capabilities. As the carriers have increasingly used packet-switched nets, automated tools, and internetworking, the hackers have stayed abreast of the technology and the security protections of the carriers.

Of special concern, known individuals in the hacker community have ties with adversary organizations. Hackers frequently have international ties; telecommunications systems provide almost worldwide access. Telecommunications service is often obtained fraudulently, so physical separation does not prevent the maintenance of relationships among computer criminals.

The age and apparent motivation of intruders appears to be undergoing a gradual change. The average age of those individuals under scrutiny is the mid- to late-twenties. Financial gain appears to be more dominant than before as a motivation for perpetrating intrusions. There is, of course, potential for the recruiting of "insiders" to work with "outsiders." Of course, in every company, disgruntled insiders are a well-known risk even without recruitment from the outside.

Economic distress in the evolving world situation in some cases gives impetus to intelligence efforts to acquire information and advanced technology of commercial value. Recent testimony before Congress indicates almost 20 foreign governments in Asia, Europe, the Middle East and, to a lesser degree, Latin America are carrying out economic intelligence-gathering. Intelligence agents in former communist countries who have been thrown out of their jobs could add to the reservoir of professionally trained intelligence mercenaries. A number of witnesses at

congressional hearing testified that economic espionage by foreign governments and companies that will harm U.S. interests is on the rise or will rise.

The number of attempted intrusions through international gateways from abroad is increasing. Although major carriers have increased their abilities to resist, there has been a lot more cleverness demonstrated in those who are trying to break through the gateways, at times achieving administrative privilege over the carrier's network management center system.

Traditionally, intelligence services have been interested in disruption as well as in collection. While early concern about organized hacker activities was well placed, it is a leap to connect "demonstrated collusion among hackers" to "group intent to take down the PSN." To date reporting has not made a close connection. However, with respect to the potential for extraction of significant information, the value of the PSN as an intelligence target---that is, a source of information for intelligence-gathering---is clearly established.

As reported by the "scoping" task force, a serious **potential** threat exists: a resourceful adversary starting with the hacker information base. Increasingly, it appears that such an adversary could penetrate the PSN and monitor or disrupt telecommunications serving NS/EP users.

Collusion. Collusion among hackers has been demonstrated in the last several years. Individuals in an organized effort are assigned tasks on the basis of their areas of software and hardware expertise. Besides skills in electronic intrusion, skills in physical entry into network facilities and modification of facility circuitry have been documented----a good example is the Kevin Poulson case currently in litigation in California.

The hackers organize, in a "pecking order," to obtain and share information. The most detailed information is shared on a restricted basis. For example, a dozen or more individuals will associate under a cognomen and may utilize a "top-level" electronic BBS, with identities masked by aliases. Among some hacker circles, there is open talk about how to intrude.

It is routine for top-level hackers to exploit those in lower levels to carry out their intent. There are some BBSs that all hackers can use. However, in order to join a higher-level group and gain access to its information, individuals are required to prove themselves, e.g., "Get me admin privileges on ten systems." To do so they may be required to perform tasks that serve the purposes of the higher level and that involve illegal acts.

Techniques. Hackers continue to "social engineer," to impersonate company personnel in order to extract even more detailed information than before. One group of hackers relied significantly on impersonation to achieve their purposes.

In addition, during 1991, observers have seen an escalation in the technical expertise of intruders. There has been a dramatic increase in electronic intrusion skills, shifting away from the use of "brute force" methods used earlier to gain access.

Packet-switched circuits are being used as a pathway to get to data and software that control switched circuits (both data and voice); subsequently, traffic has been diverted and reconfigured. In certain cases, the intruders are using the data network to manage the voice networks.

A recent development in the use of hacker tools is an ability to completely circumvent passwords. Hackers have gained unauthorized access to a utility program that allows an intruder to "sit on" a circuit at a node and collect logons and passwords as they go through on the circuit. This technique allows even "strong" but reusable passwords to be compromised. After logging in utilizing a purloined password, a hacker can implant a "Trojan horse" program to gather information from the circuits that they choose to target.

Dialback modems for access control have been defeated by (1) intruding into network element database information and diverting the dialback calls to an intruder's phone, or (2) by tricking the callback unit into dialing out into the intruder's session by simulating the network tones and sequences that the dialback unit is expecting.

In addition, modems have been covertly connected directly off switches. Physical penetrations are supported by information shared on BBSs about picking or loading locks and defeating cipher locks.

While intruders have "hacked" directly into the PSN carrier's software, others went through data nets to get to the software/data that controls all PSN traffic. In one case, for example, hackers used the following route: from a public data net, to an interexchange carrier (IEC) net, to a local area network X.25 product, to an operations support system (OSS) used to monitor the health of the network over a statewide area.

Vulnerabilities. Penetrations continue to exploit weaknesses in security practices and in protection mechanisms, or firewalls, in Network Elements, Operations Systems, and Operating Environments.* Some equipment vendors continue to produce weak systems and hackers find the systems' weaknesses and exploit them; intruders are also much more capable of detecting previously unrecognized flaws.

Previously adequate security practices are now being compromised by techniques cited above, e.g., dialback modems are being defeated, and modems have been connected directly off switches, thus defeating dialup access controls. Planting a Trojan horse to get logons and passwords as they pass by (the "packet-switched" technique) also allows covert access over the X.25 network. This type of intrusion is often repeatable, as well as difficult to detect. Subsequent logons using the stolen password constitute impersonation of legitimate users.

---

*Examples of Operating Environments are UNIX, registered trademark of Unix Systems Laboratories; SunOS, registered trademark of Sun Microsystems; and AIX, registered trademark of IBM.

The public data nets serve as data communications pipes between customers, including those who can access the pipes with a portable terminal. Hackers have used these pipes to plant a Trojan horse so as to take control of network element functions, diverting and reconfiguring traffic.

Countermeasures. There should be an effort to spread a firewall around all of the Operations, Administration, Maintenance and Provisioning (OAM&P) of a company. If a large geographical area is involved, with many network elements, firewalls should be installed between network domains. However, access should be possible using a single token and passing that user ID among network elements; otherwise, craftpersons will have to have separate tokens for each network element, which would be cumbersome.

There remain issues about what form of network protection should be implemented first, if all cannot be undertaken. If, for instance, a Network Operations Center has access to it protected by a token system (use of a one-time password), this represents a firewall. However, if someone "hangs" a modem off the operations center, then there is a "crack" in the firewall. This raises the issue of the value of the extra effort and expense of buying the token system for dialin access, if it can be circumvented because of the lack of other protections.

Risk. There is a growing dependence on computers in telecommunications systems. Data networks' interconnections are increasingly automated and, without the presence of appropriate firewalls, they can extend the vulnerability of any system to those to which it is connected. The best security in any network currently can be undermined by connectivity to a poorly defended network.

As a result of the introduction of common channel signaling, data network bridges now connect Signaling System Number 7 (SS7) network element islands. This concentrates information flow in fewer network elements, i.e., Signal Transfer Points (STPs), and leads to greater vulnerabilities. In addition, the current move to interconnect STPs across company boundaries potentially provides the hacker with more paths to explore, and could extend his geographic "reach" dramatically.

Table 1 illustrates, by type, penetrations of operations support systems, network elements, and X.25 networks that have affected network integrity in the past. Results of each type of intrusion are also given. It should be noted that intrusions of a type already experienced *could* result in service shutdown. The consequence of disrupting both of the mated pair of Signal Transfer Points' is that common channel signaling call setup can stop, with significant reduction in communications capabilities.

The risk to the PSN as a whole, a function of vulnerabilities and threat, remains difficult to quantify. The threat is currently recognized by service providers and vendors and steps are being taken to address the problems of *current* networks. However, the development cycle on network elements is too long a process to assure quick, permanent solutions.

In general, the NSIEs, the task force, and the panel for NSIE evaluation believe that the risk of harm to U.S. interests from hacker intrusions is higher than the lower of two possibilities it

Table 1. Intrusions Affecting Network Integrity

Type of Target	Result
Service Control Point (SCP)	Unauthorized accounts added
Signal Transfer Point (STP)	Shutdown of single mate of pair
Network Element (NE)	*Recent Change memory modified/ service interrupted
NE Memory Operations	*Recent Change modified/lost
Provisioning System	Unauthorized service enabled
Loop Maintenance System	Communications monitored
Documentation Support System	Proprietary information stolen
X.25 Packet Network	Diagnostic tools compromised, communications monitored and access controls (e.g., closed user groups) defeated
Central Office (physical entry)	ID badges and keys stolen
Digital Crossconnect System	OAM&P accounts added, Administrative (e.g., superuser) privileges gained

*Believed due to intruder's attempt to cover tracks

originally reported in their report [1]. It should be further noted that the move to use *open systems standards, such as X.25 and Open Systems Interconnection platform, can make penetration easier unless adequate protection is supplied.*

The task force is concerned that security aspects of *future* PSN systems and systems interconnection currently lack a unified focus or approach. No single standards group is addressing network security on an end-to-end basis. The work being done by NIST in coordination with European bodies acknowledges the importance of cooperative effort at a time when international internetworking is growing.

The task force believes that, as a corollary of the international coordination process, *U.S. industry and Government need to coalesce around a single consistent set of security standards that can be applied to reduce vulnerability in the PSN.* The task force regards such an effort as instrumental in reducing risk to U.S. interests from electronic intrusions.

2.6 FUTURE DIRECTIONS

The task force concludes that further work in network security should:

- Foster a total system view of PSN security, recognizing its interconnected nature and the need for standards for, and implementation of, commercially applicable network security measures.

- Expand the scope of network security activities, focusing on industry-wide information exchange as well as research and development that will benefit the PSN.

Further NSTAC efforts could be focused in several areas:

Area 1. To evaluate the NSIE and pursue follow-on efforts. In view of the importance of the network security area, follow-on efforts relating to it are appropriately elevated to the IES level. The responsibility for the governance and evaluation of the NSTAC NSIE could be assigned to a small panel of IES members with a chair to lead and represent the panel. Four to six IES representatives could be selected to constitute this panel, but allow IES representation from any NSTAC member company that wishes to attend. The following functions need to be performed:

- Monitor the entire NSIE process and provide support or direct initiatives that will improve effectiveness of the NSIE process.

- Evaluate, in conjunction with the GNSS, the effectiveness of the NSIE process and, in particular, the NSTAC NSIE.

- If there is consensus that an industrial NSIE is desirable, act as a core group to initiate migration of the industrial component out from NSTAC sponsorship.

Area 2. To actively foster the emergence of a single consistent set of network security standards for the PSN. The subcommittee could establish a group of industry experts from NSTAC member companies that could be proactive on the development and adoption of a single consistent set industry-wide. This work is best done by a group of experts with design and operations expertise and standards awareness. The experts could work with the standards community, aiming to provide guidance and motivation to standards bodies to get interested and active in this area. Priority areas of focus could be access control and defining the right firewalls to protect interconnected systems from intrusions. The experts of the group could:

- Interact directly with standards bodies
- Identify a proposed framework for completing a set of network security standards that are consistent with each other
- Identify methods to advance completion and adoption of such a standards set in a timely manner
- Identify need and actions required, if appropriate, to establish a separate standards body for PSN security

Government participation in this activity could be welcomed.

Area 3. Continue involvement in R&D information exchange. The IES subcommittee could sponsor another joint industry/Government meeting, or set of meetings, focusing on the R&D needs areas described in this report. It could also identify a mechanism to continue information exchange between industry and Government, beyond the lifetime of task force sponsorship, on the needs of the PSN for research and technical development.

Area 4. Represent the NSTAC, on NSIE matters, to the Federal Communications Commission's Network Reliability Council (NRC). The NRC has recognized the NSIE as the appropriate body to address the reliability aspects of the PSN relating to electronic intrusions.

Area 5. Represent the NSTAC to the Government Network Security Subgroup. The IES needs a continuing relationship with the Deputy Manager, OMNCS, and the Government Network Security Subgroup that he chairs. Such a link can communicate industry activities to the Government and assist coordination with Government in efforts that require a joint focus.

Area 6. Support the IES on other network security-related issues. Needs not encompassed in the above activities could be addressed as they arise.

The IES could, as a consequence of transferring responsibility for overview of network security activities to a more permanent base, deactivate the Network Security Task Force.

SECTION 3

RECOMMENDED ACTION PLAN FOR THE IES

The Network Security Task Force recommends that the IES:

1. Request that the NSTAC endorse an NSTAC initiative as stated in section 4.

2. Create a small IES Network Security Subcommittee (four to six IES members), with a chair to lead and represent the subcommittee. Any other IES representative would be welcome to attend meetings of the Network Security Subcommittee. The Subcommittee should:

   a. Oversee the Network Security Information Exchange. The subcommittee will monitor and evaluate the entire NSIE process and provide assistance and guidance to the NSTAC NSIE; if called for, it will recommend a follow-on NSIE mechanism and act as a core group to initiate migration of the industry component out from NSTAC sponsorship.

   b. Establish and oversee the proposed NSTAC Network Security Standards Oversight Group. The subcommittee will establish, from NSTAC member companies, a group of industry experts who will actively foster the development and adoption of a single consistent set of network security standards for the PSN. The experts will be individuals with design and operations expertise and standards awareness. Standards will embrace architecture, design, operations, interfaces, and assurance. The experts will work with the standards community, providing them with guidance and motivation to develop and accept industry-wide standards of the above nature. Aiming to get standards bodies interested and active, the experts of the group will:

      (1) Interact directly with standards bodies

      (2) Identify a proposed framework for completing a set of network security standards that are consistent with each other

      (3) Identify methods to advance completion and adoption of such a standards set in a timely manner

      (4) Identify need and actions required, if appropriate, to establish a separate standards body for PSN security

   Government participation in this activity, where appropriate, is to be welcomed.

c. Continue involvement in R&D information exchange. The subcommittee will identify a mechanism to continue information exchange between industry and Government about the needs of the PSN for research and technical development.

d. Represent the NSTAC, on NSIE matters, to the Federal Communications Commission's Network Reliability Council.

e. Represent the IES on matters relating to network security (including the NSIEs) in dealing with the Deputy Manager, OMNCS, and the Government Network Security Subgroup that he chairs

f. Support the IES on other network security-related issues

3. Recommend that the Chairman of the NSTAC write a letter to the President that:

a. Informs him of the NSTAC initiative and a projected objective that industry and, where appropriate, Government *coalesce around a single set of standards and working agreements to reduce network security risks in the public switched network.*

b. Transmits the proposed NSTAC statement in section 4

c. Asks him to publicly support the NSTAC initiative

d. Recommends that he establish a Government focal point for network security standards where coordination and unified action are required.

4. Deactivate the Network Security Task Force.

SECTION 4

PROPOSED NSTAC PLAN OF ACTION

Whereas

Electronic intruders have demonstrated the capability to (1) deny, or interfere with, PSN service to targeted users and; (2) extract significant information from targeted circuits

The NSTAC is sponsoring an exchange of information among NSTAC companies on the threat, vulnerabilities, incidents and countermeasures relating to electronic intrusions and manipulations of elements of the PSN

The NSTAC's awareness of the need to reduce network security risks in the PSN of the future has been heightened since 1990, and

As a consequence the NSTAC recognizes that the security of all networks in the PSN must not depend upon the security of the weakest interconnected network

the NSTAC will provide impetus for a concerted effort to reduce risks to the PSN from electronic intruders in current systems, to foster related information exchange conducted broadly across the telecommunications industry, and to take steps to enhance the network security of current and future systems.

As part of this initiative, the NSTAC Principals will:

1. Continue to support the NSTAC Network Security Information Exchange, as needed, at least until NSTAC XV in the spring of 1993, to include approval of staff and resources for exchange of information on analysis of vulnerabilities and detailed evaluation of incidents to determine root causes and evaluate countermeasures

2. Provide needed resources and staff for an NSTAC NSSOG, consisting of individuals with design and operations expertise, to work with the standards community and actively foster a single set of network security standards for the PSN

3. Endorse joint industry and Government exercises to test the capability to work together to mitigate security problems

The NSTAC Principals will further act to promote, within their own organizations, a greater level of awareness of network security.

The NSTAC will ask the President to publicly support the NSTAC initiative, and to establish a Government focal point for network security standards where coordination and unified action are required.

LIST OF REFERENCES

1. *Report of the Network Security Task Force*, November 1990, National Communications System, Arlington, VA, pp. 22-26.

2. Memo, Chairman of the PCC-NSTIS to the Manager, NCS, April 23, 1990.

3. *Status Report of the Network Security Task Force for NSTAC XIII*, August 1991, National Communications System, Arlington, VA.

4. *Computers at Risk, Safe Computing in the Information Age*, 1991, National Research Council, National Academy Press.

5. Nelson, Ruth, "Mutual Suspicion for Telecommunications Systems," GTE, Network Security Task Force, January 30, 1992.

6. Minimum Security Functionality Requirements for Multi-user Operating Systems, Draft, Issue 1, National Institute of Standards and Technology, January 16, 1992.

7. *Generic Framework Requirements for Network Element and Network System Security, Framework Technical Advisory*, FA-NWT-000815, Issue 1, Bellcore, December 1991.

8. *Bellcore Operations Systems Security Requirements*, June 1991, Technical Advisory, TA-STS-001194, Issue 1, Bellcore.

9. *Bellcore Standard Operating Environment Security Requirements*, June 1991, Technical Advisory TA-STS-001080, Issue 2.

10. Department of Defense Trusted Computer System Evaluation Criteria, December 1985, DOD STD 5200.28.

11. John C. Nagengast, "Defining a Security Architecture for the Next Century," January 1992, *Journal of Electronic Defense*, pp. 51-53.

12. Defense-Wide Information Systems Security Program (DISSP) Action Plan, August 1991, Defense-Wide Information Systems Security Program Office.

APPENDIX A

TASK FORCE PARTICIPANTS

Task Force Members

AT&T	Mr. Dave Bush	ITT	Mr. Joe Gancie
Bellcore	Mr. Randy Schulz	McCaw	Mr. Richard McElhenie
Boeing	Mr. Bob Steele	MCI	Mr. Joe Cassano
Comsat	Dr. Al Dayton	NTI	Dr. Jack Edwards
GE	Mr. Don Pidgeon	GTE	Mr. Jim Moore
Sprint	Mr. G. Jay Nelson	UNISYS	Mr. Herb Benington, Chair

Other Participants

GTE	Mr. Lowell Thomas	MMC	Mr. John Hocker
Harris	Mr. Bob Domino	NTI	Mr. Bob Petrie
US West	Mr. Jon Lofstedt		

Task Force Support

Office of the Manager, NCS Joint Secretariat	Major Gordon Powell
MITRE Corporation	Ms. Eleanor Harris Ms. Jaton' West
Booz-Allen & Hamilton, Inc.	Mr. Ted Phillips Mr. LeRoy Schubert
Special Advisor	Mr. Henry Kluepfel, Bellcore

APPENDIX B

R&D AND STANDARDS SUBGROUP

Subgroup Members

AT&T	Mr. Dave Bush	NTI	Dr. Jack Edwards
Bellcore	Mr. Randy Schulz	Sprint	Mr. G. Jay Nelson
Boeing	Mr. Bob Steele, Chair		

Subgroup Support

Office of the Manager, NCS Joint Secretariat	Major Gordon Powell
MITRE Corporation	Ms. Eleanor Harris
Booz-Allen & Hamilton, Inc.	Mr. Ted Phillips

APPENDIX C

MUTUAL SUSPICION
BRIEFING AND DISCUSSION HIGHLIGHTS

The concept of Mutual Suspicion relates to the identified need for a development to introduce an appropriate level of suspicion among trusted elements of the PSN. While the research described most directly applies to Area 2, it is related to Areas 1, 5 and 6 as well. Mutual Suspicion was assigned first priority for a more detailed briefing as a step to initiate follow-up on subjects identified during the September 1991 R&D and Standards Subgroup meeting.

Mutual Suspicion research, being pursued under contract to NSA, was briefed [5] by the contractor and discussed with those present at the R&D Subgroup meeting. Related and consequent issues were discussed at the subsequent NSIE and task force meetings. The pivotal points, from the standpoint of the task force, are abstracted in the following paragraphs.

The research on mutual suspicion is conceptual, with no solution yet determined. However, the presentation represented an initial approach to solving the following problem:

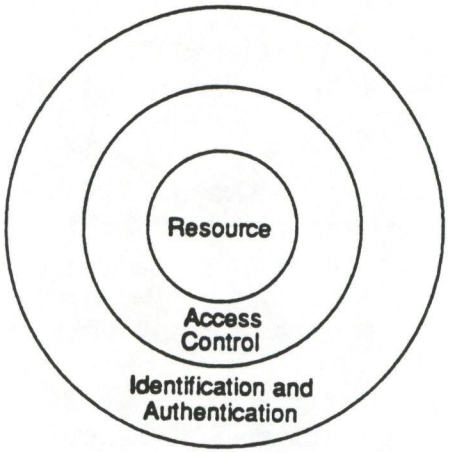
> Since you can't have control over the whole world (in this case, the PSN), you must put protections around your own world, which you do have control of (your own system).

The presenter emphasized that trust is not an absolute, it is a measure of risk. In setting up a network with adequate security, one cannot absolutely guarantee that nothing will go wrong. However, a failure should not "do in" the network, allowing an intruder to have access throughout the system, and potentially into other systems or networks.

In large networks such as the PSN, communication connectivity is constantly changing in ways beyond the control of each system in the network. The risk depends on the size of the network and the number of potential interconnections. A large network without firewalls is a vulnerable target, where the weakest point may provide entry, and the penetrated system may be used to gain further access.

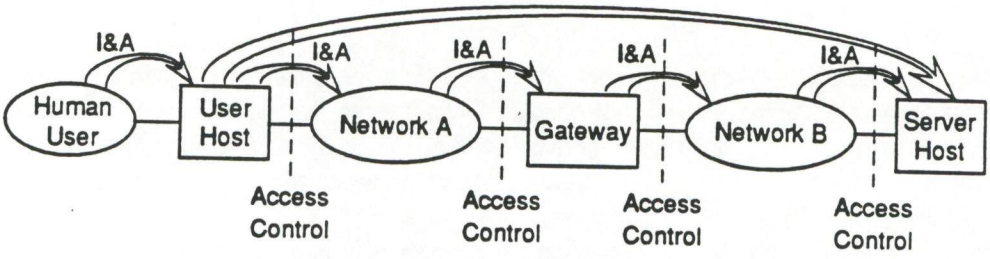
In addressing network security against hackers, users with no legitimate access are a problem. The Orange Book addresses users that are already in the network, but are without full privileges. One of the most difficult problems to be addressed in large networks is that user characteristics are hidden by the network, and that the user may have significant processing help in mounting an attack---for example, a Cray computer can dial in looking like a dumb terminal.

Local control of resources according to local policies. Computing capability, data, and communications are resources that must be protected by each resource owner. Enforcement of access control can reflect different policies across the network. Authenticated identification (implicit or explicit) is needed for access control.



Identification and authentication function is the outer ring of protection around the computing or communication resource.

Figure C-1a



Each resource owner makes independent access control decisions based on the authenticated identity of the requester of the service.

Source: Nelson, 1992

Figure C-1b

Figure C-1. Mutual Suspicion Concepts

Each resource owner must enforce its own policy. Policies of all owners must be consistent to permit secure resource sharing. The access control policy of each user should include label-based, identity-based, and functional access control.

While there has been strong emphasis in DOD work on label-based (labels such as Secret, etc.) access control, there is a great need for identity-based access control as well, whenever and wherever there is a need to distinguish one individual from another. While the use of passwords was developed initially to address identity-based access control, the use of one password by a number of individuals who are members of a group defeats the objective of identifying individuals. In addition, proper password discipline is difficult to enforce.

Functional access control, which hasn't been addressed as strongly as the other two areas, should adhere to the principle of limitation of access to the level of authentication uncertainty. That is, uncertainty about authentication can be used to limit user access (see figure C-1). For example, if only the owner of information can appropriately change that information--say, a directory entry--then the network should not allow "just anyone" who is on the network to change it.

Access control is necessarily limited by the authentication information used to make the decisions. The identification and authentication function should be the outer ring of protection around the computing or communication resource (see figure C-1a).

Access control by authentication uncertainty. Uncertainty inherent in the type of authentication information should limit access to the computer or communications resource. If the user is authenticated, then the user should get access privileges. If only the user's host is authenticated, then the user should get the minimum privilege of any user on that host. If only network connection is authenticated, then the user should get the minimum privilege of any network user. Superuser and Diagnostic Access ought to be limited to local users only or very strongly authenticated users from specific, authorized sites.

Network-based auditing. Network protocols give information about the source of a remote terminal access: link, network address, remote host. This information can be correlated with log-on information for access control decisions and auditing. Use of this capability would have allowed recent intruders to be traced much more easily, but current systems throw the path information away. A system given as an example records only the port number of the local computer port---although the information about the source of the access is present at the time of system entry because of protocols, it is not kept; it would be useful if it were.

Network firewalls. Each resource owner should make independent access control decisions based on the authenticated identity of the requester of the service. Redundant, independent security mechanisms should exist at key points across the full reach of any data connection (see figure C-1b). Identification and authentication should precede access at junctions between networks. The firewalls so formed would limit the extent of damage caused by failure or subversions. Pairwise encryption keys can be utilized in the process.

Resources to be protected in telecommunications systems include communications service, processor data, and processing capability. Pieces of the internal system should be authenticated to each other. Both machines and people are involved in the operation of any network. Machine-to-machine authentication should identify a machine as part of the network or as an internetwork interconnection. People with special privileges must be authenticated to machines, and machines must be able to determine the privileges of the identified person.

To accomplish interconnections of telecommunications systems, protocol standardization is necessary and represents progress. Connectivity and compatibility don't automatically mean access. Resource control should always limit access according to policy. Firewalls and conservative management algorithms will limit damage from security failures.

GLOSSARY

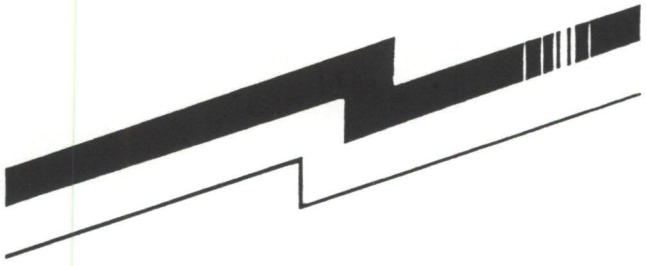
BBS	Bulletin Board System
CIA	Central Intelligence Agency
COTS	Commercial off the shelf
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISSP	Defense-Wide Information Systems Security Program
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
GNSS	Government Network Security Subgroup
GSA	General Services Administration
GSSP	Generally Accepted System Security Principles
IEC	Interexchange Carrier
IES	Industry Executive Subcommittee
INFOSEC	Information security
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
MSFR	Minimum Security Functionality Requirements
NCC	National Coordinating Center
NCS	National Communications System
NE	Network Element
NIST	National Institute of Standards and Technology
NRC	Network Reliability Commission
NSA	National Security Agency
NS/EP	National Security and Emergency Preparedness
NSC	National Security Council
NSIE	Network Security Information Exchange
NSSOG	Network Security Standards Oversight Group
NSTAC	National Security Telecommunications Advisory Committee
NSTIS	National Security Telecommunications and Information Systems
OAM&P	Operations, Administration, Maintenance and Provisioning
OMNCS	Office of the Manager, National Communications System
ONA	Open Network Architecture

OSI	Open Systems Interconnection
OASD-C3I	Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence
OSS	Operations Support System
OSTP	Office of Science and Technology Policy
PCC-NSTIS	Policy Coordinating Committee on National Security Telecommunications and Information Systems
PPSN	Public Packet Switched Networks
PSN	Public Switched Network
SCP	Signal Control Point
SS7	Signaling System 7
STP	Signaling Transfer Point
USSS	U.S. Secret Service

Enhanced Call Completion (ECC)
Task Force
Report

Final Report of the Enhanced Call Completion (ECC) Task Force

July 1992



Enhanced Call Completion (ECC)
Task Force
Report

Final Report of the Enhanced Call Completion (ECC) Task Force

July 1992

Final
Report of the
Enhanced Call Completion
(ECC)
Task Force

Distribution of this report is approved within the telecommunications industry and to selected individuals

Final

July 1992

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF EXHIBITS

LIST OF TABLES

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

In December 1990, the Industry Executive Subcommittee (IES) of the National Security Telecommunications Advisory Committee (NSTAC) charged the Enhanced Call Completion (ECC) Task Force to investigate the technical feasibility of enhancing call completion for national security and emergency preparedness (NS/EP) users during periods of public switched network (PSN) congestion or damage. The task force first identified features that could enhance access to, transport through, and egress from the PSN. It later addressed regulatory, competitive, and standards issues that might impede implementation of ECC features.

The ECC Task Force's investigation focused primarily on providing NS/EP calls with preferential treatment in the PSN. The task force determined that special features available only to NS/EP identified users must be implemented in the PSN to ensure NS/EP calls a higher probability of call completion than general public calls. Network-based call-by-call features have been identified. In order for the NS/EP user to take advantage of these features, the NS/EP call must be identified and its identifying mark transported along the call path through the network. Although there are several ways to invoke the identification of an NS/EP call, the task force agreed the High Probability of Completion (HPC) standard would be the most effective means for transporting the NS/EP identifier in the Signaling System No. 7 (SS7) network. The HPC standard is in jeopardy within the Exchange Carrier's Standards Association (ECSA) T1S1 Committee. The Government and the NSTAC should continue to actively support the HPC standard to ensure its near-term adoption because it is a fundamental requirement for developing ECC services.

The task force looked at features and capabilities to enhance end-to-end call completion. Its study revealed that some features will also improve network reliability through redundancy. The task force's report identifies several existing and planned features and capabilities that the Government should investigate to enhance call completion. Some of these features are dependent on the NS/EP call identifier and some are not. This report describes the NS/EP application, availability, and acquisition procedures for each feature and for the NS/EP call identifier. In the appendices of the report, the task force also identifies PSN access and egress related capabilities for customer premises equipment (CPE), PSN augmentations available to the NS/EP user, and future enhanced call completion capabilities the Government should monitor.

The ECC Task Force recommends that the IES establish an ad hoc group of former ECC Task Force members to assist the Government in receiving active support from industry for the near-term adoption of the HPC standard. In addition to using existing PSN features, the Government should take the necessary steps to implement new PSN features and capabilities to achieve greater enhancement of NS/EP call completion. These steps include sponsoring industry forums to define ECC functional requirements and to resolve implementation issues. The task force recommends that the

Government work with the NSTAC's Funding and Regulatory Working Group (FRWG) to investigate potential regulatory issues associated with authorizing and requiring NS/EP call-by-call preferential treatment in the PSN. Finally, the task force recommends that the Government use the ECC Task Force report as a reference in modifying or implementing current or future services and technologies in the PSN.

1.0 INTRODUCTION

1.0 INTRODUCTION

1.1 PURPOSE AND ORGANIZATION

The ability for national security and emergency preparedness (NS/EP) users of the public switched network (PSN) to complete calls during emergencies is a national concern. This document identifies existing and potential features to enhance call completion and defines the necessary steps to acquire nationwide enhanced call completion (ECC) services. The document is organized as follows:

- Section 1.0 – Provides background for the enhanced call completion issue and establishes the framework for the task force
- Section 2.0 – Addresses the Government's requirements for enhanced call completion capabilities
- Section 3.0 – Reviews the current state of the industry and examines regulatory, competitive, technical, and standards issues that impact enhanced call completion
- Section 4.0 – Describes the requirement for an NS/EP call identifier that would give preferential treatment to NS/EP calls in the PSN
- Section 5.0 – Identifies current and potential features that enhance call completion and may rely on an NS/EP call identifier
- Section 6.0 – Discusses the impact of ECC services on the PSN and the general public
- Section 7.0 – Defines the procedures necessary for the Government to obtain a nationwide enhanced call completion service
- Section 8.0 – Presents the conclusions of the task force
- Section 9.0 – Presents the recommendations of the task force.

1.2 BACKGROUND

At its August 22, 1990 meeting, the Industry Executive Subcommittee (IES) Funding and Regulatory Working Group (FRWG) recommended establishing the NS/EP ECC Task Force. The FRWG's recommendation resulted from its investigation of regulatory issues that affected the NS/EP caller's ability to request automatic hunting for an alternate long distance carrier if its primary interexchange carrier (PIC) is unable to complete the call. The Government defined this ability as "assured access." Discussions between the Government and the FRWG resulted in the conclusion that the Government had additional concerns, such as the preferential transport and termination of NS/EP calls

through the PSN. Therefore, the FRWG recommended the establishment of a new task force to determine how current and potential technologies and services could ensure the NS/EP user increased access to the PSN and enhanced completion of the call without interruption, with minimum delay, and on a preferential basis during network damage or congestion.

As a result of the FRWG's recommendation, the National Security Telecommunications Advisory Committee (NSTAC), at its December 13, 1990 meeting, tasked the IES to establish a task force to investigate the means to enhance call completion for NS/EP users during periods of congestion or damage to the PSN.

1.2.1 Task Force Charge

The NSTAC charged the task force to:

- Define enhanced call completion
- Identify technical approaches/requirements for enhanced call completion
- Investigate technical aspects of automatic call rerouting
- Identify and evaluate alternatives for enhancing existing National Communications System (NCS) programs and initiatives, especially Telecommunications Service Priority (TSP)
- Assess impact of enhanced call completion on PSN
- Recommend an enhanced call completion plan of action for near- and long-term enhancements
- Report findings and recommendations by NSTAC XIV.

On December 19, 1990, the ECC Task Force, composed of representatives from AT&T, Bellcore, Contel, GE, GTE, McCaw Cellular Communications, MCI, NTI, PTI, and Sprint convened its first meeting and elected Dr. Sushil Munshi, Sprint, as Task Force Chairman. See Appendix A for the current task force membership.

1.2.2 Definition of Enhanced Call Completion

In response to its first charge, the task force defined the concept of enhanced call completion as follows:

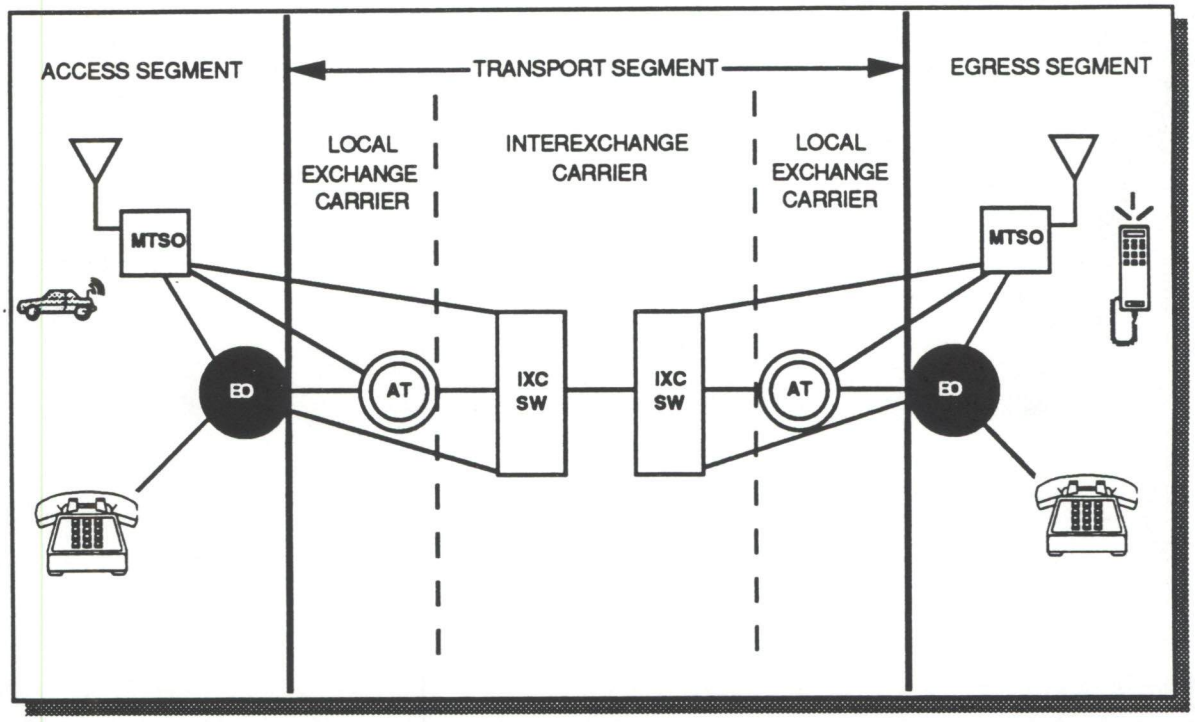
> Enhanced call completion is a set of network features and capabilities that permit NS/EP users to complete calls over the PSN with minimum delay during network damage or congestion. Additionally, network damage

and/or congestion includes extraordinary levels of physical stress and traffic overload caused by natural or man-made phenomena.

1.2.3 Task Force Work Plan and Methodology

The task force examined three segments of the PSN: access, transport, and egress, shown in Exhibit 1-1.

EXHIBIT 1-1
Wire Line and Mobile Access, Transport, and Egress Segments of the PSN



LEGEND	
AT	= Access Tandem
EO	= End Office
IXC SW	= Interexchange Carrier Switch
MTSO	= Mobile Telephone Switching Office

The task force identified and evaluated existing, planned, and potential features in the three segments of the PSN, illustrated in Exhibit 1-1, that could enhance NS/EP call completion. The task force described each feature, its NS/EP application, its availability, and the steps necessary to acquire it. The task force also investigated possible impediments to implementing ECC services by examining regulatory, competitive, technical, and standards issues. During the final stage of its investigation, the task force formulated procedures for obtaining nationwide enhanced call completion services. The task force's evaluation of ECC features and capabilities is presented in Section 5.0 and Appendices C and D.

2.0 STATEMENT OF GOVERNMENT'S NS/EP REQUIREMENTS

2.0 STATEMENT OF GOVERNMENT'S NS/EP REQUIREMENTS

The Government needs industry assistance and support in initiating, coordinating, restoring, and reconstituting NS/EP telecommunication services during all circumstances that impair service, including conditions of crisis or emergency, to meet the requirements of Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions.* The Government recognizes that the PSN is not engineered to provide 100 percent availability of telecommunication services continuously, and under all conditions. However, during periods of stress, the PSN should grant a higher level of service for NS/EP users than is available to the general public. To meet these requirements, NS/EP users may need to subscribe to, or otherwise arrange for, special telecommunication services that provide increased reliability during periods of network damage and/or congestion.

In addressing the problems of network damage and/or congestion, the Government has two basic objectives: First, NS/EP users should have a higher probability of timely call completion, beginning with priority receipt of dial tone; and second, the services should be economical and technically feasible.

The next section analyzes the state of the PSN and the regulatory, competitive, technical, and standards issues that might affect the Government's ability to obtain a higher level of service for NS/EP users.

3.0 SUMMARY OF ISSUES—STATE OF THE INDUSTRY

3.0 SUMMARY OF ISSUES—STATE OF THE INDUSTRY

The PSN is designed to provide equitable daily telecommunications service to all users. However, system stress caused by natural or man-made disasters, can dramatically increase the demands upon the PSN's surviving assets and cause its services to be degraded.

Typically, the Government's need for telecommunications service increases during emergencies as the NS/EP community responds. This can further increase the stress on the PSN and thus deny the NS/EP community the level of service it needs. To prevent this, many NS/EP users have augmented their telecommunication services with extensive private line networks that are considered to be immune to PSN congestion.

The telecommunications industry is challenged to provide the NS/EP community with the preferential treatment it needs during periods of stress, while still providing its business and residential users with the best possible service. This challenge was addressed by the ECC Task Force.

The task force has identified several regulatory, competitive, technical, and standards issues that are relevant to implementing enhanced call completion services for the NS/EP user in the PSN. These issues are discussed in this section.

3.1 REGULATORY ISSUES

Three regulatory issues need to be addressed to provide NS/EP users with preferential treatment:

1. The facilities of the PSN are available for equal use by the Government and the public. Providing one user community preferential treatment at the expense of other users without a waiver from the Federal Communications Commission (FCC) may be in violation of the universal service concept embodied in Section 202 of the 1934 Communications Act.

2. The community of NS/EP users should include Federal, State, and local government users with emergency responsibility. If State and local government users are not included, state regulators may be concerned that State and local emergency and essential PSN services will not be available when needed because preferential treatment is given to the Federal Government. This uncertainty could spur protracted concerns over the ability of the local exchange carriers (LEC), interexchange carriers (IXC), and cellular carriers to provide equal and ubiquitous services within the PSN.

3. The question of who should bear the burden of the cost to improve NS/EP services should be resolved. The regulatory process mandates

that users who create costs be charged service rates that fully recover those costs. Although it is certainly possible to charge NS/EP users for selected ECC services and features, the regulatory pressure to ensure all costs are recovered from the cost causer may make some ECC capabilities prohibitively expensive.

3.2 COMPETITIVE ISSUES

The present competitive and economic pressures on the telecommunications industry often work against the objectives of the NS/EP user community. Service providers are concerned with ways to reduce costs, increase return to shareholders, and maintain competitive services. It is conceivable, therefore, that some service providers might be reluctant to provide ECC services because of low volume and/or low revenue potential. This is a concern because any reduction in the number of participating service providers would jeopardize the availability of ubiquitous ECC services.

3.3 TECHNICAL ISSUES

The PSN has undergone a great technological evolution in the past 10 years. Innovations in its transmission systems, switching systems, signaling systems, wireless technologies, and network support systems allow the industry to provide more features. Applications of these features that can enhance NS/EP call completion are discussed in Sections 4.0 and 5.0.

3.3.1 Transmission Systems

The telecommunications industry has adopted fiber optic technology as the digital transmission system of choice because of its economy, its increased channel capacity, and its premium quality.

Initially, fiber optics were deployed as point-to-point systems. This practice created a vulnerability because there was usually insufficient capacity in other transmission systems to restore the services disrupted by a failed fiber optic system. However, as the industry continues to deploy fiber optic transmission systems in the PSN, it closes these point-to-point systems into rings or loops. This allows for rapid restoration of failed service between two end points because traffic is transmitted in both directions around the ring.

To increase the efficiency of the PSN and dramatically enhance its service restoration capabilities, industry is deploying more sophisticated multiplexing and control systems in the PSN. Multiplexing systems are evolving into intelligent, remotely controlled digital cross connect systems and transmission switching hubs. These systems are being augmented with Synchronous Optical Network (SONET) transmission technology. This will result in more efficient transmission of traffic and significantly enhanced service restoration capabilities.

3.3.2 Switching Systems

Switching systems within the PSN have evolved from electromechanical technology to elaborate computer-controlled systems. Modern switching systems, through software programming and the addition of peripheral devices, can provide voice, data, or video service; however, a number of older switching devices in the LEC networks still constrain the ubiquitous offering of advanced services.

In the past, the cost per mile of transmission facilities and the concern for long distance transmission performance influenced network designers to use more switches to minimize transmission mileage. With the tremendous cost efficiency and transmission performance of fiber optic technology, engineering design practices have changed and now a minimum number of switches are used. Today, the PSN is a network of larger switching systems comprising end office switching, access tandem switching, and interexchange switching.

This architecture increases the survivability of the PSN because LECs have increased connectivity and multiple IXCs serve most locations within the United States. Further, the IXCs are fully interconnecting their switches within their networks and employing nonhierarchical traffic routing programs for optimum use of network facilities.

3.3.3 Network Signaling

Signaling System No. 7 (SS7) is intended to become a universal signaling system and is generally replacing the old in-band signaling network in most of the LEC and IXC networks. Within the United States, most PSN carriers will provide compatible interfaces so that the individual SS7 systems will work together as one system. SS7 deployment is virtually complete in the major IXC networks and the major LECs expect it to be completed by 1994. There is concern, however, that some small LECs may not evolve to SS7.

Ubiquitous ECC services are dependent upon nationwide deployment of SS7 networks because these networks will provide the ability to transport the NS/EP identifier and other special signals.

3.3.4 Wireless Technologies

No other segment of the U.S. telecommunications industry has approached the rate of growth recorded in the last 9 years by the cellular industry. From a zero base in 1983, the number of U.S. cellular subscribers has grown to more than 7.5 million, licensed systems to more than 900, and cell sites to more than 6,000. As these systems continue to grow, new technological advances are furthering the growth and utility of the industry and are making wireless mobile telecommunication services more available, accessible, and cost effective. The application of modern switching, signaling, and transmission technologies within the cellular networks, along with the transition to digital radio technology, is enhancing the capabilities of cellular

systems. These capabilities include automatic call delivery throughout North America, as well as increasing system capacity and privacy.

In the future, both conventional geosynchronous orbit and low earth orbit mobile satellite systems, currently under development, will offer even greater telecommunication alternatives for NS/EP users. When combined with terrestrial-based cellular systems, these mobile satellite systems will afford vastly improved cost-effective access alternatives.

In addition, the cellular industry and other vendors are exploring new wireless technologies and concepts. The FCC has issued several experimental licenses to companies wishing to explore the concept of Personal Communications Networks (PCN) or Personal Communications Services (PCS). These experiments, based for the most part on the use of microcells (tiny cells with a radius of 700 yards or less), will determine if a cost effective service can be created that satisfies a need beyond current cellular service. It is anticipated that these techniques may prove most effective in providing service to high density population corridors and urban locations or in offering wireless Private Branch Exchange (PBX) services within office buildings.

3.3.5 Network Support Systems

The PSN is designed to carry maximum traffic during peak busy periods. When normal traffic loads are within this designed maximum level, the network operates without the intervention of network management controls. However, when the network experiences a failure that affects service or is under stress, traffic demands may exceed the available network resources. When this occurs, network management controls are placed into the network to properly manage excess traffic loads and ensure the maximum number of call completions with available resources. Traffic that fails to complete through the network may block other traffic, causing the traffic overload to increase. The network controls in current switching technology are implemented from remote network management control centers and permit the carriers to regulate network traffic flow.

Recent software and hardware deployments provide network switching systems with a wide array of management tools, diagnostic capabilities, sophisticated data base management and control, and extensive man-to-machine interfaces that significantly enhance maintainability of network elements.

The complexity of today's PSN requires a high level of automatic computer support. Network traffic modeling systems determine the number of switch ports and the amount of transmission capacity needed between switching nodes, automatically order the required facilities, and examine traffic flow to determine the most efficient routing for the traffic. Expert systems convert these routing models into routing tables for each switch in the network and automatically load them in the switching and signaling data bases. Although these automated support systems do not provide NS/EP users with

precedence over the general public, they do configure the PSN for optimum service for all users under normal operating conditions and during some periods of congestion.

3.4 STANDARDS ISSUES

The PSN has evolved into a high quality, ubiquitous service composed of a continuum of many individual LEC and IXC networks. The high level of interoperability and service ubiquity provided among these networks and between the networks and terminal equipment is possible because of the adherence to telecommunications standards by carriers and equipment manufacturers. Developing and promulgating standards will be an important element in the development and deployment of unique ECC features throughout the PSN.

An example of ECC dependence on the standards process is the need for the implementation of the High Probability of Completion (HPC) standard. During the investigation of potential ECC features, the task force determined that this standard would be the logical and fundamental means for transporting the necessary NS/EP call identifying mark through the PSN.

The standards issues addressed in this section are treated more fully in the discussion of the HPC standard in Section 4.0. Regulatory, competitive, and technical issues are discussed throughout Sections 5.0, 6.0, and 7.0.

4.0 NS/EP CALL IDENTIFIER FOR PROVIDING CALL-BY-CALL PREFERENTIAL TREATMENT

4.0 NS/EP CALL IDENTIFIER FOR PROVIDING CALL-BY-CALL PREFERENTIAL TREATMENT

The task force reviewed a number of existing and planned PSN features to identify features with the potential to increase NS/EP call completion. During this review, the NS/EP identifier was determined to be a critical element in providing call-by-call preferential treatment and is essential in meeting the Government's need for enhanced call completion. In addition to providing call-by-call preferential treatment, the NS/EP identifier could also be used in conjunction with existing PSN features to enhance call completion. This section describes NS/EP call identification and a means for transporting the NS/EP call identifier through the PSN.

4.1 NS/EP CALL IDENTIFIER

Description. The NS/EP call identifier capability would identify an NS/EP call, accompany that call through the PSN, and enable preferential treatment. The NS/EP identifier would prompt operational elements of the PSN, including cellular systems, to differentiate between NS/EP calls and general public calls and provide the NS/EP calls with special handling in signaling, switching, and traffic routing. Several methods could be used individually, or in some combination, to activate the call identifier: personal identification number (PIN), automatic number identification (ANI), essential service protection (ESP), special screening, line classmark, and destination address.

NS/EP Application. The ability to distinguish an NS/EP call from a general public call is essential for providing the full benefit of enhanced call completion. When the call is identified, the carriers could process the call using methods such as 1) providing special treatment in common channel signaling (CCS) systems; 2) enabling special switch translations; or 3) disregarding protective network control mechanisms. After the call is identified as NS/EP, the identification would have to be transported through the network from the originating end office to the terminating end office for the most effective treatment.

Availability. Technical capabilities required to provide enhanced call completion are usually dependent on the capabilities of the network switching machines, the robustness of the network, and the signaling system. However, because of the high level of effort, cooperation, and coordination required among LECs and IXCs to recognize and transport the mark, a significant amount of time probably will be necessary to develop and implement an NS/EP call identification feature.

Acquisition. When the NS/EP identifier is implemented, NS/EP users will be able to order a preferential treatment capability with NS/EP switched-voice/data traffic. As an example, only one IXC is under contract with the Government to provide a service that meets many of these requirements and the LECs are supporting this service. The NS/EP call identifier for that service is

the combination of the destination address and unique incoming trunk screening.

4.2 NETWORK TRANSPORT OF THE NS/EP CALL IDENTIFIER

Efficient transport of an NS/EP identifier across networks could best be accomplished by using special classmarks within the SS7 network. The need for such a capability has been recognized and industry's proposed standard for it, the HPC standard, begins to answer that need.

Description. HPC is a network capability that utilizes a specific value of the calling party category within the initial address message (IAM) of the SS7 protocol. Today, only a few of the many possible calling party categories have been assigned. The HPC setting in the IAM could be used to enable algorithms that provide preferential treatment for NS/EP calls as they progress through the PSN.

NS/EP Application. NS/EP calls would be identified within SS7 networks by the setting of the calling subscriber with priority code in the calling party's category of the IAM by the originating signaling office. As the NS/EP call progresses through the PSN, this code could enable special routing and preferential treatment to ensure the higher probability of call completion. In addition to carrying the NS/EP call identifier, the NS/EP call IAM would be assigned the highest message priority level (MPL) permitted for PSN customer calls. This level is one level higher than the MPL assigned to general public calls. The elevated handling priority of the NS/EP call IAM would be recognized at all signaling points in the call path.

NS/EP calls could be established by using service-specific mechanisms such as special routing capabilities to enable PSN connectivity in ways not provided by standard network routing. NS/EP calls could also be exempted from certain restrictive network management controls that apply to normal commercial traffic.

Availability. The PSN will have the capability to transport the NS/EP call identifier nationwide when all IXC and LEC SS7 networks are interconnected. However, it may take several years to implement a service in the PSN that takes advantage of the call-by-call capability and services based on the HPC standard. HPC will not be available to NS/EP users until it has been approved, accepted, implemented, and supported by the various carriers. The HPC standard is in jeopardy within the Exchange Carrier's Standards Association (ECSA) T1S1 Committee. The Government and the NSTAC should continue to actively support the HPC standard to ensure its near-term adoption because it is a fundamental requirement for developing ECC services. The effectiveness of HPC and the resulting service will depend on the service description, its cost, and the willingness of all carriers to provide it.

Acquisition. The HPC capability would likely be implemented as an integral part of the overall ECC service. Call-by-call costs associated with HPC

would probably be low to moderate and would likely be included in the basic rate for an NS/EP call using the ECC service. The development, deployment, and administrative costs of a service using HPC could range from moderate to high, depending on the services defined and the size and complexity of the user community.

Section 5.0 recommends ECC features the Government should obtain to provide NS/EP users with a higher level of service. It includes features that are dependent on, and other features that are independent of, the NS/EP identifier.

5.0 CURRENT AND POTENTIAL PSN FEATURES TO ENHANCE NS/EP CALL COMPLETION

5.0 CURRENT AND POTENTIAL PSN FEATURES TO ENHANCE NS/EP CALL COMPLETION

In this section, 14 features are discussed that could enhance call completion. Section 5.1 describes seven features that are dependent on or enhanced by the NS/EP call identifier. Section 5.2 describes seven features that are not dependent on the identifier, but which could provide increased call completion. In addition to the features described in this section, the task force identified other features in Appendices B, C, and D that could benefit the NS/EP user. Appendix B describes customer premises equipment features that could enhance call completion. Appendix C describes current PSN augmentations, which NS/EP users can order from many service vendors, that provide redundancy and increased reliability. Appendix D describes PSN features under development that the Government should monitor for potential future deployment.

Each of these sections is introduced by a table identifying the feature and its availability. A description, the NS/EP application, the availability, and the acquisition strategy are provided for each feature.

5.1 ECC FEATURES DEPENDENT ON AN NS/EP CALL IDENTIFIER

The features depicted in Table 5-1 represent modifications of existing PSN features. The use and transport of an NS/EP identifier would be required for NS/EP traffic to take advantage of these features. Features such as Calling Name Delivery (CNAM), when used in conjunction with the NS/EP call identifier, would greatly enhance the utility of the service. The feature is described in Appendix D, rather than in this section because customer premises equipment (CPE), which is not included in the PSN, is required for CNAM.

TABLE 5-1
ECC Features Dependent on the NS/EP Call Identifier

SECTION	FEATURE	AVAILABILITY
5.1.1	Special Application of and Exemption from NM Controls	Not Planned
5.1.2	Enhanced Alternate Routing (IXC)	Not Planned
5.1.3	Enhanced Alternate Routing (LEC)	Not Planned
5.1.4	Trunk Queuing	Not Planned
5.1.5	Off Hook Waiting for Outgoing Trunks	Not Planned
5.1.6	Dynamic Trunk Reservation	Not Planned
5.1.7	Mobile Subscriber Priority Service	Not Planned

5.1.1 Special Application of and Exemption from Network Management Controls

Description. Network management controls are a set of measures used by service vendors to prevent or reduce degradation in PSN service and to ensure that the PSN is operating with optimum efficiency and effectiveness. Controls may be invoked at the service vendor's discretion or may be based on intercompany agreements in the standards organization. Controls may be invoked when customer demands, equipment malfunctions, or other events cause a deviation from engineered traffic loads and result in abnormally high traffic overflow or blockage.

Controls are either protective or expansive. Protective controls limit traffic going into a switch, trunk group, or destination address. Expansive controls generally increase the capability to carry excess traffic by increasing routing choices. Control measures include route cancellation and route expansion, and can be implemented in traffic percentages.

Special application of network management controls could provide NS/EP identified calls with special traffic handling privileges that would not be available to the general public. Exemption from network management protective controls would provide NS/EP identified calls with immunity from cancellation controls, which could restrict call completion processing functions or routing choices for general public calls. NS/EP calls could continue to be enhanced by expansive controls.

NS/EP Application. In the future, network traffic management could enhance NS/EP call completion by expanding the network for all users, expanding portions of the network only for NS/EP users, or selectively reducing nonpreferential traffic to allocate remaining resources for NS/EP. The ability of network traffic management surveillance and control mechanisms to identify and selectively control traffic in favor of NS/EP calls is quite limited. If NS/EP calls were automatically identified in the network, they could have access to special routing mechanisms and/or expansive controls that would improve their probability of completion. Without a readily identifiable designation, however, a call cannot be identified as an NS/EP call; and the opportunity to selectively favor NS/EP calls in the activation of network management expansive controls would be more difficult. Similarly, NS/EP traffic cannot be shielded from protective controls unless discrete routing mechanisms can be acted upon.

The following network management capabilities could be developed when an NS/EP call identifier is implemented on a call-by-call basis in the PSN.

- Exemption from protective controls that cancel NS/EP traffic.
- First access to idle network capacity for NS/EP calls through expansive controls, such as reroutes.

- Exemption of NS/EP traffic from code controls such as call gapping. NS/EP personnel could then call into emergency areas where normal access is blocked.

- Provision of preferential treatment for NS/EP calls through trunk reservation controls, which could be specific to a traffic class, dialed number, or code reserving "n" trunks during emergencies. (See Section 5.1.6 for a description of dynamic trunk reservation.)

- Automatic alternate routing of NS/EP calls from one carrier to another when problems exist in the network. (See Section 5.2.2 for a description of automatic call rerouting.)

- Provision of first preference to NS/EP call setup messages in the SS7 network.

Availability. Network management controls are implemented by service vendors at their discretion to ensure optimum PSN performance. Customers, including the Government, currently do not have the option of requesting the implementation of network management controls. Special application of or exemption from network management controls for NS/EP traffic could be developed as part of an NS/EP preferential service when the NS/EP identifier is implemented and appropriate modification is made to PSN switches and network management programs.

Acquisition. The steps necessary to obtain any or all of these network management features may be time consuming and difficult. Consensus is required from industry on deployment, implementation, administration, and billing issues to obtain a ubiquitous capability (See Section 7.0).

5.1.2 Enhanced Alternate Routing in the IXC

Description. Enhanced IXC alternate routing programs would provide IXC networks additional capability to transport NS/EP calls to their destinations by affording them special routing controls and paths within an IXC or among IXCs that would not be available to general public calls.

Historically, the PSN relied on a five-level switching hierarchy to complete calls across the network. This approach employed extensive, rigidly set alternate routing programs to maximize the paths available to any call in the network. However, the major IXCs are rapidly migrating toward new routing programs that use flat network architectures and non-hierarchical routing techniques in which all switches in an IXC's network are of equal level, and are directly connected to all other switches in that IXC's network. The IXCs use these techniques to ensure that traffic on their networks is completed economically, to balance traffic loads, to avoid network congestion, and to complete the maximum number of calls that the network can support during overload periods. Thus, the role of alternate routing in the PSN is changing so

that it is used more often to improve efficiency of a network than to handle trunk group overflow and to provide survivability.

NS/EP Application. Enhanced alternate routing in the IXC and LEC networks can significantly benefit users by providing greatly enhanced traffic routing options or call paths. When NS/EP traffic is identified by the NS/EP call identifier, the IXC networks can provide a variety of additional routing options for NS/EP calls. These alternate routing options can include expanded routing within an individual carrier's network, access to special trunking to other carriers (e.g., the NCS Carrier Interconnect Program), access to special network services and capabilities (e.g., Government Emergency Telecommunications Service [GETS]), or access to government-owned or leased telecommunication resources (e.g., Defense Information System Network [DISN], Federal Telecommunications Service [FTS] 2000, and Mobile Transportable Telecommunications [MTT] service capabilities).

Availability. The major IXCs have the capability to provide an enhancement to their routing programs to provide a preferential service package for NS/EP users. The exact nature of the enhancement that the Government could obtain from each IXC would depend on specific government needs and the design of the IXC's network and basic routing program.

Acquisition. The Government will have to negotiate with the individual carriers for alternate routing capabilities that exceed normal applications. This will ensure that NS/EP traffic can be identified and partitioned (if necessary) in the carriers' networks, and that this traffic can be excluded from protective network management controls. Further enhancements can be achieved by implementing special trunking among carriers or government networks, and implementing special access arrangements. This activity is already underway in the NCS Carrier Interconnect and MTT programs.

There would be no additional cost to the Government for basic alternate routing because it is part of the basic network service. The carriers could incur some relatively minimal costs to establish enhanced alternate routing in the network/switch software tables to support special NS/EP trunking arrangements. The carriers might also incur some additional administrative costs in maintaining NS/EP software routing tables or the network management and control capabilities to implement them.

5.1.3 Enhanced Alternate Routing in the LEC

Description. Current routing capability in LEC networks in major metropolitan areas often consists of two routes: a direct route and an alternate route via a tandem office. Traffic is offered to the direct route first, and if no trunks are available, traffic is then routed to the tandem route. If no trunks are available to the tandem switch, traffic will receive an all-trunks-busy signal. Tandem routing is a standard engineering practice for service vendors. The tandem route is generally considered as the final route.

Network management controls can be used to establish alternate routing capability on an ad hoc basis to establish temporary routes and tandem offices when congestion or damage has impacted network performance. Ad hoc alternate routing can be achieved by applying network management controls. It is used at the discretion of the LECs and provides the same benefits for all users.

Enhanced alternate routing could route NS/EP marked calls over trunks in the LEC network to other end offices serving as temporary tandem offices to ensure capacity for NS/EP traffic during network overloads. Such a reroute could be manually or automatically activated.

NS/EP Application. NS/EP calls would first be routed to the normal routing pattern, perhaps a direct route and a tandem route. If the call is unable to be completed on those routes, capacity could be reserved from these facilities for NS/EP users by denying the general public access to these routes. The NS/EP user would then have an improved chance for call completion. Alternatively, calls could be routed to another end office that is acting as a temporary tandem office and use the temporarily idle network capacity to complete the call.

Availability. Many LECs provide this type of alternate routing arrangement. The major IXCs can also provide this service but its need may not be as great in those networks because of their flat, non-hierarchical routing programs.

Acquisition. Enhanced alternate routing would be obtained directly from the LEC. Cost of the service would depend on the number of subscribers that would require the service and the number of times that the service would be activated. The cost to provide the basic service is probably low but the cost for service activation is probably moderate.

5.1.4 Trunk Queuing

Description. Trunk queuing would enable the PSN to provide preferential treatment for NS/EP calls by holding them in queue to wait for idle trunks during network congestion.

NS/EP Application. NS/EP calls would be held in queue until a trunk became available, at which time the first call in queue would have access to the trunk on a first-in, first-out (FIFO) basis. The calls remaining in the queue would be held until subsequent trunks became idle, rather than being routed to an all-trunks-busy tone trunk. In many networks, routing plans have been designed and implemented for the carrier to maximize the use of its trunk network, thereby reducing blocked call conditions. These routing arrangements tend to eliminate the need for the trunk queuing feature except in emergencies. In an emergency condition, the queuing algorithm could be activated to favor NS/EP calls. In follow-on networks, an NS/EP mark could be the indicator that this call attempt should be queued.

This capability would apply only when the trunk network is congested so that no additional calls can be rerouted and the user must wait for the call to be completed.

Availability. The availability of the trunk queuing feature for NS/EP calls is dependent on the provision of capabilities throughout the PSN. An NS/EP call identifier and modification of the PSN switches to provide the service would be required if trunk queuing is to be a service throughout the PSN.

Acquisition. The queuing capability would be obtained as a basic service for NS/EP users.

5.1.5 Off-Hook Waiting for Outgoing Trunks

Description. Off-hook waiting for outgoing trunks is a Centrex-implemented feature that is derived from three other Centrex features (automatic route selection, trunk queuing, and virtual facility groups) that allow an authorized user who encounters an all-routes-busy condition to wait off-hook for a designated time period for an idle trunk.

This capability allows a call to remain off hook and scan every "X" seconds for an idle trunk if it has failed to find one on the initial search. This capability is implemented in some types of end office switches. All the elements that make this capability are basic features in these switches, providing they are equipped with Centrex capabilities.

The current version of off-hook trunk waiting for outgoing trunks allows a list of route choices to be scanned for idle capacity at a minimum of every 2 seconds. Although off-hook trunk waiting does not permit trunk groups to be scanned as fast as trunk queuing, which scans trunk groups every 200 milliseconds, it does provide many distinct advantages and benefits.

Currently, queuing is assignable only to private trunking arrangements. Off-hook trunk waiting for outgoing trunks can be assigned to any trunk group type (private or public), including direct trunking to an IXC point of presence (POP). The wait time (queue time) can be user assignable. That is, it can be engineered longer than the existing trunk queuing time (multiple queue periods of 2 to 90 seconds).

NS/EP Application. An NS/EP call must be identified to direct it to the NS/EP Centrex function that would provide the off-hook trunk waiting capability. Off-hook trunk waiting for outgoing trunks can be used for the following call types: originating calls, tandemed calls, and terminating calls.

Availability. Off-hook waiting for outgoing trunks can be made available without any additional vendor software development.

Acquisition. This capability would be obtained as a service or part of a service provided by the LECs. Because it is an existing feature in Centrex

switches, off-hook waiting could be made available to NS/EP calls by creating an NS/EP Centrex partition in these switches. The cost of such an arrangement would be moderate.

5.1.6 Dynamic Trunk Reservation

Description. The dynamic trunk reservation capability permits the reservation of voice grade trunks in the PSN for certain classes of calls under designated conditions. It could be implemented and activated in a number of ways.

First, network services vendors could allocate specific numbers of trunks between switching machines for different classes of services, such as plain old telephone service (POTS) and data, and manage traffic to maximize throughput. Within these classes of service, premium levels of services could be obtained that would provide for higher completion rates based on access to more of the network. These bandwidth allocations by class of service and level of service would be engineered and deployed by the vendor based on historical and marketing information.

A second method for dynamic trunk reservation is the use of network management controls to provide the capability to reserve trunks in an idle condition for a specific purpose or service. For example, the service vendor, under predetermined conditions, could operate a control that would reserve one or more trunks in its network for NS/EP traffic as soon as it became idle. When an NS/EP call accesses the idle trunk, the network would reserve yet another idle trunk or trunks.

A third method of dynamic trunk reservation could be achieved by designating specific trunks as a subgroup within a trunk group. This subgroup would normally be used for the carrier's commercial traffic; however, under predetermined conditions, a network management control could be activated that would prohibit commercial traffic from accessing this trunk subgroup, thereby reserving the trunks for the specific traffic. This scheme would require engineering and deployment as well as periodic verification of the trunk subgroup and network management center methods and procedures.

The fourth form of dynamic trunk reservation is the acquisition of facilities dedicated to government traffic between designated switching machines. These facilities would be managed as network trunk groups; however, the carrier's commercial traffic would be prohibited from using them. These trunk groups could be active constantly or activated and deactivated under predetermined conditions.

Trunk reservation features could be available for the LEC access, IXC, or LEC egress portions of the PSN, and could also accommodate government PBXs under directly connected scenarios.

NS/EP Application. When the NS/EP call is recognized by the network, it would have a higher rate of completion with dynamic trunk reservation if:

- It has the maximum amount of access to the network trunks.
- The network management controls to reserve trunks within the network are enabled.

Availability. Most of the trunk reservation approaches and capabilities are now technically available and are usually dependent on the capabilities of the switching machines, operations support systems, and service vendor methods and procedures.

Acquisition. Dynamic trunk reservation capabilities could be obtained as a service or as part of a service provided by LECs and IXCs.

5.1.7 Mobile Subscriber Priority Service

Description. Mobile subscriber priority service refers to a service that could enable selected mobile telephone subscribers or groups of subscribers to receive precedence over other network subscribers in acquiring access to and transport through the network. Priority access software is under development by at least one major cellular equipment vendor. With this software in place, the cellular system could provide specifically designated cellular subscribers with precedence-based access to and transport through the cellular system. Transport of a precedence call beyond the cellular system into the PSN will require the development of standards and agreements between and among cellular and land line telephone companies.

Implementation of priority service can take many forms that range from the permanent dedication of assets to call-by-call priority with queuing and/or preemption, depending on the user's requirements and the service provider's ability to support the capabilities. In addition, provision of priority service within the PSN requires regulatory revision if this capability inhibits service for the general public.

NS/EP Application. For the NS/EP caller, priority access and service form one of the basic building blocks for ensuring enhanced call completion. An interrelationship exists between this service and numerous other ECC capabilities and features for the provision of priority service to NS/EP users. Identification of a quantifiable NS/EP user community and development and implementation of an NS/EP call identifier are important to the provision of many NS/EP priority services. In addition, a government-managed system to establish and control the assignment and use of such priorities must be in place before any meaningful system can be implemented.

Availability. Today, primarily due to market and regulatory concerns, priority service is not generally available within cellular systems, although dedication of facilities/equipment (cellular channels) for high priority

government subscribers is done on a limited basis. This dedicated approach is costly and not universally available. However, basic cellular system design lends itself to the provision of precedence in the network. Each cellular telephone is identified by an electronic serial number (ESN) which, along with its mobile identification number (MIN), uniquely identifies that phone to the cellular system's call processor. The cellular system is in constant communication with the activated cellular phone through a control channel. Through this mechanism, it knows the location (by cellular system and by cell) and status of each mobile subscriber in the system's area.

Acquisition. Although some features of today's cellular network are in place and lend themselves to the provision of priority service, the Government, as the only potential user of this service, must take the necessary steps to resolve the regulatory issues.

The Government must also be willing to fund the system modifications necessary to provide NS/EP users with priority service. This may entail a contractual arrangement between the Government and each of the involved cellular carriers for the development and provision of this capability nationwide.

5.2 ECC FEATURES NOT DEPENDENT ON AN NS/EP CALL IDENTIFIER

TABLE 5-2
ECC Features Not Dependent on the NS/EP Call Identifier

SECTION	FEATURE	AVAILABILITY
5.2.1	Presubscription Override	Current
5.2.2	Automatic Call Rerouting	Not Planned
5.2.3	Priority Dial Tone	Current
5.2.4	Local Exchange Carrier Bypass	Current
5.2.5	PSN Partitioning*	Current
5.2.6	Diverse PSN Access from Cellular Systems*	Current
5.2.7	Position Locating/Tracking for Cellular Systems*	Planned

* Could be enhanced by an NS/EP identifier.

5.2.1 Presubscription Override

Description. Equal access provides long distance customers the option of presubscribing to one IXC as their PIC for inter-local access and transport area (interLATA) calls. Long distance calls dialed by the customer, who has

presubscribed to an IXC, will be routed automatically to that IXC. The customer can override the presubscription by indicating on a per-call basis that a different IXC is desired.

Each IXC that subscribes to equal access has been assigned a carrier access code (CAC) that consists of digits 1 and 0 plus a unique three-digit carrier identification code (CIC). Customers can elect, on a per-call basis, to manually override their presubscription by dialing the 10XXX code for a different IXC to carry that particular call. This capability is useful when the customer's presubscribed carrier is unable to complete the call.

NS/EP Application. The 10XXX code provides NS/EP users and the general public, the ability to manually select an IXC on a per-call basis and to override their presubscription. The code also presents a limited capability for NS/EP users to direct their calls to alternate routes, i.e., different IXCs.

Availability. This capability is provided in all locations where customers have a choice of more than one IXC for interexchange call origination, and where the local switching system is capable of providing equal access to the IXCs.

Acquisition. The 10XXX code capability, where available, is now an inherent part of equal access telephone service and there is no cost to implement it.

5.2.2 Automatic Call Rerouting

Description. Automatic call rerouting is a technically feasible feature that would permit a LEC to automatically switch an NS/EP call to presubscribed alternate IXCs when access to the customer's preferred carrier is unsuccessful.

NS/EP Application. The FRWG determined that there is a regulatory constraint that prevents automatic call rerouting from being implemented. If the regulatory constraint was removed from the LECs, automatic alternate route choices to other IXCs to complete the call could be provided to NS/EP traffic. The automatic call rerouting feature would eliminate the need to hang up and make another attempt to place the call over a different IXC by dialing the presubscription override code, 10XXX.

Availability. One method of providing this service would require NS/EP originating access lines to be individually identified in calling line records in LEC end offices as eligible for automatic access to more than one IXC. This would require enlargement of the basic translation field for customer lines to accommodate additional PICs. Another method would require a means to concentrate originating NS/EP calls in a special Centrex arrangement that could provide access to multiple IXCs using the Centrex route advance capability. Development and implementation costs for either arrangement could be high due to the number of switching offices involved.

Acquisition. The Government would have to work with the FCC to obtain a waiver of the current Interexchange Carrier Subscriber Plan (refer to FCC Docket No. 83-1145), which permits end users to select only one primary interexchange carrier to carry interLATA calls. This service might not be supported because of high operational and administrative costs.

5.2.3 Priority Dial Tone

Description. The priority dial tone feature improves the likelihood that essential or critical users receive a dial tone during switch overloads or network congestion. This feature is available in many versions of local central office switching systems under the names of line load control (LLC) and/or essential service protection (ESP). The latter is also known by other acronyms, including essential line service (ELS or ESL) and dial tone protection (DTP). LLC and ESP use markedly different methods of operation, which are identified below.

During periods of long dial tone delays, LLC denies a dial tone to certain groups of lines to relieve switch congestion. As dial tone delays subside, a fraction of the denied lines are returned to service. As service further improves, all lines are eventually restored. Even with this restrictive treatment of nonessential users, dial tone delays experienced by essential lines can still be long and the throughput of the system can be degraded.

ESP in modern switches allows the microprocessor that performs line scanning to identify call origination from a line marked as ESP. During periods of congestion and dial tone delay, attempts from such lines are placed in a priority queue that is handled before the normal dial tone queue. In ESP-equipped offices, dial tone attempts are also handled on a last in, first out (LIFO) basis. This strategy was introduced in modern switches to mitigate the abnormally high level of ineffective call attempts caused by customers dialing before receiving a dial tone, which results in partial dials. While call-in-progress work, such as digit analysis and network connections and disconnects, is done at an even higher priority level, all requests originating from the ESP queue are served before the non-ESP call attempts in a lower level queue. In general, if the total number of ESP-equipped lines and their resultant calls is modest (less than 15 percent of office capacity), ESP calls during overloads and congestion are provided excellent dial tone results and non-ESP calls are only minimally affected.

NS/EP Application. NS/EP callers with critical response roles during national emergencies who require the use of the PSN could benefit by being assigned an ESP line. Often during emergencies, dial tone resources are strained or delayed because of local or focused calling. With ESP, the probability of obtaining timely dial tone is greatly enhanced. Studies have shown that LLC does not significantly reduce dial tone delays; and because of the troublesome implications to non-ESP lines, LLC is used only as a last resort.

Availability. An informal poll of NSTAC companies indicates that not all carriers provide or are equipped to provide ESP. Additionally, some central

offices cannot provide ESP. If ESP is not offered and the user is served by an office that can provide ESP, perhaps the Government could request that the feature be activated. If it is available in a nearby serving office, the Government might also consider purchasing foreign exchange service from the same or different service vendor in that equipped office.

Acquisition. The assignment of specific customers to ESP is available in certain local central offices and is a telephone company prerogative. Generally, if customers perform critical emergency functions, they could qualify for ESP. To obtain ESP from a local telephone company, critical government users should call their LEC marketing or business office contacts, inquire if that capability is offered in their serving area, and request it. Currently, there is no charge for the service by most service vendors.

5.2.4 Local Exchange Carrier Bypass

Description. Bypass of the local exchange portion of the PSN has been available for several years and in many forms. The Government and large corporations purchase or lease facilities for "corporate networks" that directly connect various locations to provide communications between communities of interest. Cellular services could also be considered a form of LEC bypass. Due to the increased mobility of today's communications user, the cellular industry was established to provide users with mobile access to the PSN through radio technology.

LEC bypass is used for access to or egress from IXCs, mobile satellite systems, or other specialized carriers to avoid transit of network services provided by the LEC.

NS/EP Application. NS/EP applications of LEC bypass typically could be used for direct inter- or intraLATA access/egress of the PSN for either bulk, wide-band, switched (FTS2000), point-to-point, or circuit-by-circuit services.

Availability. Such bypass services are available from many IXCs, cellular carriers, alternate network providers (ALTs), specialized common carriers, and LECs.

Acquisition. These services are standard tariff offerings and can be obtained through normal procurement channels for communication services. Depending on the application of bypass, the cost to the user could be moderately higher than using LEC direct access services.

5.2.5 PSN Partitioning

Description. Partitioning in telecommunication networks is the separation of network traffic into disparate groups for the purposes of managing these groups of traffic in a dissimilar fashion or providing unique service capabilities. Typically, the traffic is separated to afford a selected user

group some level of special treatment. The actual partitioning of the network can be accomplished through a variety of hardware or software techniques.

Hardware partitioning is achieved by identifying certain physical network facilities that support a specific user group. The traffic generated by this user group is then directed into engineered facilities and/or routing tables that isolate these users from the rest of the network traffic. Under this type of partitioning, users could be identified by specific line assignments within a given end office or by trunk groups that originate from selected customer premises equipment. This type of partitioning requires the user to make calls from predefined locations to receive any preferential treatment.

Software partitioning is achieved by first identifying an individual user's call attempt as it enters the network; then by means of either appending an NS/EP identifier to the call setup information, or placing the traffic into a special routing category (a software partition), the network can provide preferential treatment to the call attempt anywhere in the network. Under this type of partitioning, users could be identified by the ANI information passed to the network, by a unique PIN, through an NS/EP identifier, or through the use of uniquely dialed digits into the network, which would identify the traffic as belonging to a given user group deserving preferential treatment on the network.

NS/EP Application. NS/EP traffic could benefit from network partitioning by receiving special treatment in the network during periods of severe network overload. Protective network controls such as call block and call gap, which shed originating traffic to protect the network from congestion and possible damage, are applied on individual partitions in the network. For NS/EP user traffic to be exempt from these types of network controls, it must be in a partition separate from that of the public traffic.

Availability. Network partitioning by means of a hardware separation is universally available. It requires the identification of selected users and special engineering of network facilities. Hardware partitioning is most practically applied to the local network, including access to the IXCs. Because the local network is designed to concentrate traffic from the individual users (line assignments) into the network trunking, most network blocking occurs between the user and the LEC access tandem or interexchange switch. There is an inherent impracticality related to establishing hardware partitions all the way through the IXCs to the distant city.

Partitioning by means of software techniques is relatively new in the PSN, and represents the future industry trend for user group traffic management. Many LECs are developing software partitioning capabilities in their respective networks, which will allow preferential treatment in the local network, and identification of this traffic to the IXCs. The three major IXCs provide network partitioning in their networks. These partitions can be used to provide preferential treatment to NS/EP traffic within the IXCs' networks, including access to special government facilities such as the Carrier Interconnect Program

facilities and the MTT Program. There are efforts underway to interconnect the local and interexchange SS7 networks, which would facilitate passing preferential treatment information among carriers. This would allow for end-to-end preferential treatment of NS/EP traffic in the PSN. It is estimated this capability will be widely dispersed in the PSN within the next 5 years.

Acquisition. Because partitioning in the PSN is typically a technique employed by the telecommunications industry to manage traffic or provide unique services, it is not a tariffed service offering. Therefore, the Government will probably have to work with the LECs' and IXCs' service planning groups to obtain this capability. Some of the carriers already provide services that are partitioned in their networks for management purposes. In these cases, the Government could incorporate these service offerings into its communication requirements or negotiate with the carrier to include these existing services into service offerings that are partitioned.

The cost of partitioning service for NS/EP traffic will vary with the capabilities of the LECs and IXCs providing the service. In general, hardware partitioning will be more expensive than software partitioning because it requires engineering of the capability and the capture of physical facilities. The carrier will need to recover the costs associated with engineering time and the cost of the facilities that are no longer in the general revenue stream. Depending on the scope of the requirement, this approach could have very significant installation and recurring monthly costs. Software partitioning is relatively inexpensive because the costs associated with this approach consist of a one-time development cost, which is shared by all users, and a relatively low, recurring administrative cost. It is quite possible that to properly implement a partitioning capability would require both hardware and software partitioning techniques. An example of this approach might be to implement a hardware solution in the local network to permit access to IXCs that provide a software partitioning capability.

5.2.6 Diverse PSN Access from Cellular Systems

Description. Diverse PSN access is the capability of today's cellular networks to directly interconnect with other elements of the PSN at the end office, access tandem, and interexchange carrier network switching levels. Thus, this capability allows cellular originated calls to be routed around a failed network node or routed directly to an IXC switch for designated traffic.

Network access diversity also exists to route specifically identified subscribers' calls to private or special purpose networks (e.g., DISN, FTS2000). As cellular systems are linked through "seamless" cellular networks, additional call setup and routing paths will be available to the cellular subscriber.

NS/EP Application. The diversity provided by this capability increases the probability of completion of the cellular user's access to or egress from the network by providing alternative connection paths into and out of the local exchange area, in some cases tying directly into IXC networks.

Availability. Basic call routing diversity is an integral feature of cellular service and is available to the NS/EP subscriber at no additional cost beyond normal cellular service.

Diverse access is available in some cellular carriers' networks today and is technically feasible in all cellular networks. Expansion of diverse connectivity for specific NS/EP requirements or direct interconnection with private or government networks is also technically feasible today and can be offered in many cellular systems as a special feature/capability.

Acquisition. If specific government and/or NS/EP requirements exist within an area of cellular service, these capabilities can be contracted for and acquired through the serving cellular provider. As "seamless cellular networks" develop from the current regional implementation to nationwide coverage, users with NS/EP requirements will be able to contract with network providers for additional special access and routing capabilities.

5.2.7 Position Locating/Tracking in Cellular Systems

Description. This capability describes the cellular network function that tracks, locates, and delivers a call to a specific subscriber, both within the home system and when that subscriber is "roaming," within a visited cellular system.

A basic feature of cellular architecture is the continuous monitoring, by the call processor, of subscriber status and call progress. For example, as an active mobile subscriber travels within the geographical area of a cellular carrier, the processor continuously monitors the mobile subscriber's location (primary cell site) to process calls.

When a subscriber roams into another cellular service area, the subscriber's presence is detected by the visited system. An action is then initiated to allow or deny service to the subscriber dependent on validation of the subscriber and availability of service agreements between the home and visited system's operators. Today, most cellular system providers permit semiautomatic roaming within their systems. This method allows subscribers to make outgoing calls as they normally would in their home systems. However, a caller trying to telephone a roaming subscriber must know the location of the subscriber and dial a number that routes the call to the appropriate distant switch. The caller must then dial the mobile subscriber's number. This clumsy and time consuming procedure does not provide a satisfactory service solution.

NS/EP Application. With the recent deployment of intelligent network capabilities, common channel signaling, and the development of intervendor cellular switch-to-switch compatibility standards, fully automatic cellular call delivery and standard feature package transfer are rapidly becoming available to cellular subscribers traveling anywhere within the network. This capability removes the restrictions that make cellular use difficult and confusing outside

the home system, provides rapid subscriber validation, automatically delivers incoming calls, provides a natural extension of cellular features and benefits, and enhances the personal number concept of "one person-one number" regardless of location. It is this feature, when combined with the provision and transport of a unique NS/EP call identifier and other intelligent network features, that will provide enhanced call delivery and completion for the mobile NS/EP user.

The intelligent network can also provide the required verification of the calling person and the authorization and priority of the call. This verification can be provided through a variety of mechanisms ranging from the simplest—the use of a PIN—through the more difficult—the use of an intelligent peripheral (IP) employing voice recognition and an authorized user data base.

Availability. The future development of integrated PCS will add additional capabilities and benefits for enhancing NS/EP call completion. Among PCS capabilities being investigated within the industry are cellular/global positioning system (GPS) integration, microcellular and wireless PBX applications, dual-mode cellular/mobile satellite terminals, and the entire spectrum of advanced intelligent network (AIN) features and capabilities.

Acquisition. The automatic call delivery features described above are rapidly becoming an integral part of some cellular carriers' standard service offerings. The Government can obtain these capabilities as part of its service requests from carriers capable of providing this service. The marketplace will determine whether advanced features will be offered as standard service offerings or will require specific procurement requests on a regional or nationwide basis.

Section 6.0 describes the impact of ECC services on the PSN and the general public user.

6.0 IMPACT OF ECC FEATURES ON THE PSN AND THE GENERAL PUBLIC

6.0 IMPACT OF ECC FEATURES ON THE PSN AND THE GENERAL PUBLIC

Implementation of the ECC features discussed in this report would have only minimal effect on PSN operation. Generally, provision of available features would have no impact on network operation. Development and implementation of some potential features would add some complexity to the functions that switches, signaling networks, and control systems would have to perform, but, based on available information, the overall effect on network operation is considered to be negligible.

The impact of ECC features on service to the general public will be minor because of the relatively small number of identified NS/EP users. NS/EP users' calls would receive preferential treatment over general public calls only in common usage areas of the PSN, where bidding for dial tone, vying for trunks, handling of initial address messages in the SS7 network, etc., take place. The use of ECC features on the NS/EP users' access and egress services would not affect the general public's use of the PSN. In addition, many ECC functions would be provided through features that would accord special privileges, rather than priority treatment, to NS/EP calls and would have no impact on general public calls.

Implementation of the HPC standard, as described in Section 4.2, would be the most significant priority factor for ECC. This capability would provide priority handling of initial address messages for NS/EP calls, and, although there might be a slight delay in the handling of general public calls, the general public user would be unaware of any delay.

Table 6-1 lists ECC features, indicates the PSN access, transport, and egress segments where they would be applied, and whether or not the features would have an adverse effect on PSN operation and the general public user.

The legality of implementation of those ECC features that would affect general public calls in any way is subject to review and approval by the FCC even though the technical impact of these features would be negligible. Because the predicted effect of ECC services on the PSN and the general public user is relatively small, the impact issue is not expected to be an obstacle to developing plans and procedures for implementing enhanced call completion services nationwide, as discussed in Section 7.0.

TABLE 6-1
Analysis of the Impact of ECC Services on the PSN

Section	Feature	Network Segment Application	Impact on the General Public User	Impact on the PSN
5.1.1	Special Application of Network management Controls	Transport	Yes	No
5.1.2	Enhanced Alternate Routing (IXC)	Transport	Yes	No
5.1.3	Enhanced Alternate Routing (LEC)	Transport	Yes	No
5.1.4	Trunk Queuing	Transport	Yes	No
5.1.5	Off-Hook Trunk Waiting	Transport	Yes	No
5.1.6	Dynamic Trunk Reservation	Transport	Yes	Yes
5.1.7	Mobile Subscriber Prioriy Service	Access	Yes	No
5.2.1	Presubscription Override	Access	No	No
5.2.2	Automatic Call Rerouting	Access	No	No
5.2.3	Priority Dial Tone	Access	Yes	No
5.2.4	Local Exchange Carrier Bypass	Access and Egress	No	No
5.2.5	PSN Partitioning	Transport	No	No
5.2.6	Diverse PSN Access and Egress from Cellular Systems	Access and Egress	No	No
5.2.7	Position Locating Tracking for Cellular Systems	Access and Egress	No	No

TABLE 6-1 (concluded)
Analysis of the Impact of ECC Services on the PSN

Section	Feature	Network Segment Application	Impact on the General Public User	Impact on the PSN
Appendix C	Avoidance Routing	Access and Egress	No	No
Appendix C	Diverse Routing	Access and Egress	No	No
Appendix C	Dual Hosting (LEC/IXC)	Access and Egress	No	No
Appendix C	Dual Homing (IXC)	Access and Egress	No	No
Appendix C	Trunk Subgrouping	Transport	No	No
Appendix C	Very Small Aperture Terminal (VSAT)	Access and Egress or Transport	No	No
Appendix D	Dual Homing (LEC)	Access and Egress	No	No
Appendix D	Mobile Satellite Communications (MSAT)	Access and Egress	Yes	Yes
Appendix D	Multilevel Precedence and Preemption (within NS/EP domain)	Access, Egress, and Transport	No	No

7.0 RECOMMENDED ENHANCED CALL COMPLETION PLAN OF ACTION

7.0 RECOMMENDED ENHANCED CALL COMPLETION PLAN OF ACTION

This section discusses how the Government could obtain the ECC features described in this report. While some features are single vendor features (e.g., route diversity, priority dial tone, and dual homing), others require coordinated handling between LECs, cellular carriers, and IXCs (e.g., enhanced LEC/IXC routing, special exemption from network management controls, and LEC/IXC trunk queuing). Depending on the Government's requirement for such services—whether to serve a limited number of fixed NS/EP locations or to be available everywhere—different acquisition approaches would be required.

Obtaining nationwide enhanced call completion services would be a major challenge for both industry and Government. A truly nationwide service would be a service that is available from all LECs, cellular carriers, and a sufficient number of interexchange carriers. There is no recent precedent for obtaining such services. Hence, there is no formal industry process for developing and implementing them.

New services are frequently offered by vendors within their own networks and occasionally those services require cooperation from connected carriers. Most often, however, new services implemented since divestiture have been confined to the networks of a single provider, whether a LEC, cellular carrier, or IXC. Since divestiture, there have been only five major new nationwide functionalities under development, and these are in various stages of implementation:

- 800 Database — a user service that is being implemented at the urging of the FCC to provide users 800 telephone number portability.
- Line Information Database — a telephone company service developed for the carriers to validate credit cards and protect themselves against fraud.
- Common Channel Signaling Interconnection — a telephone company service (i.e., SS7) that reduces call setup and connect times thereby improving the productivity of the network.
- Telecommunications Service Priority — an FCC-authorized user service that authorizes preferential treatment for NS/EP users in the restoration and provisioning of telecommunications services by common carriers.
- Equal Access — a requirement based on conditions of the Modified Final Judgement (MFJ) that LECs provide IXCs equal access arrangements for originating and terminating PSN interLATA calls.

No nationwide services, other than TSP, have been developed for a single end-user customer that uses the resources of local exchange, cellular, and interexchange carriers.

The following sections suggest steps the Government might take to obtain three forms of nationwide ECC services: (1) available ECC services; (2) targeted ECC services not currently available but required from only a limited number of carriers; and (3) future ubiquitous ECC services.

7.1 ECC SERVICES CURRENTLY OFFERED BY SERVICE VENDORS

For these types of services, the Government simply has to order the service. If the Government desires that all NS/EP users take advantage of an existing ECC service that they might not be aware of (see Appendix C for possible examples), the Government needs to provide specific guidance to these users. The tariff for such services might include an installation charge, a monthly recurring charge, and/or non-recurring charges. For certain types of features there might also be a special construction charge depending on the type of service desired (e.g., avoidance routing).

7.2 NEW ECC SERVICES OFFERED BY A LIMITED NUMBER OF VENDORS

The approach of using a limited number of vendors would be appropriate when the Government does not require a truly nationwide service, but requires instead that only a limited number of fixed NS/EP locations be served. In this circumstance, a limited number of service vendors would be requested, through a government Request for Proposal (RFP), to develop a special service application. To reduce costs, the service could be defined so that it has application to other network users, potentially spreading the cost of development. A greater demand would also encourage a service vendor to undertake the development, since a more substantial need in the marketplace might produce a greater return on investment. If the Government wants to restrict ECC services to Federal NS/EP users only, it should be encouraged to enlarge the presently identified NS/EP user community. In either case, the Government should study the impact of a large increase in NS/EP user traffic on the general public traffic in the PSN and on ECC cost sensitivities if it plans to expand the NS/EP user base. In the latter case, higher priority could be given to the most critical National Security users over all other ECC users, if the Government were concerned about potential ECC congestion.

The steps required to implement new ECC features in a limited number of IXC, LEC, and cellular networks do not differ significantly from the steps required to implement any new PSN service, with one major exception. That exception is that certain ECC features, i.e., those that give call-by-call preferential treatment to NS/EP users, would violate Section 202(a) of the Communications Act of 1934, which prohibits preferential treatment for any "class of persons" (e.g., NS/EP users) by common carriers. Therefore, regulatory action may be required. An amendment to FCC regulations would authorize and permit preferential treatment for NS/EP users. However, only

those vendors selected and awarded contracts by the Government would be required to provide such preferential services. Further details on the FCC regulatory amendment process are found in Section 7.3.

In the case of a limited number of ECC vendors, the Government would be requesting the service and specifying the service requirements. The steps described here are intended to be generic for an end-to-end and call-by-call ECC feature such as trunk queuing (see Section 5.1.4). Such end-to-end features inherently require that LECs and IXCs can support the feature across their network boundaries. Under certain circumstances, the "Limited Source Selection" provisions of the Federal Acquisition Regulations (FAR) allow acquisition from a limited number of sources.

The overall process for ECC feature acquisition from a limited number of vendors may be divided into three basic stages: the Request for Information (RFI), the RFP, and contract award and implementation. The key to success throughout the acquisition process is frequent government-industry interaction. The familiar government contracting approach is reviewed here in light of the special ECC requirements.

7.2.1 The RFI Stage

To initiate an ECC feature acquisition, the Government should consider issuing an RFI to selected LECs, cellular carriers, and IXCs. The vendors selected would be those in whose service areas NS/EP users have their normal office locations or in which they would function during an emergency. Although this first step adds some time to the process, it provides the Government with an industry sounding board regarding the general technical and economic feasibility of providing the service. The RFI would contain a statement of objectives and a high-level description of the service and would request from industry certain information needed to prepare the RFP. In response to the RFI, for example, industry might suggest that a longer RFP response period for proposal preparation is needed. If many questions were received on the RFI, the Government should consider holding a Government-industry forum to discuss them. In the case of end-to-end ECC features, the ECC Task Force suggests that holding a Government-industry forum, involving selected LECs, cellular carriers, and IXCs would be desirable.

7.2.2 The RFP Stage

The selected carriers' responses to the RFI would enable the Government to prepare and issue the RFP. To ensure that it has properly captured carrier responses to the RFI, the Government might first issue the draft RFP, requesting further comments. After incorporating industry comments, the Government would then issue the final RFP. More than one RFP may be needed, even for a Limited Source Selection, since there may be differences in what the Government requires from LECs, IXCs, and cellular carriers. The RFPs must contain detailed feature requirements and specifications.

The ECC Task Force suggests that Government assist industry by sponsoring additional Government-industry technical forums during the RFP response period. These forums would enable the Government to discuss ECC feature requirements and address other issues associated with the RFPs.

7.2.3 Carrier Response to RFP/Level of Effort Assessment

The next set of steps concerns the carriers' response to the RFPs. The first step is the development of LEC-IXC consensus, a step which is essential for an end-to-end ECC service, since carriers must agree to support the service across network boundaries.

Once LEC-IXC consensus is obtained, each carrier can determine its own level-of-effort (LOE) or cost to develop and implement the service, encompassing the following elements:

- Equipment R&D and engineering design (equipment vendor subcontract).
- Equipment modification by equipment vendor (subcontract).
- Capital investment required for network implementation.
- Installation and test (this, and the above elements, are often referred to as engineered, furnished, and installed [EF&I] costs).
- Operation, Administration, and Maintenance (OA&M).
- Operation Support Systems modification.

The LOE may vary widely among the carriers due to differences in their networks. After individual company LOEs are developed, another Government-industry forum should be held to ensure that each carrier has taken into account all of the relevant cost factors. This step should include a confirmation of internetwork operating procedures.

Having validated or revised its individual LOE estimate as a result of the Government-industry forum, each carrier can now prepare and submit its bid to the Government. By this point in the process, each selected carrier will either have established a business case for offering the service, or else will have withdrawn from the process. The individual company bids will include precise pricing information for offering the service.

7.2.4 Contract Award and Implementation

The next step is Government review and selection of carrier bids. Ideally, all Limited Source Selection bids would be accepted so that the Government could meet its requirements for the NS/EP locations to be served. In practice, all bids might not be accepted due to such factors as government budgetary

constraints or unresponsive bids. For each selected bidder, the Government then awards a contract, including a Statement of Work (SOW), and either specifies the method of funding or agrees to pay the tariffed service price for a specified time period at a certain traffic level.

Each selected carrier then prepares an ECC tariff for approval by the appropriate regulating body if required, or otherwise contracts directly with the Government to develop and implement the service.

7.3 NEW NATIONWIDE ECC SERVICES

Because NS/EP users' telecommunications requirements are both mobile and fixed, a truly nationwide ECC service must be supported by all LECs, cellular carriers, and IXCs across the country. Using the RFP process described in Section 7.2, the Government would need to issue and process approximately 2000 carrier proposals. This would be an impractical and costly undertaking for the Government.

The Government should investigate whether an FCC rulemaking is necessary to require industry to implement a nationwide service. Amending the existing FCC Telecommunications Service Priority (TSP) Report and Order or developing a new FCC Report and Order to authorize and require call-by-call preferential treatment for NS/EP users could be the most effective means for acquiring nationwide call-by-call ECC services. In contrast to the case of a limited number of ECC vendors (discussed in Section 7.2), call-by-call preferential treatment for NS/EP users would not only be authorized but would be required by the new rulemaking.

There are two basic steps involved: (1) preparing and issuing the FCC Report and Order and (2) implementing nationwide ECC services in conformance with the order.

7.3.1 FCC Report and Order Preparation and Issuance

The ECC Task Force believes that the TSP Report and Order (rule) provides an example and a precedent for a nationwide legal and regulatory approach to authorizing call-by-call preferential treatment. That is, just as NS/EP telecommunication users require priority in restoration and provisioning during emergency conditions, those same users might require that their calls be given preferential treatment during emergencies. The TSP rule could be amended by appending authorization of call-by-call preferential treatment to it. Alternatively, a new FCC rule could be prepared.

The proposed FCC rulemaking should follow the same process as that used in the preparation of the TSP rulemaking, but may require less effort because the groundwork has been laid and the framework exists. There are four basic steps: (1) The NCS petitions the FCC for permission to prepare a draft of the Notice-of-Proposed Rulemaking (NOPR). The NCS draft would be prepared with NSTAC assistance. (2) The FCC issues the NOPR. (3) The NOPR is

open for public comment, including comments from the telecommunications industry, Federal, State and local government, and the general public. (4) The FCC issues the final rulemaking.

The call-by-call rule would, as with TSP, "authorize and require" common carriers to provide preferential treatment to NS/EP telecommunications users. Any or all of the call-by-call ECC features discussed in this report would be considered as preferential treatment. Whereas the scope of TSP includes both private line and certain PSN services, the call-by-call rule would extend the TSP concept to cover PSN switched services more completely. (It is assumed that government private line users are already free to implement a call-by-call preferential system, such as exists in the DISN).

A determination must be made as to whether the existing TSP categories and criteria, used to qualify NS/EP telecommunications services for priority restoration and provisioning, could also be used to qualify services for preferential ECC treatment. For example, the TSP subcategories and criteria within the "Essential NS/EP" category might all be mapped into two or more "precedence" levels for ECC purposes. The Government could then choose to continue to give the subcategory "National Security Leadership" within the Essential NS/EP category the highest overall ECC precedence, while combining the other subcategories and criteria into a single, lower precedence level. Both of these precedence levels would receive preferential treatment over other PSN calls.

The same protection of carriers from violation of the Communications Act of 1934 offered by TSP should be offered by the new rule. As with TSP, only ECC features that the "selected vendor is able to provision" (TSP Appendix, Section 4.0, Scope) would be required to be provided. The ability of a vendor to provide the service would not mean that the vendor has to have the service ready to offer; rather, it would mean that the vendor has to have the technological capability in place to develop the service (i.e., has SS7 deployed and interconnected with other networks). As with TSP, carriers would recover their cost through "cost-causative cost recovery mechanisms" (TSP Section VI; paragraph 127). Most likely these mechanisms would be through special tariffs designed to recover the costs from the government users who order the services.

The ECC Task Force believes the FCC would approve the call-by-call ECC features discussed in this report. None of those features preempt general PSN user calls. Any delays caused would, except under the most extreme circumstances, be unnoticeable by the general PSN user.

An FCC rulemaking would be the method to ensure that ECC services are offered nationwide. Rather than having to contract with approximately 1,100-LECs, 2,000 cellular carriers, and 400 IXCs, the Government would mandate that all carriers having the technological capability offer the service. Most carriers will be deploying SS7; therefore, an FCC rulemaking would achieve the provisioning of call-by-call ECC preferential treatment by a majority of the

industry. Furthermore, this regulatory approach to implementation has the advantage of not requiring payment in advance from already strained government budgets. Carriers will nevertheless be assured of cost recovery, including a reasonable return, through tariffs and the expected amount of government traffic. Given the industry's recent experience with TSP, the ECC Task Force suggests that if this acquisition approach is chosen, the Government raise awareness throughout all levels of Government of the benefits to be derived so that the expected traffic levels are realized.

7.3.2 Implementation of New Nationwide ECC Services

The implementation of new nationwide ECC services to serve NS/EP users regardless of location is without precedent and will require innovative approaches from both Government and industry to achieve successful implementation. There will be a need for significant Government and industry interaction. There are a number of other steps required beyond the FCC rulemaking to implement these ECC services, as identified below.

- The ***functional requirements definition stage*** will require that the Government evaluate and select ECC services to be implemented and specify the government functional requirements in detail. As part of this effort, the Government will have to determine a realistic number of NS/EP users and their ability to pay for the use of these ECC services. This process of requirements definition will necessitate government interaction with industry to refine the concepts and select the most useful ECC services for implementation. The ECC Task Force believes that the Government should sponsor Government-industry forums to assist in the selection of the most promising ECC services. The result could be publication of the Government's detailed functional requirements for ECC services in the *Federal Register.*

- The ***concept development stage*** is next, where detailed business case and service requirements analyses are undertaken. This effort would be led by industry and would encompass assessment of the impact of ECC services regarding operations, technology, risks, and economic benefits.

- The ***standards development stage*** would compare existing capabilities and interconnection standards to the new ECC requirements. New standards would be promulgated as necessary. Several standards bodies may be involved in this portion of the effort, including the ECSA and the Telecommunications Industry Association (TIA). It is expected that industry would rely on existing ECSA and TIA bodies to carry out this effort (e.g., the ECSA T1 committee, Network Operations Forum [NOF], Industry Carrier Capability Forum [ICCF] and the TIA TR45 committee).

- The ***technical requirements and manufacturing stage*** would encompass detailed technical requirements development by service

vendors in conjunction with manufacturers, and agreements on how these services will interact with other network capabilities. It is necessary for industry to provide consistent or standard implementation of the desired ECC services where possible. However, there may be differences in certain cases. For example, network management exemptions will most likely be implemented differently among service vendors since different types of network management controls exist in the IXC and LEC networks.

- The ***service development stage*** would be accomplished by each affected IXC and LEC and would include: funding, equipment orders, installation, testing, OA&M plans, and training programs.

- The final part is the ***implementation stage*** where the new ECC services are tested, rates filed with regulatory bodies, and the services offered to NS/EP users.

Sections 8.0 and 9.0 present the conclusions and recommendations of the ECC Task Force, respectively. They are followed by the appendices of the report.

8.0 CONCLUSIONS

8.0 CONCLUSIONS

The conclusions presented in this section focus on the current and future capabilities of the PSN; the need for the NS/EP call identifier and the means to transport it through the PSN; regulatory concerns; and the need for an ECC services implementation plan.

- The NS/EP user can take advantage of certain features and capabilities to enhance call completion in the PSN such as avoidance routing, diverse routing, dual homing (IXC), dual hosting (LEC/IXC), and trunk subgrouping. Services provided by a VSAT arrangement could also provide an alternate means of access to the PSN.

- To provide call-by-call ECC on an end-to-end basis, an NS/EP call must be identified and its identifying mark transported along the call path through the network. After a call has been identified as an NS/EP call, it could be given preferential treatment over general public calls.

- There are several ways to invoke identification of an NS/EP call at its point of origin to prompt the generation of an identifying mark that would be transported with the call setup signals through the PSN.

- The HPC standard allows for an identification mark to be transported with the call set-up signals in the SS7 network. This mark identifies NS/EP calls for preferential treatment and is a fundamental requirement for developing ECC services. Because acceptance of the HPC standard within the standards bodies may be in jeopardy, the continued support of the Government and the advocacy of NSTAC member companies is needed to ensure the standard's approval.

- NS/EP users would be able to use CPE to further enhance ECC services by subscribing to a service such as the calling name delivery service. This service allows the calling party to determine the alphanumeric information sent, e.g., name, code word, or other calling party identification, and permits the called party to respond appropriately.

- The TSP system authorizes priority NS/EP circuit installation or restoration in the PSN. Further investigation is required to determine whether the FCC TSP Report and Order could be used to authorize and require call-by-call preferential treatment of NS/EP calls.

- ECC acquisition approaches may depend on whether the Government decides to provide ubiquitous or limited ECC services.

- As part of the ECC acquisition process, government-sponsored technical forums would assist the Government in defining high-level ECC functional requirements.

- While transporting NS/EP calls under the ECC services scheme may delay the completion of general public calls during periods of stress, the impact on the general public would be negligible.

- The cost of ECC services is inversely proportional to the size of the NS/EP user base. The current user base could be expanded by identifying additional Federal, and State, and local government emergency telecommunication users. The Government should consider conducting an impact study to determine the effect of a large increase in NS/EP user traffic on the general public traffic in the PSN and on ECC cost sensitivities as the NS/EP user base expands.

- Call-by-call ECC services are dependent on SS7. Nationwide deployment of SS7 is essential for nationwide ECC services.

- Automatic call rerouting to alternate IXCs is technically feasible, but the Interexchange Carrier Subscriber Plan (refer to FCC Docket No. 83-1145) allows assignment of only one primary IXC, i.e., a presubscribed IXC to carry interLATA calls originated on a specific access line or PBX trunk. Although automatic call rerouting to alternate IXCs is feasible, associated administrative and operational costs, combined with competitive realities, limit this feature's acceptability by LECs and IXCs.

9.0 RECOMMENDATIONS

9.0 RECOMMENDATIONS

A minimum level of ECC services can be provided now, but a greater, more effective level of service could be achieved in the long term. In the near term, the Government should explore the advantages of PSN augmentations available to the NS/EP user.

The task force recommends the Government use existing features in the PSN, work with standards and regulatory bodies on an ongoing basis, and monitor potential ECC capabilities to provide the NS/EP user with ECC services.

- The Government should take the following steps to enhance call completion for NS/EP users:
  - Take advantage of existing and emerging services, features, and capabilities in the PSN.
  - Continue to support the near-term adoption of the HPC standard by the ECSA T1 Committee.
  - Investigate the NS/EP advantages of a calling name delivery service.
  - Work with NSTAC's FRWG to investigate potential regulatory issues associated with authorizing call-by-call preferential treatment and requiring ubiquitous ECC services in the PSN.
  - Sponsor industry ECC forums to further define ECC functional requirements and resolve implementation issues.
- The Government should use the ECC Task Force report as a reference for modifying or implementing current or future services and technologies in the PSN.

The IES should deactivate the ECC Task Force and establish an ad hoc group to help the Government advocate and support approval of the HPC standard, work with the FRWG to investigate potential regulatory issues, and implement ECC network capabilities.

APPENDIX A

ENHANCED CALL COMPLETION TASK FORCE

APPENDIX A

ENHANCED CALL COMPLETION TASK FORCE

Chairman: Dr. Sushil Munshi, Sprint

AT&T	Mr. David Bush
Bellcore	Mr. Randall Schulz
GE	Mr. Donald Pidgeon
GTE	Mr. James Bean
McCaw Cellular	Mr. Richard McElhenie
MCI	Mr. Joseph Cassano
NTI	Dr. John Edwards
PTI	Mr. Frank Adams

*Mr. G. Jay Nelson, Sprint, is a supporting member of the task force.

APPENDIX B

CUSTOMER PREMISES EQUIPMENT ENHANCED CALL COMPLETION FEATURES

APPENDIX B

CUSTOMER PREMISES EQUIPMENT ENHANCED CALL COMPLETION FEATURES

CPE, such as PBX equipment plays an important role in access to the PSN for those NS/EP users it serves. This appendix points out some attributes of modern PBX systems that should be considered in the overall planning for providing enhanced call completion services to NS/EP users.

Section 5.0 describes a number of PSN features that can contribute to enhanced call completion for NS/EP critical users. Additional enhancement of call completion can be provided for many critical users who are served by PBXs that have trunks to the PSN and to one or more private switched networks. These trunks can be assigned to particular transmission facility routes to take advantage of PSN special routing features for access/egress circuits, as described in Appendix C. Table B-1 shows the kinds of special circuit routing that can be used with various kinds of CPE and indicates the greater access/egress capabilities of PBX and multiline key equipment as compared to a single line set.

TABLE B-1
Compatibility Of PSN Enhanced Call Completion Features With Customer Premises Equipment

	Single Line Set	Multi-Line Key Equipment	PBX
Priority Dial Tone (ESP)	XXX	XXX	XXX
Avoidance Routing	XXX	XXX	XXX
Diverse Routing		XXX	XXX
Dual Hosting		XXX	XXX
Dual Homing		XXX	XXX
Bypass Local Network		XXX	XXX
NS/EP Identifier	XXX	XXX	XXX

A PBX may also have multiple alternative and diverse means of PSN access and egress that naturally provide increased opportunity to originate and terminate calls to and from the PSN. Modern PBXs generally have the capability to connect to the following:

- LEC networks for local and long distance service

- Foreign exchange service to local exchange switches in distant cities
- One or more private switched networks that provide automatic or manual crossover to the PSN
- Direct connection to interexchange carrier switches for Wide Area Telephone Service (WATS) or 800 service
- Direct connection to interexchange carrier switches for access to virtual private line networks
- ISDN via Primary Rate Interface (PRI)
- Cellular systems via cellular trunks
- VSAT systems
- MSAT systems when available.

In addition, modern digital stored program controlled PBXs have many sophisticated internal features that inherently improve the ability of station users to originate or receive external calls. The most important of these features are listed in Table B-2. Definitions of these features can be found in Appendix G.

The combined use of PBX features listed in Table B-2, special routing of access/egress circuits, and ECC features of the transport segment of the PSN could provide the most favorable call completion conditions for NS/EP users served by PBXs.

It should be noted that as more sophisticated ECC capabilities are introduced into the PSN, it will be very important for such capabilities to be compatible with PBX equipment. Two important issues are:

- If an NS/EP call identifier is available in the PSN to enhance NS/EP calls, PBXs that serve NS/EP users must be able to accept and forward the call identifier to the PSN.
- If Multilevel Precedence and Preemption (MLPP) is introduced into the PSN for NS/EP service, PBXs that serve NS/EP users must be compatible with the MLPP signaling requirements of the PSN.

TABLE B-2
Customer Premises Equipment Enhanced Call Completion Features

PBX Feature	Access or Egress Function	Transportable to Interexchange Carrier
Abbreviated Dialing	Access	No
Attendant Override	Access and Egress	No
Authorization Codes	Access	Yes
Automatic Call Distribution	Egress	No
Automatic Identification of Outward Dialing	Access	Yes
Automatic Route Selection	Access	No
Call-by-Call Service Selection	Access and Egress	No
Call Forwarding	Egress	No
Call Pickup	Egress	No
Call Transfer	Egress	No
Call Waiting	Egress	No
Calling Number Identification	Access and Egress	Yes
Conferencing – Attendant – Meet-Me – Pre-Set – Progressive – Three-Way	Access and Egress	No
Executive Override	Access and Egress	No

TABLE B-2 (concluded)
Customer Premises Equipment Enhanced Call Completion Features

PBX Feature	Access or Egress Function	Transportable to Interexchange Carrier
Facility Restriction Level	Access	No
Hotline Service	Access	No
Last Number Dialed	Access	No
Multiple Numbers for Given Line	Egress	No
Remote Network Access	Access	No
Remote Call Forwarding	Egress	No
Time of Day Routing	Access	No
Trunk Queuing	Access	No
Vocal Preemption of Trunks	Access	No
Voice Mail	Egress	No

APPENDIX C

PSN AUGMENTATIONS AVAILABLE TO THE NS/EP USER

APPENDIX C

PSN AUGMENTATIONS AVAILABLE TO THE NS/EP USER

Appendix C contains descriptions of additional PSN features that NS/EP users could procure from PSN carriers to enhance call completion. Because application of most of these features is generally limited to single customer locations, they would have a lesser effect on enhancing call completion than those features described in Section 5.0 of this report. However, features such as avoidance routing, diverse routing, dual homing (IXC), dual hosting, and VSAT, although not universally available, could be obtained at some locations by individual NS/EP users, or individual NS/EP user locations, to provide diverse access to the PSN.

Although the feature, trunk subgrouping, is not applicable for an individual user and is only available in the PSN on a limited basis, its use could potentially be expanded into additional components of the PSN.

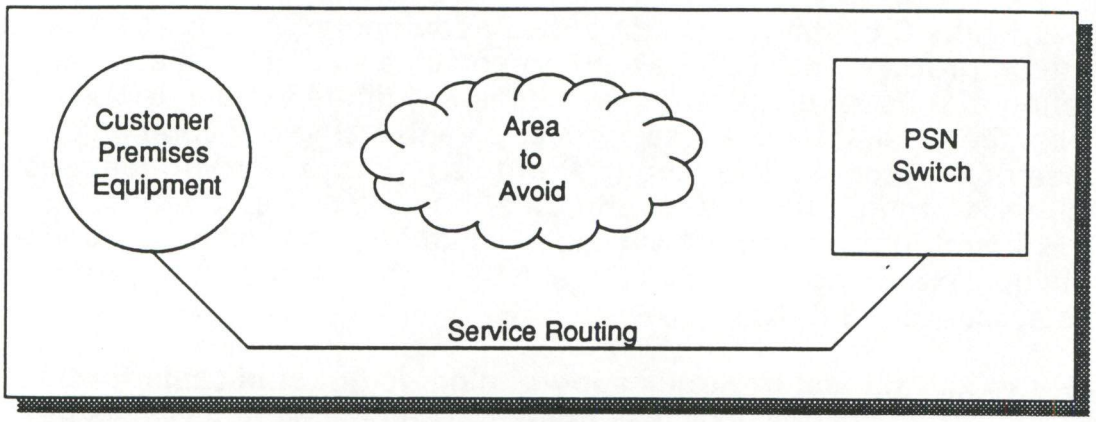
Table C-1 lists the features described in this appendix.

TABLE C-1
NS/EP User Initiated PSN Augmentations

FEATURE	AVAILABILITY
CUSTOMER INITIATED	
Avoidance Routing	Current
Diverse Routing	Current
Dual Homing (IXC)	Current
Dual Hosting (LEC/IXC)	Current
Trunk Subgrouping	Current
Very Small Aperture Terminal (VSAT)	Current

Avoidance Routing

EXHIBIT C-1
Typical Avoidance Routing Arrangement

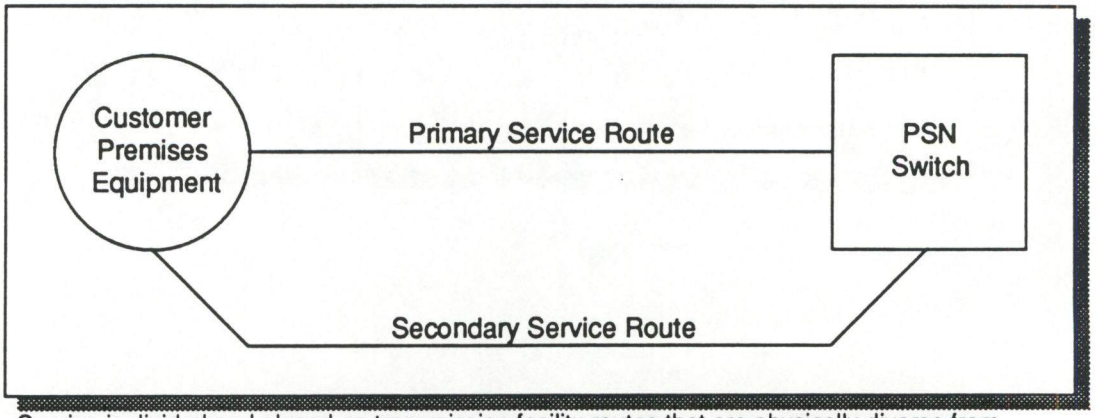


Service is placed on a facility route that bypasses an area of vulnerability.

Avoidance routing of circuits is a tariffed feature that permits a customer to enhance survivability of private network services or PSN access/egress services by directing the vendor to assign them to transmission facilities that avoid points of known vulnerability. This service may not be tariffed in all areas; however, in those areas where it is not tariffed, a customer might be able to obtain it under a special construction contract. Services provided via avoidance routing might be less susceptible to damage from a particular event and therefore could help ensure connection to the PSN for an NS/EP user. Cost of the service may vary according to service vendor and facility availability.

Diverse Routing

EXHIBIT C-2
Typical Diverse Routing Arrangement

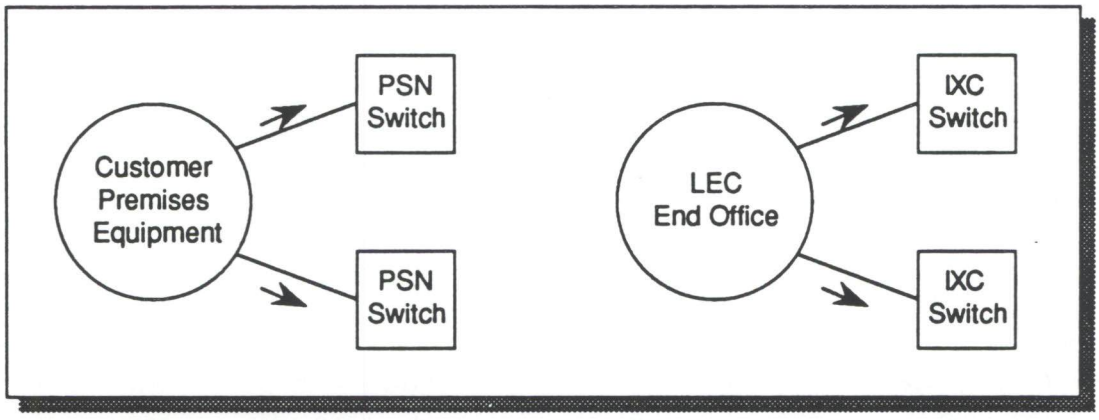


Service is divided and placed on transmission facility routes that are physically diverse from each other.

Diverse routing of circuits is similar to avoidance routing in that it is also a tariffed feature that may be used to enhance survivability of a customer's connection to a private network or the PSN. Diverse routing can be provided for a customer who has two or more circuits serving a location and wants them to be provided over physically separated, i.e., diverse, facility routes. The ability of a vendor to provide diverse routing depends on the availability of separated facility routes. In areas where separated facility routes do not exist, it may be possible for a customer to contract for the construction of a diverse route. Diverse routing could be used to advantage by an NS/EP user to switch service to a second route if the primary route fails. Cost of the service may vary according to service vendor and facility availability.

Dual Hosting in the LEC and IXC

EXHIBIT C-3
Typical Dual Hosting Arrangements (LEC/IXC)

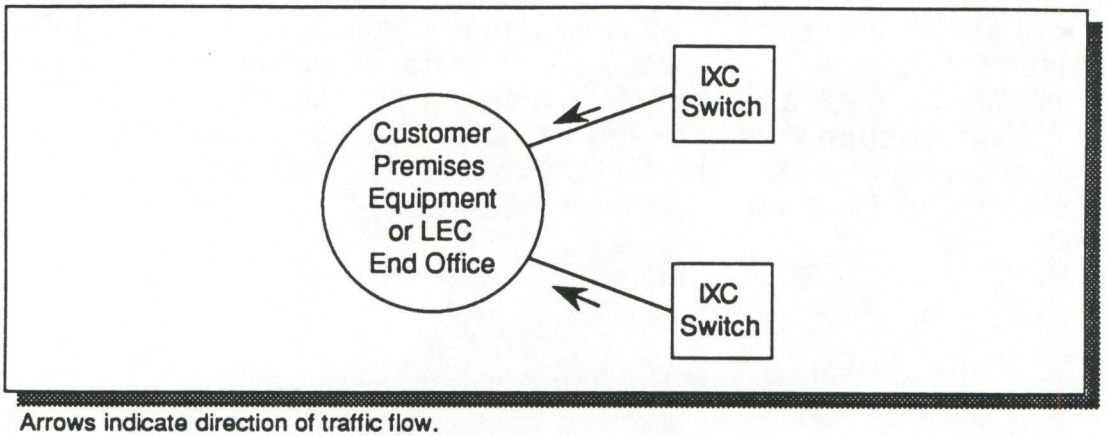


Arrows indicate direction of traffic flow.

Dual hosting implies the connection of a lower level switch in the hierarchy of a switched network to two other switches of a higher level in the same switched network. This arrangement allows forwarding of originating traffic from the lower level switch into the network through either of the two higher level switches. Dual hosting can enhance survivability by providing two points of access to the network from the lower level switch because if one switch would fail, service would be available through the other switch. Dual hosting could be employed for NS/EP communications by connecting Centrexes that serve NS/EP users to two access tandems or to two IXC switches for outgoing traffic. Another possibility would be to connect PBXs that serve NS/EP users to two LEC end offices or to two IXC switches for outgoing traffic. Ordinarily, diverse routing, described previously, would be used to route circuits between the low-level switch and the higher level switches. Costs would vary according to the particular situation and the providing vendor.

Dual Homing in the IXC

EXHIBIT C-4
Typical Dual Homing Arrangements (IXC)

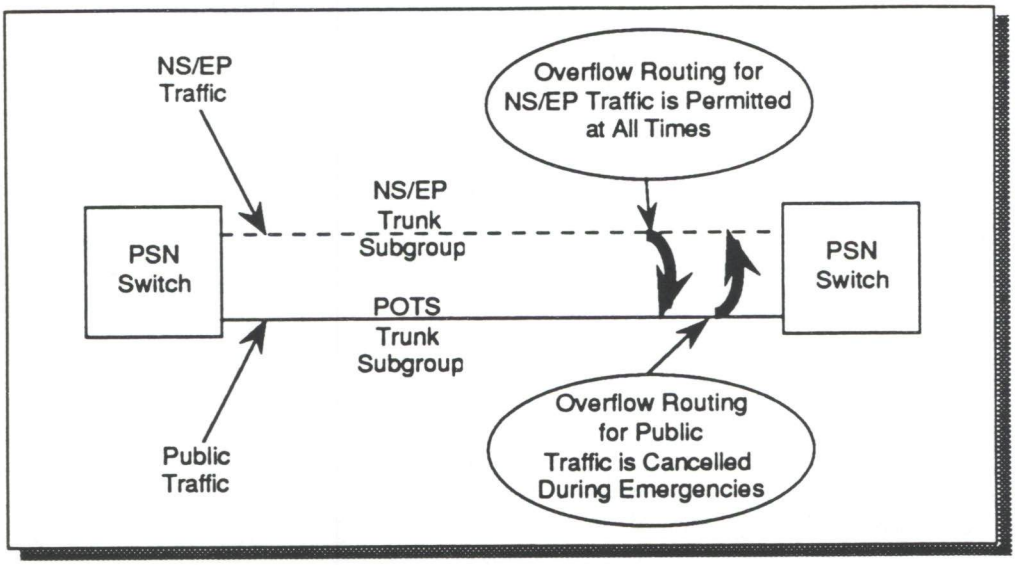


Arrows indicate direction of traffic flow.

Dual homing is similar to dual hosting in that it also implies the connection of a lower level switch in the hierarchy of a switched network to two other switches of a higher level in the same switched network for survivability purposes. The difference is that dual homing provides for the passing of traffic incoming from the network through either of the higher level switches to the lower level switch using a single telephone number address. This service requires special traffic routing capability that is currently available only in IXC networks. This limits application of the service to connections from IXC switches to Centrexes or to PBXs that serve NS/EP users. Diverse routing and dual hosting on IXC switches, described previously, would ordinarily be provided in conjunction with dual homing. Costs would vary according to the particular situation and the providing vendor.

Trunk Subgrouping

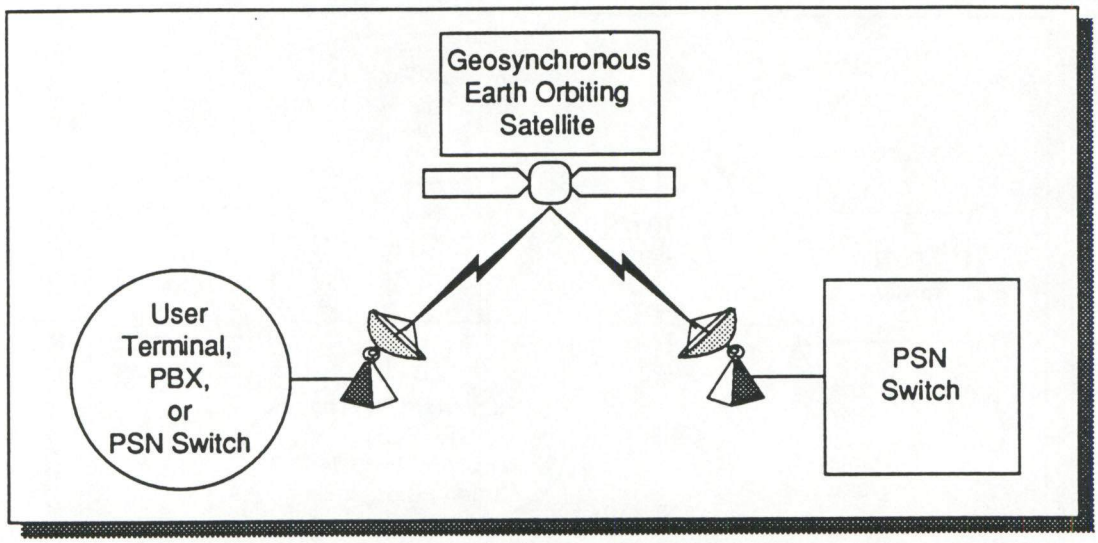
EXHIBIT C-5
Typical Trunk Subgrouping Arrangement



Trunk subgrouping is a PSN feature that can be applied to an interoffice trunk group hunting sequence so that the trunk group is split effectively into two parts or subgroups. One subgroup is then designated for general public traffic and the other subgroup is designated for specifically targeted traffic, such as NS/EP traffic. During normal day-to-day operation, general public traffic would be directed to the general public subgroup as first choice with overflow into the NS/EP subgroup permitted. Conversely, NS/EP identified calls would be directed to the NS/EP subgroup as first choice with overflow to the general public subgroup permitted. During emergencies, overflow of general public traffic to the NS/EP subgroup could be cancelled through implementation of network management controls, thereby dedicating the NS/EP subgroup to NS/EP traffic and still permitting NS/EP traffic to overflow to the general public subgroup. Subgrouping could be provided in any central office switch that would have the ability to differentiate between general public traffic and NS/EP traffic. Cost may vary according to the vendor and the type of switch involved.

Very Small Aperture Terminal (VSAT)

EXHIBIT C-6
Typical VSAT Arrangement



Transmission systems that operate via satellite using VSATs can be an important and versatile means of providing backup capability for transmission facilities that carry NS/EP communications. VSAT facilities can be used to augment existing transmission facilities or to replace failed transmission facilities between PSN switching nodes or between an NS/EP user location and a PSN switching node. Fixed VSATs can be provided at important locations and activated as required for NS/EP purposes. A similar capability can be provided with transportable VSATs that can be stored at strategic locations and rapidly deployed to otherwise isolated communications centers or to disaster sites to establish emergency communications. VSAT operational capability of this nature is described in detail in the Final Report of the Commercial Satellite Survivability Task Force, December 1989.

APPENDIX D

FUTURE POTENTIAL CAPABILITIES TO ENHANCE CALL COMPLETION

APPENDIX D

FUTURE POTENTIAL CAPABILITIES TO ENHANCE CALL COMPLETION

Appendix D contains descriptions of several conceptual features the task force identified that could provide additional assurance of NS/EP call completion. MSAT communications appears to be the most promising and earliest available of these technologies, but it will not be available for several years. Dual homing (LEC) would provide diverse access to the PSN for individual customer locations but may not be available for some time. MLPP could be effective for ECC; but it would not be available for several years because it would require extensive development work and coordination among the PSN carriers.

The last three services listed in Table D-1 could benefit the NS/EP user; however, they would not have any impact on the processing of calls though the PSN. Calling Name Delivery (CNAM) and Calling Name Blocking (CNAB), Calling Line Identification Presentation and Restriction (CLIP/CLIR), and User-to-User Signaling neither enhance completion of a call nor give it preferential treatment. These services only provide information about the calling party to the called party.

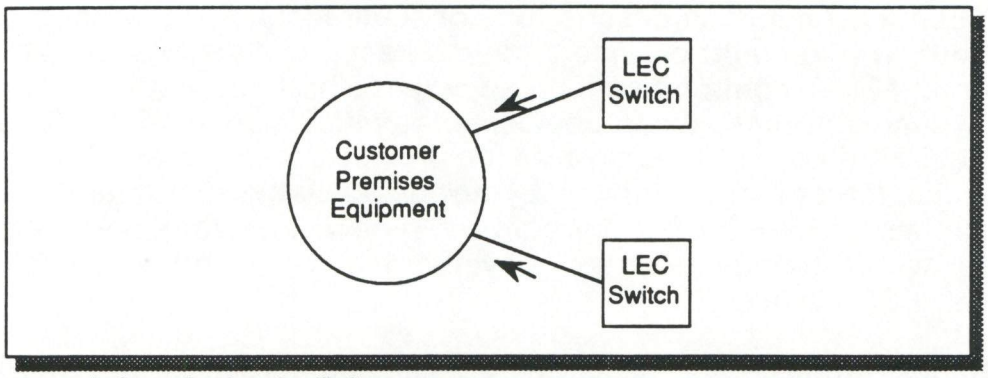
Table D-1 lists the features described in this appendix.

TABLE D-1
Potential Capabilities Enhance To Call Completion

FEATURE	AVAILABILITY
POTENTIAL CAPABILITIES	
Dual Homing (LEC)	Potential
Mobile Satellite (MSAT) Communications	Potential
Multilevel Precedence and Preemption (MLPP)	Potential
Calling Name Delivery (CNAM) and Calling Name Blocking (CNAB)	Potential
Calling Line Identification Presentation and Restriction (CLIP/CLIR)	Potential
User-to-User Signaling	Potential

Dual Homing in the LEC

EXHIBIT D-1
Typical Dual Homing Arrangement (LEC)

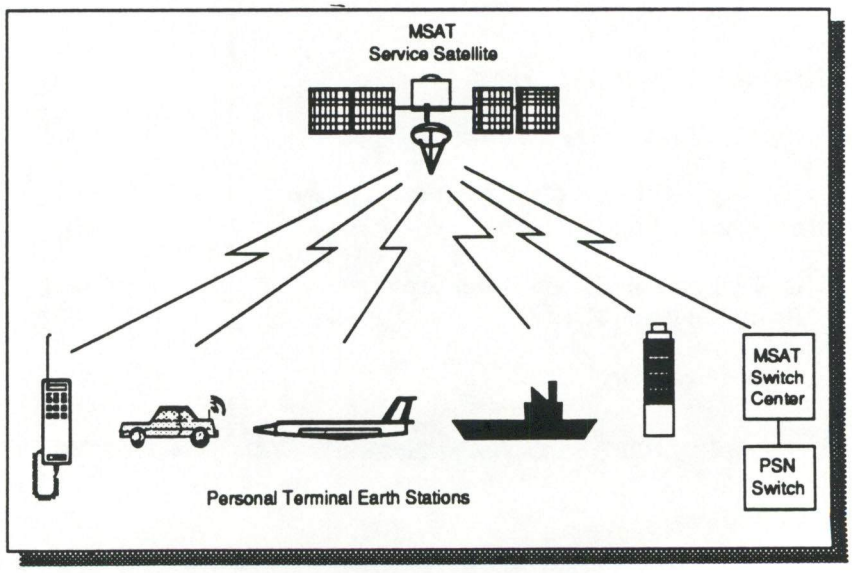


Arrows indicate direction of traffic flow.

Dual homing in a LEC network would be a survivability and reliability arrangement wherein the user service connection to the PSN would be provided at two separate end offices for traffic incoming from the network to a customer's PBX using a single telephone number address. This service would require special traffic routing capability that is not currently available in LEC networks. Diverse routing and dual hosting (described in Appendix C) would ordinarily be provided in conjunction with dual homing of a PBX on LEC end offices. Costs would vary according to the particular situation and the providing vendor.

Mobile Satellite Communications (MSAT)

EXHIBIT D-2
Mobile Satellite Communications (MSAT)



MSAT communications systems are based on advanced technology that provides the capability to establish single channel communication links via satellite using low powered terminals that may be hand held, vehicle mounted, or stationary. MSAT users will be able to communicate directly with one another and access the PSN through gateways that will connect the MSAT system to the PSN.

NS/EP communications via MSAT systems could be useful for emergency personnel working on site in heavily damaged or isolated areas. Also, the fact that these systems might be used to bypass damaged or congested terrestrial communications systems through their ability to access and be accessed from the PSN increases the importance of MSAT systems as possible additional or alternate means of communication.

The task force did not study MSAT systems in detail because availability of information concerning their intended voice operational capability and interface with the PSN is very limited and, because voice service will not be implemented until at least 1994, there is no operational experience to evaluate.

The total cost of this service will involve the purchase of the terminal equipment plus the cost of the MSAT service itself. In each case, the cost is expected to be relatively low because it will be spread across a large number of users and it must be low enough to be attractive to the general public.

Multilevel Precedence and Preemption (MLPP)

Multilevel precedence and preemption as used in the DISN maximizes use of limited communication resources. This feature sets a level of precedence for each call attempted on the DISN and employs this precedence as a determination or guide for preempting calls of a lower precedence if necessary to complete calls with a higher precedence.

If a similar capability would be introduced into the PSN, it would be especially beneficial for NS/EP users with high priority. The MLPP function would require use of an NS/EP call identifier and the preemption feature, as proposed, would be limited to the NS/EP user's domain only. The user's domain consists of a set of MLPP users and the network and access resources that are in use by that set of MLPP users at any given time.

Telecommunications industry standards groups have approved the standard for incorporating the MLPP signaling function into the Integrated Services Digital Network (ISDN) and SS7 signaling formats. This standard is now in the publication process, but it may take 3 to 5 years before the feature can be developed and implemented.

Calling Name Delivery (CNAM) and Calling Name Blocking (CNAB) Services

CNAM is a terminating service that provides the name associated with the calling party to the called party. Provision of privacy indication or a notice of

unavailability could be provided as an alternative to the calling party's name. The name information or notice of unavailability is displayed on the called party's caller identification device before the call is answered. This name, along with its related number, could be stored for later retrieval and call back.

The same privacy considerations that apply to the delivery of the calling name apply to the calling number. A calling party could have either a CNAB permanent privacy status or could invoke CNAB on a call-by-call basis. CNAB service permits the final called party to receive the calling name of the original caller and the name of the forwarding party. Therefore, CNAB must be available for both the calling and forwarding parties.

CNAM calls are identified by SS7 networks for the calling party number. This number could identify an NS/EP calling party and send a query to a database. The response of the database could include the calling NS/EP party's name or code name plus additional information of NS/EP rank or priority. This data would be transmitted to the called party's terminal and displayed.

The CNAM service is being worked in the T1S1 standards arena as a preliminary standard. This service is envisioned for both PSN and ISDN users. When final approval is given to the CNAM service, it could take several years to implement.

The service would be implemented and offered by carriers as a tariffed service. User costs associated with CNAM should be the same as standard network features, such as the LEC's calling number identification service, because of the widespread nature of the user market and the commonality of network design criteria for end-to-end implementation.

As the calling party number information element goes through a series of exchanges, it may encounter a non-SS7 exchange. The CNAM will not operate in a non-SS7 exchange. Interworking exchanges with SS7 encountered further along in the call will transport the calling party number information element. The network may notify the calling party that the calling party number was discarded if it could not be delivered to the called party.

Calling Line Identification Presentation and Restriction (CLIP/CLIR) Services

CLIP is an ISDN supplementary service offered to a called party; it provides the calling line identification to the called party. The calling line identification information may not include the calling party's number due either to lack of network CLIP offering or to interaction with the CLIR service. The calling party number or notice of unavailability is displayed on the called party's device before the call is answered. This number could be stored for later retrieval and call back.

The current PSN also offers a CLIP service, but because of current PSN limitations often does not deliver the actual calling party number. For example,

the PSN does not know the actual number from a user calling through a private branch exchange (PBX) end instrument.

CLIR is an ISDN supplementary service offered to a calling party that restricts presentation of that calling party's identification to the called user. All ISDN calls may include a calling party number in an information element that is sent over the SS7 network. This number could be used to identify an NS/EP calling user through a CLIP-to-number or CLIP-to-name translation database on the called NS/EP user's premises before the call is answered.

As the calling party number information element goes through a series of exchanges, it may encounter a non-SS7 exchange. The CLIP/CLIR services will not operate in non-SS7 exchanges. Interworking exchanges with SS7 encountered further along in the call will transport the calling party number information element. The network may notify the calling party that the calling party number was discarded if it could not be delivered to the called party.

User costs associated with CLIP/CLIR should be the same as standard network features, such as LEC's caller identification features, because of the widespread nature of the user market and the commonality of network design criteria for end-to-end implementation.

The CLIP/CLIR services draft standard was approved by letter ballot at the T1S1 level. All comments were resolved at the May 11-15, 1992 T1S1 meeting in Chicago. The approval process has advanced to the T1 letter ballot stage. When final approval is given to the CLIP/CLIR standard, carriers can implement the service and offer it by tariff.

User-to-User Signaling Service

User-to-User Signaling Service is an ISDN supplementary service that provides a means of communication for exchange of information between two users. The network may notify the calling user that the information was discarded if it could not be delivered to the called user.

All ISDN calls may include a user-to-user information element in that it is sent over the SS7 network. This information can identify an NS/EP calling user, or contain a password, or personal identification number, or even a short message up to 128 octets. This information could be displayed or verified by a device on the called NS/EP user's premises before the call is answered.

As the user-to-user information element goes through a series of exchanges, it may encounter a non-SS7 exchange. The User-to-User Signaling Service will not operate in non-SS7 exchanges. Interworking exchanges with SS7 encountered further along in the call will transport the user-to-user information element.

This service would be implemented and offered by carriers as a tariffed service. User costs associated with User-to-User Signaling Service should be

the same as standard network features because of the widespread nature of the user market and the commonality of network design criteria for end-to-end implementation.

The standard for User-to-User Signaling was approved at the T1 level at the May 11-15, 1992 T1 meeting in Chicago. Vendors can begin to offer the service in areas where ISDN and enhanced SS7 are available to provide user-to-user service.

APPENDIX E

LIST OF ACRONYMS

APPENDIX E

LIST OF ACRONYMS

ALT	Alternate Network Providers
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AT	Access Tandem
AUTOVON	Automatic Voice Network
CAC	Carrier Access Code
CCITT	Consultative Committee on International Telephone and Telegraph
CCS	Common Channel Signaling
CIC	Carrier Identification Code
CLID	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CNAB	Calling Name Blocking
CNAM	Calling Name Delivery
CNID	Calling Name Identification
CNS	Commercial Network Survivability
CPE	Customer Premises Equipment
CSA	Communications Service Authorization
CSI	Commercial SATCOM Interconnectivity
DISN	Defense Information System Network
DTP	Dial Tone Protection
ECC	Enhanced Call Completion
EF&I	Engineered, Furnished, and Installed
ELS	Essential Line Service
E.O.	Executive Order
ESL	Essential Line Service
ESN	Electronic Serial Number
ESP	Essential Service Protection
FAR	Federal Acquisition Regulations
FCC	Federal Communications Commission

FIFO	First In, First Out
FRL	Facility Restriction Level
FRWG	Funding and Regulatory Working Group
FTS2000	Federal Telecommunications System 2000
GETS	Government Emergency Telecommunications Service
GPS	Global Positioning System
HPC	High Probability of Completion
IAM	Initial Address Message
ICCF	Industry Carrier Capability Forum
IES	Industry Executive Subcommittee
IFB	Invitation for Bid
IP	Intelligent Peripheral
ISDN	Integrated Services Digital Network
IXC	Interexchange Carrier
LATA	Local Access and Transport Area
LEC	Local Exchange Carrier
LIFO	Last In, First Out
LLC	Line Load Control
LOE	Level-of-Effort
MFJ	Modified Final Judgement
MIN	Mobile Identification Number
MLPP	Multilevel Precedence and Preemption
MLPQ	Multilevel Precedence and Queuing
MPL	Message Priority Level
MSAT	Mobile Satellite
MTSO	Mobile Telephone Switching Office
MTT	Mobile Transportable Telecommunications
NCS	National Communications System
NOF	Network Operations Forum
NOPR	Notice-of-Proposed Rulemaking
NPA	Numbering Plan Area
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
OA&M	Operation, Administration, and Maintenance

PBX	Private Branch Exchange
PCS	Personal Communications Service
PIC	Primary Interexchange Carrier
PIN	Personal Identification Number
POP	Point of Presence
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PSN	Public Switched Network
RBOC	Regional Bell Operating Companies
RFI	Request for Information
RFP	Request for Proposal
SONET	Synchronous Optical Network
SOW	Statement of Work
SS7	Signaling System 7
SSN	Survivable Signaling Network
TIA	Telecommunications Industry Association
TSP	Telecommunications Service Priority
TSR	Telecommunications Service Request
VSAT	Very Small Aperture Terminal
WATS	Wide Area Telephone Service

APPENDIX F

GLOSSARY

APPENDIX F

GLOSSARY

Abbreviated Dialing – A feature by which a telephone user can attempt a call by dialing a two- or three-digit code that instructs the central office to obtain the actual desired number from a look-up table and transmit it into the network to connect the calling line to the called line.

Advanced Intelligent Network (AIN) – A concept for Intelligent Networks that allows the flexible placement of logic either in adjunct processors associated with network switches or in centralized control points. From an NS/EP perspective, AIN will enable the user to call up selected software packages and create a customized network configuration.

Alternate Routing – The ability of a network to select alternate paths in the network to route traffic to its destination when the primary route is congested or out of service.

Assured Access – See Automatic Call Rerouting

Attendant Override – A feature that allows a PBX operator to interrupt a telephone call in progress.

Authorization Codes – A unique multidigit code used to allow an authorized subscriber privileged access to a network, system, or device. If the code is validated, the call is allowed to advance.

Automatic Call Distribution – A system designed to evenly distribute traffic by directing incoming calls to the most idle terminal in a group of terminals.

Automatic Call Rerouting – An automatic capability at the local exchange carrier end office and/or access tandem to select alternate interexchange carriers in the order predetermined by the subscriber if the designated primary carrier network cannot be accessed.

Automatic Identification of Outward Dialing – A feature that enables a switching system to identify the telephone number of the line originating a call, without operator intervention.

Automatic Route Selection – A feature that enables a switching system to choose the lowest cost route for long distance calls from among available options. If all trunks in the first choice group are busy, the next group is checked and the procedure continues until an available trunk is found or until an all-trunks-busy condition is encountered.

Avoidance Routing – A special routing arrangement that provides improved survivability by routing selected circuits over paths that avoid known or possible sources of difficulty such as areas of congestion or target areas.

Call Blocking – A network management control measure that limits the number of calls being sent to a specific destination address NXX code or area code.

Call-By-Call Service Selection – A feature that provides improved trunking efficiency between a PBX and a local exchange end office by allowing a variety of services to use the same trunk group and by distributing traffic over the total number of available trunks on a call-by-call basis.

Call Forwarding – A feature that enables calls to be rerouted automatically from one line to another or to an attendant. It permits a station user to instruct its serving switch to transfer incoming calls to a specified alternate number when the user's station is busy or unattended.

Call Gapping – A network management technique whereby blocking is instituted on calls to a specific destination address NXX code or area code. The blocking algorithm is based on allowing X number of calls into the network each number of Y seconds.

Call Pickup – A PBX feature that enables a connected extension to answer any ringing extension within an assigned call pickup group

Call Transfer – A feature whereby a call to a subscriber's number is automatically transferred to one or more alternative numbers when the called number is busy or does not answer.

Call Waiting – A feature that provides a distinctive audible tone to a busy subscriber line to notify the user when another caller is attempting to reach his or her number.

Calling Number Identification – A feature that provides the identification of the calling subscriber's number by means of a visual or audible indication at the called terminal.

Commercial Network Survivability (CNS) – A component program of the National Communications System National Level Program that focuses on providing survivable routes for NS/EP users of the PSN by augmenting selected facilities and routes at the interexchange carrier and local exchange carrier levels with additional leased and government-provided equipment and services.

Commercial SATCOM Interconnectivity (CSI) – A component program of the National Communications System National Level Program that focuses on the use of commercial satellites to reconnect isolated portions of an IXC network.

Conferencing (Attendant) – A feature that requires the use of an operator to set up conferences among more than three parties.

Conferencing (Meet-Me) – A feature for establishing a conference without operator assistance, whereby all conferees dial a special number that is connected to a multiparty conference bridge.

Conferencing (Pre-Set) – A feature for establishing a conference by the keying of a special code to the central office by the conference originator. Upon receipt of the code, the central office automatically calls all parties required to be connected to the conference call.

Conferencing (Progressive) – A feature for establishing a conference by a station user who acts as the conference originator and calls each conferee in turn and adds that person to the conference.

Conferencing (Three-Way) – A feature that allows users to set up three-party conferences without operator assistance.

Diverse Cellular Network-to-PSN Access – A survivability and flexibility feature that enables cellular networks to directly interconnect with other elements of the PSN at the local exchange carrier end office, access tandem, and interexchange carrier network switch levels.

Diverse PSN-to-Cellular Network Egress – A survivability and flexibility feature by which direct egress connectivity to the mobile telephone switching office (MTSO) can be provided from access tandems and interexchange carriers as well as from the local exchange carrier end offices.

Diverse Routing – A survivability feature in which access lines or channels serving the same facility are routed over different geographically separated paths.

Dual Homing – A survivability and reliability arrangement that provides for the provision of user service so that connection to the PSN is provided by two different switching centers for terminating calls.

Dual Hosting – A survivability and reliability arrangement that provides for the provision of user service so that connection to the PSN is provided by two different switching centers for originating calls.

Dynamic Nonhierarchical Routing – Computer controlled routing of calls depending on actual traffic at the time that the call is presented for service; in contrast to hierarchical routing where various classes of switching offices each have a defined level of responsibility, calls are not automatically passed up the hierarchical structure for routing on a final choice circuit. Instead, all switches operate at the same routing level and calls are completed over high usage circuits, providing increased flexibility.

Enhanced Call Completion – A set of network features/capabilities that permit NS/EP users to complete calls over the PSN with minimum delay during network damage and/or congestion.

Essential Service Protection – A service arrangement that ensures that a small number of customer lines designated as "essential" have priority over the general public for reception of dial tones during periods of PSN overload. Such service may also be known as Priority Dial Tone and ELS.

Executive Override – A feature of some telephone systems that permits certain users to monitor or enter telephone conversations on other extensions.

Facility Restriction Level (FRL) – A feature that limits user calling privileges for incoming and outgoing calls. The FRL determines if a call attempt is permitted and which routes can be used or denied in the routing process.

High Probability of Completion – A proposed standard that is designed for Signaling System 7 message formats that would mark NS/EP calls from end to end and would provide priority to NS/EP call originations during periods of congestion.

Hot Line Service – A feature that provides automatic dialing of a predesignated number by going off-hook.

Integrated Services Digital Network – A switched network capability providing end-to-end digital transparency where voice and data services are transported over the same switching and transmission facilities.

Last Number Redial – A feature that enables a user to redial the last number dialed by pressing a single button or entering a code.

Local Network Bypass – A connectivity arrangement that provides subscriber bypass of the end office and direct connection to the interexchange carrier network.

Mobile Satellite – A telecommunications capability that enables a user equipped with a mobile or portable satellite terminal to communicate with other mobile or portable satellite terminals on the same MSAT system or to obtain access to the PSN through the MSAT system and one of its PSN gateways. This capability is in the developmental stage, with different implementations being planned.

Multilevel Precedence and Preemption – The capability of a communications system to handle traffic at more than one precedence designation level with the capability to seize (usually automatic) system facilities being used to serve a lower precedence call, in order to serve a higher precedence call. For example, the capability of handling flash override, flash, immediate, priority, and routine traffic all in the same network and all within the specified precedence level definition limits.

Multiple Numbers for Given Line – A feature that enables two or more unique telephone numbers to be assigned to the same terminal or instrument.

Network Management Control – A set of control measures used to prevent or control degradation in the quality of network service. Such measures can be described as being protective or expansive. Protective measures limit traffic going into a switch or trunk group. Expansive measures generally increase routing choices by providing more capability than normal to carry excess traffic.

NS/EP Call Identifier – A unique identifying mark that would prompt operational elements of the PSN to differentiate between NS/EP calls and general public calls and provide the NS/EP calls with signaling, switching, and traffic routing advantages.

Off-hook Waiting for Outgoing Trunks – A Centrex-implemented capability whereby an authorized user meeting an all-routes-busy condition is allowed to wait off-hook for a designated time period while the list of trunk groups is continually scanned for an idle trunk.

Partitioning – The restriction of access to some switched facilities to provide a particular group of users with enhanced network services. Partitioning could include the use of multilevel precedence and preemption (MLPP) and related measures. The partitioning structure is sometimes changed at different times of the day or on different dates to permit the usage of the system to be changed.

Position Locating/Tracking (Cellular Network) – The ability to locate and connect a call to a mobile cellular user automatically, regardless of whether or not that user is located within his "home" or a "visited" cellular system. This capability does not require the calling party to know the whereabouts of the called party and requires only the dialing of the called party's "home" cellular number. Also known as Automatic Call Delivery or Seamless Cellular Service.

Presubscription – Choice by a customer of his selected primary interexchange carrier for inter-LATA calls.

Priority Dial Tone – (See Essential Service Protection).

Priority Service – A class of service that enables selected users to receive precedence on an end-to-end basis over other users of the services provided by the network.

Public Switched Network – The ordinary dial-up telephone system. For the purpose of this study, the PSN includes switched voice grade services provided by cellular telephone systems, local exchange carriers (LEC), and interexchange carriers.

Queuing – Holding calls and presenting them automatically to a subsystem or to operators when resources become available.

Remote Network Access – A feature that permits authorized callers to call from the PSN into a PBX and then use the features of the PBX.

Remote Call Forwarding – A service offered by some telephone companies by which all calls to a given number are automatically transferred to a different number.

Route Augmentation – Measures taken within a commercial carrier network or among multiple networks to increase the capability to carry traffic by augmenting carrier facilities with additional transmission equipment and capacity.

Signaling System No. 7 – An internationally standardized common channel signaling system optimized for operation in digital telecommunications networks over 64-kbps digital channels. SS7 uses signaling links for the transfer of signaling messages between exchanges or other nodes in the telecommunications network served by the system. Arrangements are made to ensure the reliable transfer of signaling information in the presence of transmission disturbances or network failures.

Survivable Signaling Network (SSN) – A unique service being designed by one interexchange carrier to provide enhanced survivability to its signaling network for the exclusive use of NS/EP traffic.

Time of Day Routing – A feature that provides the most economical routing of calls based on the time of day that each call is made.

Trunk Queuing – A trunk congestion control feature that, under conditions where all circuits in a trunk group are occupied, enables selected calls to be held in a queue and presented to the next available outgoing trunk either in the order of their arrival or by precedence.

Trunk Reservation – A protective control measure that alleviates the effects of trunk congestion between a pair of directly connected switches for selected traffic by dynamically reserving capacity for their use.

Trunk Subgrouping – A protective control measure, activated by administrative procedure, that divides trunk groups into trunk subgroups and restricts access to these trunk subgroups to make them available for the exclusive use of designated high priority traffic.

User Class Identifier – A service access code in a destination address, a traveling classmark, or a line or trunk classmark used to distinguish one class of user (e.g., NS/EP users) from other users with regard to the special features/options that class of user is allowed to use.

Very Small Aperture Terminal Capability – A capability that enables a user to employ a VSAT with a parabolic antenna from 1.2 to 3.6 meters in diameter to access a private satellite network and through that network, gain access to the public switched network.

Via Routing – Special routing that enables two points to be connected via a network path through other points in the network.

Voice Mail – A feature that automatically answers incoming calls and permits callers to leave recorded messages when the called stations are busy or not answered.